


P_thesis_main.pdf

 Delhi Technological University

Document Details

Submission ID

trn:oid:::27535:115673944

Submission Date

Oct 6, 2025, 2:09 PM GMT+5:30

Download Date

Oct 6, 2025, 2:16 PM GMT+5:30

File Name

P_thesis_main.pdf

File Size

32.9 MB

204 Pages

52,778 Words

262,762 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.





Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 10 words)
- Submitted works
- Internet sources




Exclusions

- 4 Excluded Sources

Match Groups

-  **248** Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks
-  **0** Missing Quotations 0%
Matches that are still very similar to source material
-  **0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation
-  **0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 0%  Internet sources
- 7%  Publications
- 0%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 248** Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks
- 0** Missing Quotations 0%
Matches that are still very similar to source material
- 0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 0% Internet sources
- 7% Publications
- 0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

- 1** Publication
Yongjin Xian, Xingyuan Wang, Xiaoyu Wang, Qi Li, Xiaopeng Yan. "Spiral-Transfor... <1%
- 2** Publication
Yongjin Xian, Xingyuan Wang. "Fractal sorting matrix and its application on chaot... <1%
- 3** Publication
A. Ponmaheshkumar, R. Perumal. "Origami-based image encryption scheme usin... <1%
- 4** Publication
Alghamdi, Yousef. "Lightweight Image Encryption Algorithms: Design and Evalua... <1%
- 5** Publication
Manjit Kaur, Vijay Kumar. "Beta Chaotic Map Based Image Encryption Using Gene... <1%
- 6** Publication
Xilin Liu, Xiaojun Tong, Zhu Wang, Miao Zhang. "A new n-dimensional conservativ... <1%
- 7** Publication
Akram Belazi, Sofiane Kharbech, Md Nazish Aslam, Muhammad Talha, Wei Xiang, ... <1%
- 8** Publication
Rohit, Shailendra Kumar Tripathi, Bhupendra Gupta, Subir Singh Lamba. "A comp... <1%
- 9** Publication
Shiya Wang, Jianbin He. "Design of new chaotic system with multi-scroll attractor ... <1%
- 10** Publication
Xiaoqiang Zhang, Xuangang Yan. "Adaptive Chaotic Image Encryption Algorithm ... <1%

11	Publication	Mohamed Yamni, Achraf Daoui, Chakir El-Kasri, May Almousa, Ali Abdullah S. AlQ...	<1%
12	Publication	Jackson J, Perumal R. "A robust medical image encryption technique using invers...	<1%
13	Publication	Varun Agarwal, Dhirendra Kumar. "Secure chaotic image encryption method usin...	<1%
14	Publication	Xingyuan Wang, Wenhua Xue, Jubai An. "Image encryption algorithm based on T...	<1%
15	Publication	Qiang Lai, Hui Zhang, Paul Didier Kamdem Kuate, Guanghui Xu, Xiao-Wen Zhao. "...	<1%
16	Publication	"Multimedia Security Using Chaotic Maps: Principles and Methodologies", Spring...	<1%
17	Publication	Omer Kocak, Uğur Erkan, Abdurrahim Toktas, Suo Gao. "PSO-based image encryp...	<1%
18	Publication	Xiaosong Gao, Xingbin Liu. "CLSM-IEA: a novel cosine-logistic-sine map and its ap...	<1%
19	Publication	Qianqian Shi, Jiayang Qu, Shaocheng Qu, Xinlei An, Ziming Wei. "Dynamical anal...	<1%
20	Publication	Abdurrahim Toktas, Uğur Erkan, Deniz Ustun. "An image encryption scheme base...	<1%
21	Publication	Tanveer Qayyum, Tariq Shah. "Hybrid image encryption algorithm based on Galoi...	<1%
22	Publication	Shuqin Zhu, Congxu Zhu. "Security Analysis and Improvement of an Image Encry...	<1%
23	Publication	Uğur Erkan, Abdurrahim Toktas, Qiang Lai. "2D hyperchaotic system based on Sc...	<1%
24	Publication	YongHui Huang, QiLin Zhang, YongBiao Zhao. "Color image encryption algorithm ...	<1%

25	Publication	Samanta, Susanta. "Design and Analysis of MDS and Near-MDS Matrices and Thei...	<1%
26	Publication	B. Rahul, K. Kuppusamy, A. Senthilrajan. "Bio-Metric Based Colour-Image-Encrypti...	<1%
27	Publication	Hegui Zhu, Yiran Zhao, Yujia Song. "2D Logistic-modulated-Sine-coupling-Logistic ...	<1%
28	Publication	B.M.K. Prasad, Karan Singh, Shyam S. Pandey, Richard O'Kennedy. "Communicati...	<1%
29	Publication	Narbda Rani, Vinod Mishra, Suvita Rani Sharma. "Image encryption model based ...	<1%
30	Publication	Xingbin Liu, Shuyi Zheng, Jing Yang. "Color image encryption scheme based on a ...	<1%
31	Publication	Lingzhi Zhou, Han Xia, Qingfa Lin, Xin Yang, Xiangwei Zhang, Man Zhou. "Two-di...	<1%
32	Publication	Muhammad Shahbaz Khan, Jawad Ahmad, Ahmed Al-Dubai, Nikolaos Pitropakis, ...	<1%
33	Publication	Lin Teng, Xingyuan Wang, Yongjin Xian. "Image encryption algorithm based on a ...	<1%
34	Publication	Zhuozhao Chen, Guodong Ye. "An asymmetric image encryption scheme based o...	<1%
35	Publication	Hong-wei Xie, Ya-jun Gao, Hao Zhang. "An image encryption algorithm based on ...	<1%
36	Publication	Feyza Toktas, Uğur Erkan, Zeki Yetgin. "Cross-channel color image encryption thr...	<1%
37	Publication	J. Jackson, R. Perumal. "A robust image encryption technique based on an improv...	<1%
38	Publication	Qiang Lai, Genwen Hu, Uğur Erkan, Abdurrahim Toktas. "A novel pixel-split image...	<1%

39	Publication	Ali Mansouri, Pin Sun, Chengzhi Lv, Yinghua Zhu, Xudong Zhao, Hongwei Ge, Cha...	<1%
40	Publication	Kartikey Pandey, Deepmala Sharma. "Novel image encryption algorithm utilizing ...	<1%
41	Publication	Patrick J. Van Fleet. "Discrete Wavelet Transformations", Wiley, 2019	<1%
42	Publication	MEHMET DEMIRTAS, Sabri Altunkaya. "A novel chirp-based 2D hyperchaotic map f...	<1%
43	Publication	Wajid Ali, Zhang Zuping, Muhammad Hussain. "A novel chaotic-based image encr...	<1%
44	Publication	Wu, Xiangjun, Dawei Wang, Jürgen Kurths, and Haibin Kan. "A novel lossless color...	<1%
45	Publication	Zhen Le, Quanjun Li, Huang Chen, Shuting Cai, Xiaoming Xiong, Linqing Huang. "...	<1%
46	Publication	Chiranjeev Bhaya, Arup Kumar Pal, SK Hafizul Islam. "A novel image encryption a...	<1%
47	Publication	R. Sujatha, H. N. Ramaswamy, C. S. Yogananda. "Math Unlimited - Essays in Math...	<1%
48	Publication	Wu, Pianhui. "Research on Digital Image Watermark Encryption Based on Hyperc...	<1%
49	Publication	Bhaskar Mondal, Shyam Singh Rajput. "Multimedia Security - Tools, Techniques, a...	<1%
50	Publication	Bin Ge, Gang Chen, Xu Chen, Zhihua Shen. "Efficient Hyperchaotic Image Encrypti...	<1%
51	Publication	"Proceedings of CECNet 2022", IOS Press, 2022	<1%
52	Publication	Paul, Partha Sarathi. "Enhanced-Entropy Chaotic Circuit Design for Overhead-Con...	<1%

53	Publication	Muhammad Sajjad, Nawaf A. Alqwaify. "A Novel RGB Image Encryption Scheme u...	<1%
54	Publication	Pankaj Rakheja, Amanpreet Kaur. "Robust phase-only hologram encryption for iri...	<1%
55	Publication	Xiuhui Chen, Mengxin Gong, Zhihua Gan, Yang Lu, Xiuli Chai, Xin He. "CIE-LSCP: c...	<1%
56	Publication	Zhongyun Hua, Zhihua Zhu, Shuang Yi, Zheng Zhang, Hejiao Huang. "Cross-plane ...	<1%
57	Publication	Pengfei Fang, Han Liu, Chengmao Wu, Min Liu. "A block image encryption algorit...	<1%
58	Publication	Xudong Liu, Xiaojun Tong, Miao Zhang, Zhu Wang, Yunhua Fan. "Image compress...	<1%
59	Publication	Yang Lu, Mengxin Gong, Zhihua Gan, Xiuli Chai, Lvchen Cao, Binjie Wang. "Exploit...	<1%
60	Publication	Hangming Zhang, Hanping Hu, Weiping Ding. "Image encryption algorithm base...	<1%
61	Publication	J.R. Anisha, Y.P. Arul Teen. "An adaptive approach for securing patient data in int...	<1%
62	Publication	Kamlesh Kumar Raghuvanshi, Subodh Kumar, Sushil Kumar, Sunil Kumar. "Devel...	<1%
63	Publication	Kehan Chen, Haijun Zhang, Fei Yan. "An adaptive image compression-encryption ...	<1%
64	Publication	M. Naim, A. Ali Pacha. "A new chaotic satellite image encryption algorithm based ...	<1%
65	Publication	Mohit Dua, Suraj Singh Jadon, Anant Raghuvanshi, Deepanshu Vishwakarma, She...	<1%
66	Publication	Qiuxia Qin, Zhongyue Liang, Shuang Liu, Changjun Zhou. "A Self-adaptive Image ...	<1%

67	Publication	Uğur Erkan, Abdurrahim Toktas, Feyza Toktas, Fayadh Alenezi. "2D er-map for im...	<1%
68	Publication	Xiaoqiang Zhang, Xuesong Wang. "Multiple-Image Encryption Algorithm Based o...	<1%
69	Publication	"Scanning Auger Electron Microscopy", Wiley, 2005	<1%
70	Publication	Cemile İnce, Kenan İnce, Davut Hanbay. "A Multilayer Nonlinear Permutation Fra...	<1%
71	Publication	Jing Yang, Xingbin Liu. "Enhancing secure storage and sharing of multi-image in c...	<1%
72	Publication	Malory, Sean James. "Bayesian Inference for Stochastic Processes", Lancaster Uni...	<1%
73	Publication	Priya Ramasamy, Vidhyapriya Ranganathan, Seifedine Kadry, Robertas Damaševi...	<1%
74	Publication	Quanyv Wang, Xiaoqiang Zhang, Xiaohu Zhao. "Image encryption algorithm base...	<1%
75	Publication	Robert Bridson. "Fluid Simulation for Computer Graphics", A K Peters/CRC Press, ...	<1%
76	Publication	Tingyu An, Tao Gao, Ting Chen, Donghua Jiang, Lulu Xu, Yuxiu Chen, Peng Zhao. "...	<1%
77	Publication	Xilin Liu, Xiaojun Tong, Miao Zhang, Zhu Wang. "A highly secure image encryptio...	<1%
78	Publication	Yonghui Huang, Qilin Zhang, Yongbiao Zhao. "A novel color image encryption alg...	<1%
79	Publication	"Proceedings of International Conference on Communication and Computational...	<1%
80	Publication	Akram Belazi, Anouar Ben Mabrouk. "A refined sine-derived chaotic map for secu...	<1%

81	Publication	Akshat Tiwari, Prachi Diwan, Tarun Dhar Diwan, Mahdal Miroslav, S. P. Samal. "A ...	<1%
82	Publication	Ali Mansouri, Pin Sun, Chengzhi Lv, Yinghua Zhu, Xudong Zhao, Hongwei Ge, Cha...	<1%
83	Publication	C. Sivaranjani Devi, Rengarajan Amirtharajan. "A novel 2D MTMHM based key gen...	<1%
84	Publication	Dani Elias Mfungo, Xianping Fu. "Fractal-Based Hybrid Cryptosystem: Enhancing I...	<1%
85	Publication	Daniel Clemente-López, Jesus M. Munoz-Pacheco, José de Jesus Rangel-Magdalen...	<1%
86	Publication	Gigengack, Fabian, Michael Fieseler, Daniel Tenbrinck, and Xiaoyi Jiang. "Image P...	<1%
87	Publication	Jianeng Tang, Feng Zhang, Hui Ni. "A novel fast image encryption scheme based ...	<1%
88	Publication	Jilei Sun. "2D-SCMCI hyperchaotic map for image encryption algorithm", IEEE Acc...	<1%
89	Publication	Jingxi Tian, Xiaoqiang Zhang, Mi Liu, Songchang Jin, Dianxi Shi, Shaowu Yang. "Re...	<1%
90	Publication	Khalid Charif, Zine El Abidine Guennoun. "A novel image encryption algorithm ba...	<1%
91	Publication	Linyu Wang, Zhongjie Luo, Jianhong Xiang, Wei Liu. "Dynamics study, synchronou...	<1%
92	Publication	Lujie Wang, Chen Zhong, Xiyu Sun, Chenchen He. "Color image ROI encryption al...	<1%
93	Publication	Mohammed S. Alshehri, Sultan Almakdi, Mimonah Al Qathrady, Jawad Ahmad. "C...	<1%
94	Publication	Prabhavathi K, Anandaraju M B, Vinayakumar Ravi. "Region Based Medical Image...	<1%

95	Publication	Qiyang Ren, Zhipeng Wang. "Designing a 1D Extended Logistic Map for a Secure I...	<1%
96	Publication	René Lozi, Safwan El Assad, Mohammed-Salah Abdelouahab. "Dynamical Systems...	<1%
97	Publication	Rim Amdouni, Mohamed Ali Hajjaji, Abdellatif Mtibaa. "Hardware Study and Impl...	<1%
98	Publication	Rim Amdouni, Mohamed Gafsi, Ramzi Guessmi, Mohamed Ali Hajjaji, Abdellatif M...	<1%
99	Publication	Roayat Ismail Abdelfatah, Reham Mohamed Elsobky, Salah Aldeen Khamis. "Ultra...	<1%
100	Publication	Unsub Zia, Mark McCartney, Bryan Scotney, Jorge Martinez, Mamun AbuTair, Jam...	<1%
101	Publication	Uğur Erkan, Abdurrahim Toktas, Samet Memiş, Qiang Lai, Genwen Hu. "An image...	<1%
102	Publication	Wei Chen, Yichuan Wang, Cheng Shi, Guanglei Sheng, Mengyang Li, Yu Liu, Xinho...	<1%
103	Publication	Yibo Huang, Chong Li, Zhiyong Li, Qiuyu Zhang, Fanwang Yang. "Fractal matrix sp...	<1%
104	Publication	Ömer Koçak, Uğur Erkan, İsmail Babaoglu. "Design and Practical Implementation...	<1%

Development of Robust Image Cryptography Schemes using Chaotic Mathematical Models

A Thesis Submitted
in Partial Fulfillment of the Requirements for the
Degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

Puneet Kumar Pal

Roll no. 2K21/PHDAM/12

Under the Supervision of

Dr. Dharendra Kumar
Assistant Professor



Department of Applied Mathematics
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daultpur, Main Bawana Road, Delhi-110042

October 6, 2025

© Delhi Technological University–2025
All rights reserved.

CANDIDATE'S DECLARATION

I, **Puneet Kumar Pal**, hereby certify that the work which is being presented in the thesis entitled “**Development of Robust Image Cryptography Schemes using Chaotic Mathematical Models**” in partial fulfillment of the requirements for the award of the Degree of Doctor of Philosophy submitted in the Department of Applied Mathematics, Delhi Technological University, Delhi is an authentic record of my own work carried out during the period from 22nd June 2021 to 6th October 2025 under the supervision of Dr. Dhirendra Kumar.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other Institute.

Puneet Kumar Pal
Roll no. 2K21/PHDAM/12

CERTIFICATE

Certified that **Mr. Puneet Kumar Pal** (Roll no. 2K21/PHDAM/12) has carried out his research work presented in this thesis entitled “**Development of Robust Image Cryptography Schemes using Chaotic Mathematical Models**” for the award of **Doctor of Philosophy** from Department of Applied Mathematics, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Dr. Dhirendra Kumar

Supervisor

Department of Applied Mathematics

Delhi Technological University

Delhi.

Prof. R. Sriavastava

Head of Department

Department of Applied Mathematics

Delhi Technological University

Delhi.

ACKNOWLEDGEMENT

I express my sincere gratitude to my supervisor **Dr. Dhirendra Kumar**, for his motivation and unconditional support during my research. It has been a great pleasure to work under his guidance, and I am deeply thankful for his invaluable assistance in making this work possible.

I am thankful to DRC Chairperson, **Prof. Sangita Kansal**, Head of the department, **Prof. R. Srivastava** and all DRC members for extending their support and providing all the facilities necessary for my research. I am also thankful to the Dean PG and her office staff for their prolonged support.

My heartfelt thanks go to my friends **Yash Sharma, Gagan Sharma, Yash Pathak**, and **Kunal Madaan** for their unwavering camaraderie. Their constant encouragement and willingness to read through my work have been a source of great strength throughout this journey.

I am also grateful to **HRDG-CSIR, Government of India**, for providing a fellowship with sanction order number 08/0133(13253)/2022-EMR-I that made my Ph.D. work possible.

Finally, I am deeply indebted to my family, in particular, **my parent**, for their unconditional support, patience, and encouragement have been the foundation of my success. Without their love and belief in me, I would not be where I am today.

Above all, I express my heartfelt gratitude to the **Almighty Lord Shiva** for guiding me on the right path and giving me the strength and perseverance to complete this journey.

Date: October 6, 2025

Puneet Kumar Pal

Place: Delhi, India.

ABSTRACT

With the exponential growth of multimedia data and increasing concerns over privacy and information security, image encryption has become a crucial area of research. Traditional encryption algorithms, though effective for textual data, are often inefficient for images due to their large size, high redundancy, and strong pixel correlations. Despite their importance, these image encryption algorithms face several drawbacks. First, many image-specific methods suffer from key sensitivity issues. Second, some algorithms fail to provide resistance against classical attacks, thereby compromising security. Third, some methods fail in resisting the statistical attacks and differential attacks. Fourth, some methods cannot even reduce the correlation coefficient between the adjacent image pixels.

To overcome these drawbacks, chaotic maps were used in the application of image encryption. Chaotic maps, with its inherent features of sensitivity to initial conditions, unpredictability, and ergodicity, are popular for designing secure and efficient image encryption algorithms. But a few chaotic maps available in literature suffer from limitations including narrow range of control parameter, non-uniform output distributions, low and negative Lyapunov exponents and insufficient randomness.

This thesis introduces a novel set of discrete chaotic maps designed to overcome limitations in chaos-based image encryption algorithms, such as narrow chaotic range and non-uniform distribution. The proposed maps demonstrate a significantly broader chaotic range, a uniform output distribution, and higher Lyapunov exponents, culminating in robust pseudo-random number generators. These generators form the core of a new image encryption algorithms that integrate novel confusion-diffusion architecture, specifically designed to minimize adjacent pixel correlation and maximize cipher image randomness. The effectiveness of the proposed approach is rigorously validated through a comparative security analysis against state-of-the-art algorithms. Comprehensive tests including statistical, differential, and chosen-plaintext attacks, low correlation coefficient and information entropy closer to 8, confirms the algorithm's superiority, while maintaining high computational efficiency. The collective contributions of this work establish a more secure, efficient, and reliable framework for digital image encryption.

Dedicated
To
my parents

Contents

CANDIDATE’S DECLARATION	ii
CERTIFICATE BY THE SUPERVISOR	iv
Acknowledgement	vi
Abstract	viii
List of Tables	xvii
List of Figure	xx
List of Abbreviations	xxv
1 Introduction	1
1.1 Background	1
1.2 Motivation	3
1.3 Objectives and Contributions	4
1.4 Organization of the Thesis	6
2 Preliminaries and Literature Review	9
2.1 Introduction	9
2.2 Literature review	12
2.2.1 Chaotic maps in Literature	12
2.2.2 Image encryption algorithm in literature	15
2.3 Performance measures	19
2.3.1 Performance measures for chaotic map	19
2.3.2 Performance measures for image encryption algorithm	21
2.4 Data-set description	25

3	Zirili map with application in Image Encryption	27
3.1	Background	28
3.2	Proposed Zirili map	29
3.3	Analysis of the Zirili map	29
3.3.1	Bifurcation diagram	30
3.3.2	Phase diagram	30
3.3.3	Lyapunov exponent	32
3.3.4	Permutation entropy	32
3.3.5	Sample entropy	32
3.4	Application of map in image encryption	34
3.4.1	Obtaining secret key and chaotic sequence	35
3.4.2	Modified Cyclic Diffusion with Pixel Mixing	36
3.4.3	Cascading Confusion Transformation	38
3.5	Analysis of the image encryption algorithm	41
3.5.1	Information entropy analysis	41
3.5.2	Differential attack	42
3.5.3	Histogram analysis	42
3.5.4	Correlation Coefficient analysis	43
3.5.5	Resistance to classical attacks	45
3.5.6	Occlusion attack	45
3.5.7	Noise attack	47
3.5.8	Randomness test	47
3.5.9	Execution time analysis	47
3.6	Summary	48
4	Coupled Kaplan-Yorke-Logistic map with application in Image Encryption	51
4.1	Background	52
4.1.1	Kaplan-Yorke map	52
4.1.2	Logistic map	52
4.2	Proposed coupled Kaplan-Yorke-Logistic map	53
4.3	Analysis of the Kaplan-Yorke-Logistic map	54
4.3.1	Bifurcation diagram	54
4.3.2	Phase diagram	55
4.3.3	Lyapunov exponent	57
4.3.4	Permutation entropy	58

4.3.5	Sample entropy	58
4.4	Application of map in image encryption	58
4.4.1	Sequence generation	59
4.4.2	Simultaneous confusion and diffusion process	61
4.5	Analysis of the image encryption algorithm	63
4.5.1	Information entropy analysis	63
4.5.2	Differential attack	64
4.5.3	Histogram analysis	65
4.5.4	Correlation coefficient analysis	66
4.5.5	Resistance to classical attacks	66
4.5.6	Occlusion attack	67
4.5.7	Noise attack	69
4.5.8	NIST randomness test	69
4.5.9	Execution time analysis	70
4.6	Summary	70
5	SHIELD map with application in Image Encryption	73
5.1	Background	74
5.2	Proposed SHIELD map	75
5.3	Analysis of the SHIELD map	75
5.3.1	Bifurcation diagram	76
5.3.2	Phase diagram	76
5.3.3	Lyapunov exponent	78
5.3.4	Permutation entropy	79
5.3.5	Sample entropy	79
5.4	Application of the map in image encryption	79
5.4.1	Secret key generation method	80
5.4.2	Two-step confusion operation	80
5.4.3	Dynamic diffusion operation	84
5.5	Analysis of the image encryption algorithm	86
5.5.1	Information entropy analysis	86
5.5.2	Differential attack	87
5.5.3	Histogram analysis	87
5.5.4	Correlation Coefficient analysis	89
5.5.5	Resistance to classical attacks	90
5.5.6	Occlusion attack	92

5.5.7	Noise attack	92
5.5.8	NIST randomness test	93
5.5.9	Execution time analysis	94
5.6	Summary	94
6	Modified chaotic maps with application in Image Encryption	95
6.1	Background	95
6.1.1	$e\pi$ map	96
6.1.2	Fractal Sorting Matrix	96
6.2	Proposed Sine $e\pi$ map and Non-Linear Sine hyper-chaotic map	99
6.2.1	Sine $e\pi$ map	99
6.2.2	Non-Linear Sine hyper-chaotic Map	99
6.3	Analysis of Sine $e\pi$ map and Non-Linear Sine hyper-chaotic Map . .	100
6.3.1	Bifurcation diagram	100
6.3.2	Phase diagram	101
6.3.3	Lyapunov exponent	101
6.3.4	Permutation entropy	103
6.3.5	Sample entropy	104
6.4	Application of maps in image encryption	105
6.5	Analysis of the image encryption algorithm	107
6.5.1	Information entropy analysis	107
6.5.2	Differential attack	108
6.5.3	Histogram analysis	109
6.5.4	Correlation Coefficient analysis	109
6.5.5	Resistance to classical attacks	111
6.5.6	Occlusion attack	113
6.5.7	Noise attack	113
6.5.8	NIST randomness test	114
6.5.9	Execution time analysis	116
6.6	Summary	116
7	Magic Square Matrix based Fractal Sorting Matrix and its application in Image Encryption	117
7.1	Background	118
7.2	Proposed Zirili–Logistic map	118
7.3	Analysis of the Zirili–Logistic Map	119

7.3.1	Bifurcation diagram	119
7.3.2	Phase diagram	119
7.3.3	Lyapunov exponent	120
7.3.4	Permutation entropy	123
7.3.5	Sample entropy	123
7.4	Proposed Magic Square Matrix-based Fractal Sorting Matrix	123
7.5	Application of magic square matrix-based FSM and map in image encryption algorithm	127
7.6	Analysis of the image encryption algorithm	128
7.6.1	Information entropy analysis	129
7.6.2	Differential attack	129
7.6.3	Histogram analysis	130
7.6.4	Correlation Coefficient analysis	132
7.6.5	Resistance to classical attacks	132
7.6.6	Occlusion attack	133
7.6.7	Noise attack	135
7.6.8	NIST randomness test	135
7.6.9	Execution time analysis	135
7.7	Summary	136
8	Image Encryption using multiple chaotic maps	139
8.1	Background	139
8.1.1	Tinkerbell Map	140
8.1.2	Linear Feedback Shift Register	140
8.2	Proposed image encryption algorithm	141
8.3	Analysis of the image encryption algorithm	143
8.3.1	Information entropy analysis	143
8.3.2	Differential attack	144
8.3.3	Histogram analysis	145
8.3.4	Correlation Coefficient analysis	146
8.3.5	Resistance to classical attacks	148
8.3.6	Occlusion attack	148
8.3.7	Noise attack	149
8.3.8	NIST randomness test	149
8.3.9	Execution time analysis	151
8.4	Summary	151

9 Conclusion, Future Scope and Social Impact	153
9.1 Conclusion	153
9.2 Future Scope	156
9.3 Social Impact	157
Bibliography	159
List of Publications	175

List of Tables

2.1	Chaotic maps used for comparison.	15
3.1	Information entropy values of the cipher images obtained using ZM-IEA and other existing IEAs.	41
3.2	NPCR values of the ZM-IEA and other existing IEAs.	42
3.3	UACI values of the ZM-IEA and other existing IEAs.	42
3.4	Comparison of correlation coefficient values of ZM-IEA with algorithms available in the literature.	44
3.5	Randomness test results for ZM-IEA.	48
3.6	Comparison of execution time (in seconds) of the ZM-IEA with algorithms available in the literature.	48
4.1	Comparison of information entropy values of the KYLM-IEA with algorithms available in the literature.	63
4.2	Comparison of NPCR values of KYLM-IEA with algorithms available in the literature.	64
4.3	Comparison of UACI values of the KYLM-IEA with algorithms available in the literature.	64
4.4	Comparison of correlation coefficient values of KYLM-IEA with algorithms available in the literature.	66
4.5	Randomness test results for KYLM-IEA.	70
4.6	Comparison of execution time (in seconds) of the KYLM-IEA with algorithms available in the literature.	70

5.1	Comparison of information entropy values of the SHIELD-IEA with algorithms available in the literature.	87
5.2	Comparison of NPCR values of SHIELD-IEA with algorithms available in the literature.	88
5.3	Comparison of UACI values of the SHIELD-IEA with algorithms available in the literature.	88
5.4	Comparison of correlation coefficient values of SHIELD-IEA with algorithms available in the literature.	90
5.5	Randomness test results for SHIELD-IEA.	93
5.6	Comparison of execution time (in seconds) of the SHIELD-IEA with algorithms available in the literature.	94
6.1	Comparison of information entropy values of the SEPM-IEA and NLS-IEA with algorithms available in the literature.	108
6.2	Comparison of NPCR values of SEPM-IEA and NLS-IEA with algorithms available in the literature.	108
6.3	Comparison of UACI values of the SEPM-IEA and NLS-IEA with algorithms available in the literature.	109
6.4	Comparison of correlation coefficient values of SEPM-IEA and NLS-IEA with algorithms available in the literature.	111
6.5	Randomness test results for SEPM-IEA and NLS-IEA.	115
6.6	Comparison of execution time (in seconds) of the SEPM-IEA and NLS-IEA with algorithms available in the literature.	116
7.1	Comparison of information entropy values of the ZLFSM-IEA with algorithms available in the literature.	130
7.2	Comparison of NPCR values of ZLFSM-IEA with algorithms available in the literature.	130
7.3	Comparison of UACI values of the ZLFSM-IEA with algorithms available in the literature.	131

7.4	Comparison of correlation coefficient values of ZLFSM-IEA with algorithms available in the literature.	132
7.5	Randomness test results for ZLFSM-IEA.	136
7.6	Comparison of execution time (in seconds) of the ZLFSM-IEA with algorithms available in the literature.	136
8.1	Comparison of information entropy values of the proposed IEA with algorithms available in the literature.	144
8.2	Comparison of NPCR values of proposed IEA with algorithms available in the literature.	144
8.3	Comparison of UACI values of the proposed IEA with algorithms available in the literature.	145
8.4	Comparison of correlation coefficient values of proposed IEA with algorithms available in the literature.	147
8.5	Randomness test results for proposed IEA.	150
8.6	Comparison of execution time (in seconds) of the proposed IEA with algorithms available in the literature.	151

List of Figures

3.1	3D representation of Zirili function.	29
3.2	Bifurcation diagrams of Zirili map.	30
3.3	Phase diagrams (x and y).	31
3.4	Lyapunov exponent diagram of Zirili and others maps.	33
3.5	Permutation entropy of Zirili map.	33
3.6	Sample entropy of Zirili map.	34
3.7	Image encryption algorithm leveraging Zirili Map.	34
3.8	Illustration of Modified Cyclic Diffusion with Pixel Mixing.	37
3.9	Cascading Confusion Transformation (CCT).	40
3.10	Histogram of plain and encrypted images	44
3.11	Pixel distribution of plain and cipher images	45
3.12	Resistance to classical attacks	46
3.13	Representation of ZM-IEA's resistance to cropping attack	46
3.14	Representation of ZM-IEA's resistance to Noise attack	47
4.1	Diagrams related to Kaplan-Yorke map.	53
4.2	Logistic map	53
4.3	Bifurcation diagram of the KYLM.	55
4.4	Phase diagrams (x and y).	56
4.5	Lyapunov exponent diagram of Kaplan-Yorke-Logistic and others maps.	57
4.6	Permutation entropy of KYLM.	58

4.7	Sample entropy of KYLM.	59
4.8	Image encryption algorithm leveraging KYLM (KYLM-IEA).	59
4.9	Histogram of plain and cipher images obtained using KYLM-IEA.	65
4.10	Pixel distribution of plain and cipher images obtained using KYLM-IEA.	67
4.11	Resistance to classical attacks	68
4.12	Representation of KYLM-IEA's resistance to cropping attacks.	68
4.13	Representation of KYLM-IEA's resistance to Noise attack.	69
5.1	Bifurcation diagram of SHIELD map.	76
5.2	Phase diagrams (x and y).	77
5.3	Lyapunov exponent spectrum of SHIELD map and other maps.	78
5.4	Permutation entropy of SHIELD map	79
5.5	Sample entropy of SHIELD map	80
5.6	Bit-level shuffling operation.	83
5.7	Image encryption algorithm (SHIELD-IEA).	86
5.8	Histogram of plain and cipher images	89
5.9	Pixel distribution of plain and cipher images obtained using SHIELD-IEA.	91
5.10	Resistance to classical attacks	91
5.11	Representation of SHIELD-IEA's resistance to cropping attack	92
5.12	Representation of SHIELD-IEA's resistance to Noise attack	93
6.1	Bifurcation diagram of SEPM map.	100
6.2	Bifurcation diagram of NLS map.	101
6.3	Phase diagrams (x and y).	102
6.4	Lyapunov exponent diagram of SEPM, NLS and others maps.	103
6.5	Permutation entropy of SEPM and NLS map.	104
6.6	Sample entropy of SEPM and NLS map.	104

6.7	Bit separation process	105
6.8	Histogram of plain and encrypted images: ((a)-(c)) Histogram of plain images, ((d)-(f)) Histogram of cipher images obtained using SEPM-IEA, ((g)-(i)) Histogram of cipher images obtained using NLS-IEA	110
6.9	Pixel distribution of plain and cipher images obtained using SEPM-IEA and NLS-IEA.	112
6.10	Resistance to classical attacks (a) Plain image, (b) SEPM-IEA, (c) NLS-IEA, (d-f) Corresponding histograms.	113
6.11	Representation of SEPM-IEA's and NLS-IEA's resistance to cropping attack	114
6.12	Representation of SEPM-IEA's and NLS-IEA's resistance to Noise attack	115
7.1	Bifurcation diagram of Zirili-Logistic Map.	120
7.2	Phase diagrams (x and y).	121
7.3	Lyapunov exponent diagram of Zirili-Logistic and others maps.	122
7.4	Permutation entropy of ZLM.	123
7.5	Sample entropy of ZLM.	124
7.6	Histogram of plain and cipher images	131
7.7	Pixel distribution of plain and cipher images obtained using ZLFSM-IEA.	133
7.8	Resistance to classical attacks	134
7.9	Representation of ZLFSM-IEA's resistance to cropping attack	134
7.10	Representation of ZLFSM-IEA's resistance to Noise attack	135
8.1	Diagrams of Tinkerbell map.	140
8.2	Schematic representation of linear feedback shift register	141
8.3	Proposed image encryption algorithm.	143
8.4	Histogram of plain and cipher images	146
8.5	Pixel distribution of plain and cipher images obtained using proposed IEA.	147

8.6	Resistance to classical attacks	148
8.7	Representation of proposed IEA's resistance to cropping attack	149
8.8	Representation of proposed IEA's resistance to Noise attack	150

List of Abbreviations

IEA	Image Encryption Algorithm
LE	Lyapunov Exponent
ZM	Zirili Map
PD	Phase Diagram
BD	Bifurcation Diagram
LE	Lyapunov Exponent
PE	Permutation Entropy
SE	Sample Entropy
FSM	Fractal Sorting Matrix
ZLM	Zirili-Logistic Map
KYLM	Kaplan-Yorke-Logistic Map
NPCR	Number of Pixel Change Rate
UACI	Unified Averaged Changed Intensity
LFSR	Linear Feedback Shift Register

Chapter 1

Introduction

This chapter serves as a foundational framework, presenting background in Section 1.1, motivation in Section 1.2 along with the contribution in Section 1.3. The organization of thesis is discussed in Section 1.4.

1.1 Background

In this digital age, the exchange of multimedia data have become an integral part of modern communication systems [1]. Among various forms of multimedia, digital images occupy a particularly significant position due to their extensive use across multiple critical sectors. From medical diagnostics and military operations to surveillance systems, journalism, and social networking platforms, images serve as powerful tools for conveying complex information rapidly and accurately [2]. Their visual nature makes them indispensable in contexts where text or numerical data alone may fall short in delivering comprehensive insights or interpretations. As a result, digital images are now being produced and shared across open networks at a large scale. Sometimes the digital images may contain secret information that if gets leaked, it can have serious consequences for both individuals and institutions.

However, despite their usefulness, digital images also present unique challenges from

a data processing and security standpoint. One of the fundamental characteristics of image data is its high volume. A single high-resolution image can contain millions of pixels, each carrying intensity or color information. This results in a substantial amount of data that must be handled carefully, whether during storage, processing, or transmission. Moreover, images exhibit a high degree of spatial redundancy, meaning that adjacent pixels are highly correlated [3]. In natural images, the value of a given pixel is usually very similar to that of its neighboring pixels, especially in areas with consistent textures. This high inter-pixel correlation poses specific challenges and opportunities in various domains, such as image encryption.

Image encryption is a technique that aims to protect visual data by transforming a plain image into an unintelligible format [4]. The encryption ensures that the visual content cannot be interpreted by any unintended recipient often referred to as an adversary. To encrypt images, two main operations confusion and diffusion operations are applied. Confusion refers to the process of rearranging the positions of the image pixels, while diffusion focuses on altering the actual values of the image pixels [5]. Together, the confusion and diffusion operations complement each other to achieve a high level of security [6]. While confusion destroys the spatial relationships of pixels, diffusion conceals the original intensity values and statistical patterns. Hence, effective image encryption algorithms (IEAs) must not only manage the large volume of data in digital images but also address the inherent pixel-wise correlations to maintain image integrity, confidentiality, and efficiency.

Traditional cryptographic algorithms such as the Advanced Encryption Standard (AES) [7], Data Encryption Standard (DES) [8], and Rivest–Shamir–Adleman (RSA) [9] have been extensively used to protect textual data. However, applying these algorithms directly to encrypt images can lead to several challenges due to the characteristics posed by images. Furthermore, due to their weak diffusion performance, they are not suitable for image encryption applications. To address these limitations, researchers have explored alternative encryption methods specifically suited for images. Among them, chaos-based cryptographic techniques have emerged as a highly promising domain [10, 11].

Chaos theory deals with deterministic systems that exhibit unpredictable behavior

due to extreme sensitivity to initial conditions, topological mixing, and dense periodic orbits. [12]. Chaotic systems are easy to implement and are used as pseudo-random number generators encryption applications [13, 14]. When incorporated into IEAs, chaotic systems significantly enhance security by ensuring a vast key space and offering robust resistance against various cryptanalytic attacks, such as brute-force, statistical, and differential attacks. Numerous chaotic maps have been explored for this purpose, including Logistic map [15], Sine map. These maps can be used individually or in combination to enhance the unpredictability and robustness of the encryption process.

1.2 Motivation

In recent years, a wide range of chaos-based IEAs have been proposed, leveraging techniques such as compressive sensing [16, 17, 18], DNA-based encoding [19, 20], quantum operations [21, 22], chaotic systems [23, 24], and optics-based methods [25, 26]. While these methods contribute to the advancement of secure multimedia transmission, many existing IEAs suffer from critical limitations.

Several algorithms lack sufficient key sensitivity, making them vulnerable to brute-force and differential attacks. Others fail to defend against known-plaintext and chosen-ciphertext attacks, thereby compromising the confidentiality of encrypted data. Additionally, some algorithms do not introduce adequate randomness into the ciphertext, leaving them susceptible to statistical attacks. Furthermore, many techniques struggle to significantly reduce the correlation between adjacent pixels, which weakens their ability to obscure image patterns.

Chaotic systems have been widely adopted in IEAs due to their inherent properties such as sensitivity to initial conditions, deterministic unpredictability, and pseudo-random behavior [27]. However, many recent chaotic maps used in digital encryption suffers from narrow chaotic range of control parameter, non-uniform output distribution, low or negative Lyapunov exponents (LE), and low entropy [28]. Moreover, when implemented on digital platforms, the finite-precision arithmetic can introduce periodicity and lead to the degeneration of chaotic behavior, ultimately affecting the security

4

of the algorithm.

Low-dimensional chaotic systems often lack the complexity needed to ensure high levels of security. Their behavior can become predictable under specific parameter settings, reducing their effectiveness in cryptographic applications.

This thesis is motivated by the following key challenges identified in the existing literature:

1. The existing IEAs suffer from key sensitivity issues, weak confusion-diffusion mechanism, and vulnerability to statistical and differential attacks.
2. Many chaotic maps used in IEAs exhibit non-uniform distributions, limited chaotic range, and low LEs, limiting their effectiveness.
3. Several algorithms fail to sufficiently reduce inter-pixel correlation in cipher images, resulting in compromised visual confidentiality.

To address these issues, there is a need to develop novel chaotic systems with enhanced dynamical properties, as well as robust encryption algorithms that offer high computational efficiency along with resistance to several cryptanalytic attacks.

1.3 Objectives and Contributions

The objective of the thesis is to explore and evaluate the effectiveness of chaos-based IEA. Specifically, the study aims to investigate how various chaotic maps and their integration with cryptographic frameworks contribute to strengthening confusion and diffusion mechanisms. By analysing recent advancements and hybrid approaches, the objective is

1. To develop a high-dimensional chaotic maps with unlimited range of control parameter, multiple positive LEs, uniform output distribution with its application in image encryption.

Contribution: To accomplish the objective, a set of high-dimensional chaotic maps have been developed across Chapters. In Chapter 3, a novel chaotic map is

constructed using an optimization test function, ensuring enhanced chaotic characteristics such as a wide range of control parameters and increased sensitivity to initial conditions. Chapter 4 explores the coupling of classical chaotic maps such as Logistic map and the Kaplan-Yorke map. The coupling mechanism not only increases the dimensionality but also helps in achieving multiple positive LEs and improves randomness, both essential for cryptographic strength. In Chapter 5, Logistic map and sine function are embedded into the structure of exponential map to create the SHIELD map, which offers richer dynamics and a more uniform distribution. Chapter 6 focuses on extending the existing $e\pi$ -map to develop 2D and 3D chaotic maps. Chapter 7 proposes a Zirili-Logistic map. The Zirili-Logistic map is developed leveraging functions such as sine, exponential, Zirili along with Logistic map. The chaotic dynamics of the proposed maps are analysed in terms of BD, PD, LE, SE and PE. The maps are integrated in an IEA.

2. To develop novel confusion and diffusion operations that reduces the adjacent pixel correlation along with peaks and valleys of the plain image.

Contribution: To achieve this objective, in Chapter 3 we have proposed two novel techniques, “Modified Cyclic Diffusion with Pixel Mixing” and “Cascading Confusion Transformation” to perform pixel-level diffusion and confusion effectively. In addition in Chapter 5, we have introduced “Dynamic Diffusion Operation” and “Two-Step Confusion Operation”, which further enhance the scrambling and intensity alteration of image pixels, thereby strengthening the overall encryption process. The Chapter 7 discusses magic square based-FSM. The matrix is used to shuffle the image pixels thereby reducing statistical information and pixel correlation.

3. To develop a novel key stream generation method and its application in image encryption.

Contribution: To fulfill this objective, we have proposed a novel method for generating initial seeds that serves as the input parameters for chaotic maps used in image encryption. The proposed seed generation method ensures that the initial values are highly sensitive to changes in the raw input, meaning even

a single-bit change leads to entirely different key. This sensitivity not only enhances the randomness and unpredictability of the generated chaotic key streams but also strengthens the encryption map against several attacks.

4. To develop a robust, efficient, and computationally fast IEA that is applicable to real-life problems as well.

Contribution: To accomplish the objective of developing a robust, efficient, and computationally fast IEA applicable to real-life problems, we have proposed six distinct encryption algorithms across Chapters of the thesis. Together, these contributions demonstrate a comprehensive effort toward designing secure, efficient, and practical IEA with strong applicability to various real-world scenarios.

1.4 Organization of the Thesis

The thesis is structured into nine chapters:

Chapter 2 presents introduction of chaotic maps and encryption algorithms along with the literature on existing chaotic maps and IEAs. It outlines the performance measures employed to analyze chaotic dynamics and to evaluate the robustness of IEAs.

Chapter 3 explores the development of a chaotic map utilizing the Zirili optimization function, leveraging its multi-modal and oscillatory characteristics to enhance chaotic behavior. The proposed Zirili map is analyzed for its dynamical properties and integrated into an IEA, employing modified cyclic diffusion with pixel mixing and cascading confusion transformation. Comprehensive evaluations demonstrate its high randomness, strong resistance to differential and statistical attacks, and suitability for secure digital image transmission.

Chapter 4 introduces a Coupled Kaplan-Yorke-Logistic map designed by combining Kaplan-Yorke map and Logistic map. The dynamics of map are thoroughly analyzed using various performance measures, demonstrating its high unpredictability and sensitivity to initial conditions, which are essential for secure encryption. A robust IEA is proposed that leverages the chaotic sequences generated by the map for confusion and diffusion of pixel data. The chapter further presents a comprehensive security analysis confirming the algorithm's effectiveness against several cryptographic attacks.

Chapter 5 presents the design and application of a novel chaotic map, the SHIELD map, for image encryption. The SHIELD map is developed by combining exponential and sine functions along with Logistic map. Subsequently, the chapter introduces SHIELD-IEA, an IEA that employs the SHIELD map along with a two-step confusion process (bit-level and Fisher-Yates shuffling) and dynamic diffusion operations to ensure high randomness, strong diffusion, and resistance against cryptographic attacks. Finally, the chapter describes comprehensive security and performance analysis of SHIELD-IEA, demonstrating its effectiveness in producing robust and secure cipher images.

Chapter 6 presents the development of two novel IEA utilizing modified chaotic maps derived from the 2D $e\pi$ map. The proposed maps, namely the 2D Sine $e\pi$ map and the 3D Non-linear Sine hyper-chaotic map, incorporate transcendental numbers and nonlinear functions to achieve high sensitivity to initial conditions and robust chaotic behavior. Subsequently, the chapter presents the design of IEAs using the modified maps along with the fractal sorting matrix, followed by a comprehensive security analysis, confirming the effectiveness of proposed algorithms.

Chapter 7 presents a novel IEA leveraging Magic Square Matrix–based Fractal Sorting Matrix and Zirili–Logistic map. The chapter describes formulation and detailed analysis of the ZLM using various performance measures. Subsequently, a magic square matrix-based FSM is introduced, highlighting its structural novelty and security advantages over conventional fractal sorting matrices. Leveraging both map and the matrix, a secure IEA is developed. The chapter concludes with a comprehensive security and performance analysis of the proposed IEA using several metrics demonstrating its effectiveness in producing robust cipher images.

Chapter 8 focuses on developing a secure IEA that integrates multiple chaotic maps with a linear feedback shift register to enhance the protection of digital images. The IEA employs two-step permutation and two-step diffusion processes to disrupt the plain image. A comprehensive analysis is presented using several metrics that demonstrate robustness against various attacks.

Chapter 9 concluded the key contributions of the thesis, highlighting the development and analysis of novel chaotic maps and their application to secure image encryp-

8

tion. It presents the main findings, evaluates the effectiveness and robustness of the proposed algorithms, and discusses their potential extensions and real-world applicability. Additionally, the chapter outlines the societal and technological impact of the work, emphasizing how the proposed encryption methods enhance data security and privacy in various digital communication and multimedia applications.

Chapter 2

Preliminaries and Literature Review

This chapter introduces chaotic maps and IEAs, together with a review of the relevant literature. Furthermore, the performance measures to evaluate both IEAs and chaotic maps along with data-set description, are discussed in the chapter. Section 2.1 introduces chaotic maps along with its application in IEA. The relevant literature on chaotic maps and IEA is discussed in Section 2.2. Section 2.3 describes performance measures employed to analyze the chaotic behavior of the maps, and resilience of the IEAs. Finally, Section 2.4 describes image data-set used to analyse the performance of IEA.

2.1 Introduction

Chaos theory describes the behaviour of certain dynamical systems; that is, systems whose state evolves with time may exhibit dynamics that are highly sensitive to the initial conditions. This happens even though these systems are deterministic, meaning that their future dynamics are fully defined by their initial conditions, with no random elements involved. This behaviour is known as Deterministic chaos or simply chaos. Edward Lorenz summarised chaos theory as: “When the present determines the future, but the approximate present does not approximately determine the future”. Chaotic behaviour occurs in many natural systems such as weather, road traffic, the stock markets, our brain states and so on. This behavior can be investigated through computa-

10

tional techniques such as recurrence plots. Chaos theory has applications in several disciplines, including meteorology, environmental science, engineering, cryptography, economics, biology and so on.

Chaotic systems play a crucial role in the study of non-linear dynamics, and complex systems. The definition of chaos given by Robert L. Devaney says that the system is said to be chaotic if the following features are exhibited [29].

1. **Sensitive Dependence on Initial Conditions:** A small difference in the initial conditions leads to drastically different outcomes, making long-term predictions impossible. This is popularly known as the “Butterfly effect” [30]. A consequence of the sensitivity to initial conditions is that if we start with only a finite amount of information about the system, then beyond a certain time, the system is no longer predictable. This phenomenon is most popular in the case of weather, which is generally predictable only for about a week ahead.

Regarding this, the definition for this condition is given as: For simplicity, let f be a continuous function of the closed interval $I \subset \mathbb{R}$ to itself.

Definition 2.1.1. The function $f : I \rightarrow I$ has sensitive dependence on initial conditions at $x \in I$ if there exists $\varepsilon > 0$ such that $\forall \delta > 0$, there exist y and n with $|y - x| < \delta$ but $|f^n y - f^n x| > \varepsilon$ [29].

2. **Topological Mixing:** This means that the system evolves over time so that any given region of its phase space eventually overlaps with any other given region.

The mathematical concept of “mixing” corresponds to the standard intuition, and the colored fluids are an example of a chaotic system. Mathematically, A continuous mapping $f : I \rightarrow I$ is said to be topologically transitive if, for every pair of non-empty open sets $A, B \subset I$, there exists a positive integer n such that $f^n(A) \cap B \neq \emptyset$ where f^n is the n^{th} iterate of f [29].

3. **Dense Periodic Orbits:** In a chaotic system, having dense periodic orbits means that periodic orbits come arbitrarily close to every point in the space. In other words, the system’s points are densely distributed near the periodic orbits.

Mathematically, it is defined as: every point in a chaotic attractor lies arbitrarily close to a point on some periodic orbit. In other words, for any point in the attractor and any positive distance, no matter how small, there exists a periodic orbit within that distance.

A system satisfying above conditions is considered as chaotic [29]. Furthermore, the chaotic systems are divided into two categories depending on their nature. One of them is discrete-time systems termed as map that describes the evolution of a system at discrete time steps using iterative functions. While another is continuous-time systems that describes chaotic systems evolving continuously over time.

Unlike random processes, chaotic systems are ideal candidates for cryptographic applications, especially in securing digital multimedia data such as images [31]. Chaotic systems are leveraged to generate pseudo-random sequences utilizing initial conditions and control parameters. The chaotic sequences are pre-processed to fit the operational requirements of the encryption algorithm i.e., the stages of confusion and diffusion [32]. In the confusion phase, the chaotic sequences are used to scramble the spatial positions of the image pixels. This process, also referred to as permutation or shuffling, significantly alters the structural layout of the image, breaking the inherent spatial correlation among neighboring pixels. By mapping original pixel locations to new positions in a seemingly random manner, the image's visual coherence is destroyed, thereby concealing any discernible patterns. This makes it extremely difficult for an attacker to infer the original image structure without access to the exact permutation sequence derived from the chaotic systems [33]. Following confusion, the diffusion phase introduces randomness by modifying the pixel intensity values. Here, chaotic sequences act as dynamic keys to alter pixel values using operations such as bit-wise XOR, modular addition, or subtraction. The diffusion operation ensures that a minor change in the plaintext or encryption key results in a significantly different ciphertext, making statistical attacks and differential cryptanalysis infeasible [34]. The combination of confusion and diffusion operations driven by chaotic sequences forms a robust and secure IEA.

2.2 Literature review

This section presents a review of the literature on chaotic maps and IEAs. Subsection 2.2.1 focuses on chaotic maps, while Subsection 2.2.2 discusses the literature on IEAs.

2.2.1 Chaotic maps in Literature

A significant research has been done on chaotic maps due to their unique dynamical properties and potential applications in cryptography and secure communications. Early literature primarily focused on 1D chaotic maps such as the Logistic map [15], Tent map [35], Chebyshev map [36], and Sine map [37]. Their mathematical simplicity, ease of implementation, and low computational overhead made them attractive for applying in cryptographic applications. For example, the Logistic map was widely studied as a source of pseudo-random sequences; however, subsequent analyses revealed limitations such as small key space, short periodicity, and non-uniform distribution. To address these issues, researchers explored higher-dimensional chaotic maps, including the Hénon map [38], Baker map [39] and Tinkerbell map [40], as well as continuous-time systems such as the Lorenz [41] and Rössler attractors [42]. These systems help in achieving larger key spaces, more complex trajectories, and richer dynamical behavior, thereby improving cryptographic strength.

Recent research has emphasized hybrid approaches, in which multiple chaotic maps are combined. Such methods aim to overcome non-ideal randomness, improve sequence uniformity, and mitigate dynamical degradation. The research work [43] proposed 2D cosine Logistic map (2D-CLM) by fusing the Cosine map and Logistic map. The research work [44] proposed 2D infinite collapse with Logistic map (2D-ICLM) by combining 1D-ICM and the Logistic map. The phase diagram (PD) of the map exhibits non-uniform output distribution. The research work [45] contrived a 2D Logistic coupling cubic chaotic map (2D-LCCCM) by combining Logistic map and Cubic map. The research work [46] proposed a 2D iterative Gaussian Sine chaotic map (2D-IGSCM) by combining Sine map, Gaussian map and Iterative map with infinite collapses. The map exhibits high Lyapunov exponents (LE) indicating sensitivity to

initial conditions. The research work [47] utilised the Logistic map and Sine map to develop a 2D Logistic-Sine-coupling map that exhibits better ergodicity, more complex behaviour and larger chaotic range. The research work [48] introduced 1D chaotic map by combining Chebyshev map and ICMIC map through the methods of coupling and parameter adjustment. The research work [49] proposed a modified digital chaotic sequence generator leveraging Logistic map with a coupling structure. The results show that the length of chaotic orbits, the output distribution of chaotic map, the security of chaotic sequences and the dynamical degradation of digital chaos have been greatly improved by coupling. The research work [50, 51] combined Sine map and 2D Logistic map into two new compound chaotic systems that exhibit better chaotic and hyper-chaotic properties. The research work [52] proposed the improved coupling quadratic map utilizing the classic quadratic map. The improved map exhibits more intricate non-linear dynamics, an expanded chaotic regime, and superior randomness. The research work [53] proposed a 1D two-parameter mixed coupled map lattice model. The analysis exhibits strong chaotic behavior, high sensitivity, a broad range of parameters, and an extensive chaotic region. The research work [54] proposed compound-coupled Logistic chaotic map by applying compounding coupling technique. The research work [55] proposed a 2D cross Sine²-Logistic chaotic map (2D-SLM) by combining Sine map and Logistic map. The research work [56] proposed a 2D H  non-Sine map (2D-HSM) by combining H  non map and Sine map. The research work [57] introduced 2D sine-cosine coupling chaotic map by combining the Logistic map and the Sine map that exhibits better randomness, ergodicity and wider hyper-chaotic range. The research work [58] proposed a 2D-Logistic-nested-infinite-collapse map (2D-LNIC) by combining 1D-ICM and Logistic map. The research work [59] proposed a hyper-chaotic cross-mode map leveraging the Logistic and Sine maps (2D-CLSS). The research work [60] contrived a 2D Logistic memristive hyper-chaotic map (2D-LMHM) by combining Logistic map with memristor structure. The maps demonstrated limited range of control parameters, and negative LEs at certain parameter values. Additionally, the PD reveals a non-uniform distribution, indicating irregular dynamical behavior.

With growing interest in chaotic maps, researchers have turned to optimization test functions for designing new chaotic maps. The research work [61] used the Schaffer

14

function and proposed a 2D hyper-chaotic map. The Schaffer function is used as an optimization benchmark function to exploit its strict oscillation properties. The research work [62] introduced a 2D Salomon map constructed using the Salomon function. It structurally solves the shortcomings of some traditional maps with small chaotic ranges and few control parameters. The research work [63] developed a 2D map by hybridising the Rastrigin and Griewank functions. Their nature, such as high complexity and fluctuation, makes them suitable for chaotic maps. The research work [64] used the Vincent function to develop a 2D Vincent map. The map involves logarithmic function in addition to Sine and Cosine function that enhance the complexity and diversity of the map. The research work [65] developed a 2D hyper-chaotic map using the Rosenbrock function, which has perfect swinging characteristics in modular form. The research work [66] developed a 2D fully chaotic map through a quadruple-objective optimisation strategy with an artificial bee colony algorithm. An effective model for the fully chaotic map with eight decision variables was empirically constituted. The research work [67] developed an optimal chaotic map. The map is constructed using a multi-objective optimization strategy through the artificial bee colony algorithm. An empirical model for the optimal chaotic map with four variables is first constituted, and then, the variables are optimized using the artificial bee colony for minimizing the multi-objective function composed of the information entropy and LE of the optimal chaotic map.

Apart from hybrid and test optimization function based chaotic maps, another promising direction in the design of maps is the development of memristor-based maps. The unique nonlinear characteristics and memory-dependent behavior of memristors allow them to generate rich chaotic dynamics with high complexity. Several studies have demonstrated the effectiveness of such memristor-based chaotic maps. The research work [68] proposed quadratic oscillatory-ideal memristor (QO-IM) by incorporating an oscillatory term into the discrete memristor model, resulting in diverse dynamics such as bi-stable and coexisting attractors and demonstrates their application in pseudo-random number generators with high randomness. The research work [69] proposed a multi-scroll memristive chaotic system (MMCS) that utilizes memristors with scalable memductances to create hidden grid multi-scroll chaotic attractors. It explores dy-

namical analysis and circuit implementation, demonstrating the system's complexity and feasibility. The research work [70] proposed a coupled memristor hyper-chaotic model (CMHM) leveraging the Logistic map, sine map and discrete memristor model. The CMHM is used to secure the medical images while transmission. The research work [71] proposed a chaotic map termed as discrete neural network models (DNNMs) without a discrete memristor. The map exhibits numerous periodic windows within its parameter region and demonstrates complex dynamics, including point attractors and chaotic attractors. For the purpose of comparison, a number of hybrid maps available in the literature are included in Table 2.1.

Table 2.1: Chaotic maps used for comparison.

Name (Year) Ref.	Chaotic map	Control Parameter
2D-CLM (2024) [43]	$\begin{cases} x_{i+1} = a \cos(x_i(1-x_i^2)) \\ y_{i+1} = a_1 \cos(y_i(1-x_i)) \end{cases}$	$a, a_1 \in (0, \infty)$
2D-ICLM (2024) [44]	$\begin{cases} x_{i+1} = \cos\left(\frac{a}{x_i}\right) \sin\left(1 + \frac{a}{a_1 y_i(1-y_i)}\right) \\ y_{i+1} = \cos\left(\frac{a}{a_1 x_i(1-x_i)}\right) \sin\left(1 + \frac{a}{y_i}\right) \end{cases}$	$a, a_1 \in (0, \infty)$
2D-LMHM (2024) [60]	$\begin{cases} x_{i+1} = \beta \left(2a_2 - \frac{x_i^2}{a_2}\right) + kx_i \sin(y_i) \\ y_{i+1} = k_1 x_i + k_2 y_i \end{cases}$	$\beta = 0.1, \quad k_1 = 1, \\ k_2 = 0.1, \quad a_2 = 100, \\ k \in [-1.32, -0.15] \cup [0.15, 0.26] \cup [0.32, 1.26]$
2D-IGSCM (2024) [46]	$\begin{cases} x_{i+1} = r_1 \sin(e^{x_i^2} + y_i) \\ y_{i+1} = r_2 \sin\left(\frac{y_i}{\sin(\pi x_i)^2}\right) \end{cases}$	$r_1 \in [0, 25], r_2 \in [0, 25]$
2D-SLM (2023) [55]	$\begin{cases} x_{i+1} = \sin^2(p \sin^{-1} \sqrt{y_i}) \\ y_{i+1} = \Gamma x_i(1-x_i) \end{cases}$	$\Gamma = 4, p = [0.5, \infty)$
2D-HSM (2023) [56]	$\begin{cases} x_{i+1} = 0.5(1 - \sin(1 - \omega b_1 x_i^2 - \omega b_2 y_i)) \\ y_{i+1} = \sin(\omega b_2 x_i) \end{cases}$	$\omega = 10, \quad b_1 \in [0, 5], \\ b_2 = 1.57$
2D-LNIC (2022) [58]	$\begin{cases} x_{i+1} = a_1 \sin\left(\frac{a}{y_i}\right) \left(1 - \sin\left(\frac{a}{x_i}\right)\right) \\ y_{i+1} = \sin\left(\frac{a}{a_1 x_i(1-y_i)}\right) \end{cases}$	$a, a_1 \in (0, \infty)$
2D-CLSS map (2022) [59]	$\begin{cases} x_{i+1} = \sin(\pi(cy_i(1-y_i))) \\ y_{i+1} = \sin(\pi(x_i + y_i)) \end{cases}$	$c \in [0, 4]$
2D-LCCCM (2022) [45]	$\begin{cases} x_{i+1} = \cos\left(\pi^2(4\mu x_i(1-x_i) + p_1 y_i(1-y_i^2)) + \frac{\pi}{2}\right) \\ y_{i+1} = \cos\left(\pi^2(4\mu y_i(1-y_i) + p_1 x_i(1-x_i^2)) + \frac{\pi}{2}\right) \end{cases}$	$\mu \in (0, 4), p_1 = 8.78$

2.2.2 Image encryption algorithm in literature

The evolution of image encryption reflects a continuous effort to strengthen security, beginning with chaos-driven techniques and expanding toward modern encryption frameworks. Matthews [72] first applied chaotic map for encryption in 1989, proposing them as an alternative to the one-time pad system. A significant advancement

16

was made by Fridrich [39, 73], who proposed the permutation–diffusion framework 2D chaotic maps such as the Baker and Cat maps. This framework became a foundational paradigm, inspiring subsequent studies that extended the approach with higher-dimensional chaotic maps and more sophisticated diffusion methods [74, 75].

Several researchers later integrated chaotic maps with other cryptographic tools to enhance the performance of IEAs. The research work [76] proposed encrypting plain images using chaotic maps, cellular automata, and SHA-256. SHA-256 is used to obtain the hexadecimal numbers from the image used to generate the initial values for the chaotic maps. The sequences generated from these maps are used in the diffusion and confusion processes. The research work [77] proposed an IEA utilising Sine map and Tent map with Hill cipher. Incorporating the Sine function reduces the iteration time needed for a chaotic map. This turbulent IEA exhibits remarkable speed and efficiency in terms of security and intricacy. As the iteration time lengthens, the time complexity of the IEA also escalates.

There are several research works utilizing DNA coding rules into image encryption, leveraging their parallelism and vast representation capacity to enhance security and complexity. The research work [78] proposed an IEA for color images, leveraging DNA dynamic encoding and self-adapting permutation. First, a 4D hyper-chaotic system is designed, demonstrating strong pseudo-randomness and a wide range of chaotic parameters. This system creates dynamic DNA encoding, calculation, and decoding, with hyper-chaotic sequences controlling the coding rules for added unpredictability. Additionally, a plaintext-dependent key-stream and self-adapting permutation are proposed at the bit and DNA levels of the image, respectively, enhancing the algorithm's sensitivity to the image and key. Theoretical analysis and simulations confirm the algorithm's strong security against various attacks. In the research work [79], the authors proposed an IEA combining MD5, Logistic map, piece-wise linear chaotic map, and DNA encoding. In the research work [80], an IEA utilizing 2D Logistic-adjusted-Sine mapping and the Logistic-Sine map in combination with random DNA coding is proposed. The research work [81] presents the IEA for medical images using Arnold's cat map and DNA cryptography. These hybrid schemes enhance key sensitivity and resistance to attacks, but their reliance on hashing and DNA operations increases com-

putational complexity, making real-time implementation challenging.

Another stream of research focused on constructing novel permutation and diffusion operations to overcome the limitations of classical systems. In the research work [82], an IEA leveraging the FSM in combination with the Chen system is proposed. The matrix is employed to introduce confusion into the image's pixels, while the sequence derived from the Chen system is applied to perform pixel diffusion using the global chaotic diffusion method. In the research work, an IEA [83] is proposed that utilises a random Hamiltonian path and modified Bernoulli map to manipulate pixel values of a plain image. The random Hamiltonian path is employed to obfuscate the pixel values, while the adjusted Bernoulli map is utilized to disperse the original image's pixels. At first, the authors break down the image into its individual bit planes, subsequently applying the random Hamiltonian path to each of them. Finally, the authors combine processed bit planes to generate an image with distorted pixel values. In the research work [33], an IEA was introduced utilizing 2D- $e\pi$ map (2D-EPM) combined with a bit-reversion operation. First, the plain image pixels are permuted using a sequence generated by the map. In the diffusion stage, sequences are modified through bit-reversion and then XOR-ed with the shuffled image. The research work in [84] presented an IEA employing multiple bit-permutation and diffusion operations, where chaotic sequences from a 4D hyper-chaotic map were used to disrupt the plain image. In the research work [85], an IEA was proposed utilizing the Z-scan method with an improved diffusion scheme, in which sequences are generated using a chaotic map derived from coupled map lattices. Similarly, the research work [86] proposed an IEA that leverages permutation and random multi-directional diffusion, with sequences obtained from the Cosine-Logistic-Sine map. The research work in [87] introduced an IEA built on a simultaneous permutation-diffusion framework. It incorporates a modified Josephus traversal with dynamic scrambling, where the scrambling of each pixel depends on the previously diffused pixel. Here, diffusion is embedded within the modified Josephus traversal, and all operations are driven by sequences generated from the map.

The research work [88] proposed an IEA utilizing dynamic scrambling method and a dynamic diffusion mechanism. It used chaotic sequences generated by generalized

Hamiltonian system. The system's initial values are controlled by both external and internal key streams, ensuring that cipher generation is tightly linked to a plain image, parts of the cipher image, pseudo-random sequences, and the key stream, enhancing resistance to plaintext and related attacks. The research work [89] proposed an IEA for color images. It used a plane element rearrangement and a dynamic selection row-column cross-scrambling to efficiently mix each color plane. Additionally, a cross-plane diffusion method ensures that any change in one element affects the entire image, making it more secure.

Optimization-based approaches have also been explored to improve the key generation process. The research work [90] presents an IEA utilizing key optimisation using a particle swarm optimisation algorithm and a novel modular integrated Logistic exponential map. The research work [91] proposed an IEA utilizing a conservative hyper-chaotic system and biological gene algorithms. SHA-512 computes the hash of plain image, and a key generation algorithm generates the initial keys for the hyper-chaotic system. The IEA utilized dynamic coding rules, dynamic gene uniform crossover algorithm and dynamic gene mutation algorithm to disrupt the plain images.

The research work [92] proposed an IEA that used an intertwining Logistic map and Brownian motion to disrupt the pixels of the plain image. At first, the plain image was masked with random data for a complex cipher image. In the research work [93], an IEA utilising substitution-permutation network is proposed. The sequences generated by fractal-order 1D chaotic map are utilized for encryption purposes. In the research work [94], the authors designed an improved cross-coupled map lattice. The improved map integrates a Tent map alongside modulation operations. It serves a pivotal role in the bit-level encryption process, boasting resilience against common attacks. In the research work [95], an IEA utilizing the 2D-SCMCI hyper-chaotic map is proposed. The IEA first performs scrambling operations along both rows and columns, ensuring thorough permutation of pixel positions. Subsequently, forward and backward diffusion techniques are applied to spread pixel values across the image, achieving high sensitivity to initial conditions and plaintext changes.

2.3 Performance measures

This section outlines the metrics employed to evaluate both the chaotic behavior and the resilience of IEA. The metrics used to analyze the chaotic map are described in Subsection 2.3.1, whereas those for assessing the IEA are presented in Subsection 2.3.2.

2.3.1 Performance measures for chaotic map

Dynamical analysis of chaotic maps is essential to understand their complexity, sensitivity, and unpredictable behaviour. Despite appearing random, chaotic maps follow deterministic rules, making analysis crucial for identifying underlying patterns. This understanding helps in predicting long-term behaviour and preventing undesirable outcomes in fields like cryptography. It also aids in distinguishing true chaos from noise and enables the design of maps resilient to instability. For this, several tests are used to analyse and characterize the chaotic maps. We have described a few of them here that are utilized to confirm the existence of chaotic behaviour.

Bifurcation diagram (BD)

A BD is a visual representation that shows how the long-term behaviour of a dynamical map changes as the control parameter is varied [30]. It plots the possible steady-state values (or attractors) of a map against a changing control parameter. As the parameter changes, the map can undergo bifurcations, where a single stable outcome splits into multiple outcomes, indicating transitions from periodicity to chaos. In particular, whenever a map transitions from a stable state to oscillations of increasing complexity, it can lead to chaotic behaviour, characterised by an aperiodic, sensitive dependence on initial conditions. The presence of a dense, fractal-like structure in certain regions of the BD is a hallmark of chaos, confirming its existence in the map.

Phase diagram (PD)

A PD is a graphical representation of a dynamical map's behaviour by plotting its state variables against each other, often showing how the map evolves over time in a multi-

20

dimensional space called phase space [30]. Each point in this space represents a possible state of the map, and its trajectory shows how the state changes. PD help identify patterns such as fixed points, limit cycles, or strange attractors. The presence of chaos in a PD is established when map trajectories exhibit aperiodic behavior, demonstrate high sensitivity to initial conditions, and evolve toward a strange attractors. This complex yet deterministic behaviour, where nearby trajectories diverge over time, visually demonstrates the hallmark characteristics of chaotic maps.

Lyapunov exponent (LE)

The LE is a significant metric used to analyse the chaotic dynamics of a map by quantifying the exponential divergence between two infinitesimally close trajectories as a function of change in the control parameter [30]. The LE of a chaotic map can be calculated using (2.3.1).

$$LE = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (2.3.1)$$

Where n is the maximum number of iterations, and $f'(x_i)$ is the first derivative of the chaotic map at point x_i . If the LE of the 1D chaotic map is greater than zero, the map is said to be chaotic. If a multi-dimensional map has multiple positive LEs, then the map is said to be hyper-chaotic.

Permutation entropy (PE)

PE is a nonlinear measure of complexity that quantifies the degree of disorder in a time series by analyzing the relative order of neighboring values rather than their exact magnitudes [96]. The process involves partitioning the sequences into subsequences of a chosen dimension n and delay τ , determining the permutation patterns (ordinal relations) within each subsequence, and estimating the probability distribution p_ζ of these patterns. The PE is defined as given in (2.3.2).

$$PE(n) = - \sum_{\zeta=1}^{n!} p_\zeta \log_2(p_\zeta) \quad (2.3.2)$$

where the sum runs over all $n!$ permutations ζ of order n . p_ζ shows the probability

of the occurrence of the permutation ζ . When the PE value of the data approaches 1, it exhibits chaotic behaviour.

Sample entropy

SE^1 is a measure of entropy employed to assess the intricacy of time series data. It quantitatively defines the complexity within a data. A series with higher SE implies lower regularity and, thus, higher randomness of the dynamic map. If the SE value is positive, the generated sequences are chaotic and do not follow any regular order or have a pattern that has not been seen before [97]. Let $X = \{x_1, x_2, \dots, x_n\}$ and $X_m(i) = \{x_i, x_{i+1}, \dots, x_{m-1+i}\}$ with dimension m . The SE can be calculated using

$$SE(m, r, n) = -\log \frac{A}{B} \quad (2.3.3)$$

where A and B are the number of vectors satisfying $d(x_{m+1}(i), x_{m+1}(j)) < r$ ($i \neq j$, d -Chebyshev distance) and $d(x_m(i), x_m(j)) < r$ respectively.

2.3.2 Performance measures for image encryption algorithm

To evaluate the robustness of IEA against various attack, several performance measures have been employed, including NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity), correlation analysis, entropy analysis, and histogram analysis. These measures are discussed in detail in the subsequent subsections.

Information Entropy Analysis

Information entropy is a key metric used to analyse the randomness of data [98]. A higher entropy value means greater uncertainty in predicting pixel values, which in turn indicates stronger resistance against statistical attacks. For a perfectly encrypted 8-bit image, the ideal entropy value is close to 8. The formula used to compute information entropy is given in (2.3.4).

$$H(S) = -\sum_{i=0}^{L-1} p_i \log_2 p_i \quad (2.3.4)$$

¹https://cschoel.github.io/nolds/_modules/nolds/measures.html#sampen

22

where p_i denotes the probability of the occurrence of intensity level i in the image and L is the maximum gray-scale level. S is the set which includes the numbers from $i = 0$ to $i = L$.

Histogram Analysis

The histogram of an image is a tool for analysing the distribution of pixel values. For a plain image, certain pixel values occur much more frequently than others. This creates peaks and valleys in the histogram. In case of cipher image, every pixel value should appear with roughly equal probability, so the histogram looks uniform. Its uniform distribution indicates the robust IEA and a high level of security against potential statistical attacks [99].

Adjacent Pixel-Correlation Analysis

The correlation between adjacent pixels in an image is analyzed to characterize their inter-dependency [100]. The plain images exhibit a high degree of pixel correlation, whereas the cipher images show significantly reduced pixel correlation. A lower adjacent-pixel correlation in cipher images suggests that the IEA's is resistant to statistical attacks. The correlation coefficient is defined as in (2.3.5).

$$\rho(x,y) = \frac{cov(x,y)}{\sigma_x \sigma_y} \quad (2.3.5)$$

Where $cov(x,y)$ is the covariance between x , and y . σ_x and σ_y is the standard deviation of x and y , respectively. The value of the correlation coefficient lies in the $[-1,1]$. A value closer to zero indicates no correlation, while a value closer to one shows a high correlation. In this thesis, the correlation coefficient of adjacent pixels is analyzed in three directions: horizontal (HD), vertical (VD), and diagonal (DD). For this analysis, 10,000 random pixels are selected from both the plain and cipher images, together with their corresponding neighboring pixels. The computed correlation values are presented and the pixel distributions are illustrated through graphical representations.

Occlusion attack

In any communication channel, data loss is a potential risk, which may arise from network-related issues, such as congestion or transmission errors, or from adversarial actions. The encryption and decryption algorithms must be designed to allow for partial recovery of the encrypted image, even in cases where complete data cannot be recovered. An occlusion attack, for instance, can result in a significant loss of the encrypted image during transmission [101]. The developed IEA must have potential to restore a significant portion in the decrypted image so that image content can be identified. In this thesis, a small portion of the cipher image is removed and then the image is decrypted. If the content of the image is visible, it can be concluded that the IEA is resistant to occlusion attack.

Noise attack

In the real world, information transmission is inevitably affected by noise [102]. Therefore, IEA should be able to restore cipher images that are contaminated by noise. The IEA should be capable of reconstructing noisy portion of the decrypted image, ensuring that the image content remains recognizable. In this thesis, the cipher image is corrupted with salt-and-pepper noise prior to decryption. If the decrypted image still reveals identifiable content, it can be inferred that the IEA demonstrates resistance to noise attacks.

Differential Attack

A differential attack is a cryptanalysis technique that studies how variations in the input influence the resulting changes in the output. Instead of directly analyzing the absolute values of plaintexts and ciphertexts, it focuses on how small, controlled modifications in the plaintext propagate through the encryption process and impact the ciphertext. By observing differences across multiple encryptions, attackers can exploit statistical biases or predictable behaviors in the algorithm to recover secret key more efficiently than brute-force methods.

To thwart such attacks, a robust IEA must ensure that even a one-bit change in the plain image produces an entirely different cipher image [103]. The resistance of an IEA

24

against differential attacks is typically evaluated using Number of Pixel Change Rate (*NPCR*) Unified Averaged Changed Intensity (*UACI*). These metrics are calculated using the mathematical expressions defined in (2.3.6) and (2.3.7).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (2.3.6)$$

Where,

$$D(i,j) = \begin{cases} 1, & \text{if } R_1(i,j) \neq R_2(i,j); \\ 0, & \text{if } R_1(i,j) = R_2(i,j); \end{cases}$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|R_1(i,j) - R_2(i,j)|}{255} \right] \times 100\% \quad (2.3.7)$$

R_1 is the encrypted image of the plain image, and R_2 is the encrypted image obtained from the modified plain image. For an encrypted image, the *NPCR* has an ideal value of 99.6094%, and the *UACI* has an ideal value of 33.4635%.

Resistance to Classic Attacks

Encryption algorithms are traditionally subjected to four primary categories of cryptanalytic threats: ciphertext-only attacks, known-plaintext attacks, chosen-plaintext attacks, and chosen-ciphertext attacks [104]. Each of these methods exploits different levels of information available to the adversary. Among them, chosen-plaintext attacks are regarded as the most prevalent in practical cryptanalysis, since they allow the attacker to deliberately select specific plaintexts and observe the corresponding ciphertexts [105]. This capability provides valuable insight into the structure of the encryption algorithm, making it a powerful tool for evaluating algorithmic weaknesses.

However, prior research has demonstrated that an IEA can withstand such chosen-plaintext attacks [106, 107], as long as the fundamental security requirement expressed in condition (2.3.8) is satisfied.

$$P_1(i,j) \oplus P_2(i,j) \neq C_1(i,j) \oplus C_2(i,j) \quad (2.3.8)$$

where P_1 and P_2 refer to the two original unaltered images, while C_1 and C_2 represent

their respective encrypted images. This condition ensures that the encryption algorithm retains sufficient randomness and complexity to prevent an adversary from deducing meaningful patterns.

NIST Randomness test

The NIST test suite (developed by the National Institute of Standards and Technology) is set of statistical tests to evaluate the randomness of binary sequences, especially in the context of cryptographic applications [108]. It helps in determining the randomness of encrypted image. Each test utilises a p -value obtained at a significance level $\beta = 0.01$. The random sequence is considered to pass a given randomness test if the obtained p -value is greater than β .

Execution time analysis

The running time of the IEA plays a crucial role in determining its suitability for real-world applications. The IEA has to be highly effective in keeping up with images' rapidly increasing data capacity. For this purpose, the IEA was repeated 50 times, and the mean execution time was recorded.

2.4 Data-set description

The images selected from the USC-SIPI Image Database² consist of high-quality gray-scale images. They include textures, aerial photographs, and miscellaneous scenes, with diverse resolutions. These images were chosen to represent diverse visual content, including natural textures, man-made structures, and complex patterns, making them suitable for evaluating image processing techniques.

To analyse the security and efficiency of IEA, a series of experiments on diverse images is performed. Additionally, the effectiveness and resilience of the proposed IEAs are compared with algorithms in terms of various key metrics. The IEA was implemented on a computer running Windows 11, equipped with a 2.60 GHz CPU and 8 GB of RAM. The numerical simulations were performed using Python 3.10.

²<https://sipi.usc.edu/database/database.php>

Chapter 3

Zirili map with application in Image Encryption

This chapter addresses the growing need for secure and efficient cryptographic algorithm by exploring test optimization function based chaotic map and its applications in IEA. The development of chaotic maps leveraging optimization functions has emerged as a significant area of research, particularly in the domain of IEAs. Optimization test functions have been increasingly adapted to design novel maps with enhanced chaotic properties. These maps leverage the intricate mathematical structures of optimization functions, such as high non-linearity, multi-modality, and oscillatory behavior. There are several chaotic maps [61, 62, 63, 64, 65, 66, 67] available in literature leveraging optimization functions such as the Schaffer, Salomon, Rastrigin, Griewank, Vincent, and Rosenbrock functions. These maps address limitations in traditional maps, such as limited chaotic ranges, periodic windows, and insufficient control parameters, by introducing high complexity and unpredictability suitable for secure encryption. Section 3.1 discusses the background of Zirili function. Sections 3.2 present the proposed 2D Zirili map (ZM). The analysis of ZM is discussed in Section 3.3 utilising BD, PD, LE, PE, and SE. Section 3.4 introduces the encryption algorithm utilising the proposed ZM termed as ZM-IEA. The ZM-IEA leverages chaotic sequences generated by the

ZM along with modified cyclic diffusion with pixel mixing (MCDPM) and cascading confusion transformation (CCT) to disrupt plain image. Section 3.5 discusses the analysis of the ZM-IEA utilizing several metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 3.6 summarizes the chapter.

3.1 Background

The Zirili test optimization function [109] is important due to its unique mathematical structure. It is continuous, differentiable, and multi-modal, making it highly suitable for benchmarking optimization algorithms as well as for constructing novel chaotic maps. The function is defined in (3.1.1).

$$f(x, y) = 0.5x^2 + 0.5(1 - \cos(2x)) + y^2 \quad (3.1.1)$$

where $x, y \in (-500, 500)$. The function has a global minimum $f(x, y) = 0$ at $(x, y) = (0, 0)$ including several local minima. The quadratic terms ensure convexity in both the x and y directions, while the oscillatory cosine component introduces periodic fluctuations, creating multiple local minima along the x -axis. To better understand its behavior, the function can be visualized using a 3D surface plot shown in Figure 3.1. The resulting surface reveals a parabolic bowl-like structure influenced by oscillatory ripples along the x -direction. The parabolic growth of the quadratic terms ensures that function values increase rapidly as one moves away from the origin, while the cosine component introduces alternating ridges and valleys. This interplay between global convexity and local fluctuations explains the presence of both a clear global minimum and several deceptive local minima.

By leveraging the oscillatory and non-linear nature of the Zirili function, we have constructed chaotic map with enhanced properties. The periodicity and multi-modality introduce unpredictability, while the quadratic growth ensures sensitivity to parameter variations. Together, these features contribute to stronger chaotic behavior, which is essential in designing secure IEA.

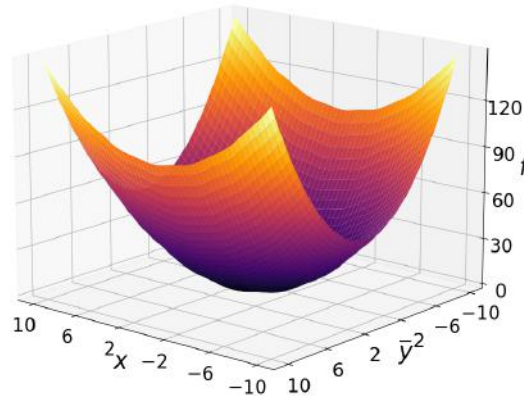


Figure 3.1: 3D representation of Zirili function.

3.2 Proposed Zirili map

The ZM is 2D discrete map involving two variables x and y and a pair of control parameters (p, q) . The map involves a Cosine function that oscillates between -1 and 1. A modular operation ensures the map's outputs fall within the $(0, 1)$ range. The map is given in (3.2.1).

$$\begin{aligned} x_{i+1} &= \text{mod} \left(2^p x_i^2 + 2^q (1 - \cos(p(\frac{\pi}{2} + q\pi x_i))) + 2^q y_i^2, 1 \right) \\ y_{i+1} &= \text{mod} \left(2^q x_i^2 + 2^p (1 - \cos(q(\frac{\pi}{2} + p\pi y_i))) + 2^p y_i^2, 1 \right) \end{aligned} \quad (3.2.1)$$

where p and q are control parameters in the range $(0, \infty)$. x_{i+1} and y_{i+1} denote the future states of the states x_i and y_i , respectively. Including coefficients 2^p and 2^q assures oscillatory motion and precludes the possibility of decay or settlement. For experiment purposes, we have utilized the values of control parameters p and q in the range $[0, 10]$.

3.3 Analysis of the Zirili map

The chaotic behavior of the ZM is comprehensively investigated by employing a range of tools, including BD to visualize the transition between periodic and chaotic regimes, PD to depict the map's state space trajectories, LE to quantify the rate of

30

divergence of nearby trajectories and confirm chaotic dynamics, PE to measure the complexity of time series based on ordinal patterns, and SE to assess the irregularity and unpredictability of the map's temporal evolution. These tests are performed and the results are discussed in the subsequent sections.

3.3.1 Bifurcation diagram

The BD of ZM is exhibited in Figure 3.2. The plots involve control parameter p and q , versus variables x and y . The values of the control parameter is set in the range $[0,10]$. The diagrams are plotted using the initial conditions $x_0 = 0.5$ and $y_0 = 0.3$. These diagrams reveal that the ZM exhibits significant ergodicity across a broad range of control parameter values. Furthermore, the BD highlight sensitivity of the ZM to variations in control parameters. Even small changes in p or q result in sensitive dynamic behaviors. This high sensitivity and complex dynamical behavior make the ZM particularly well-suited for integration into IEAs.

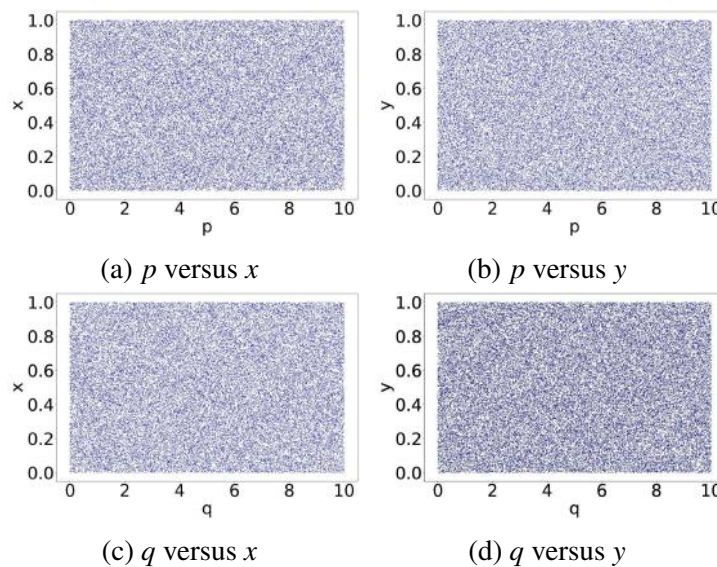


Figure 3.2: Bifurcation diagrams of Zirili map.

3.3.2 Phase diagram

The PD of ZM and other maps, as listed in Table 2.1, are exhibited in Figure 3.3. The PD are plotted using the values as ZM $((x_0, y_0, p, q) = (0.5, 0.3, 7.13, 5.38))$, CLM

$((x_0, y_0, a, a_1) = (0.5, 0.8, 5, 5))$, ICLM $((x_0, y_0, a, a_1) = (0.3, 0.1, 0.1, 0.1))$, LMHM $((x_0, y_0, \beta, k_1, k_2, \rho_1, k) = (0.5, 0.8, 0.1, 1, 0.1, 100, 0.7))$, IGSCM $((x_0, y_0, r_1, r_2) = (0.21, 0.31, 25, 23.3))$, SLM $((x_0, y_0, \Gamma, p) = (0.3, 0.4, 4, 3.6))$, HSM $((x_0, y_0, b_1, b_2, \omega) = (0.3, 0.6, 5, 1.57, 10))$, LNIC $((x_0, y_0, a, a_1) = (0.9, 0.6, 1, 1))$, CLSS map $((x_0, y_0, c) = (0.3, 0.6, 0.5))$, LCCCM $((x_0, y_0, \mu, p_1) = (0.6, 0.9, 5, 8.78))$. From the Figure 3.3, it can be inferred that the ZM's PD demonstrates a uniform distribution throughout the phase space. This indicates that the state trajectories of the ZM do not concentrate in specific regions but are instead evenly dispersed across the entire region. In contrast, the PD of other maps display non-uniform distributions. This observation suggests that the proposed map offers enhanced resistance to phase space reconstruction attacks.

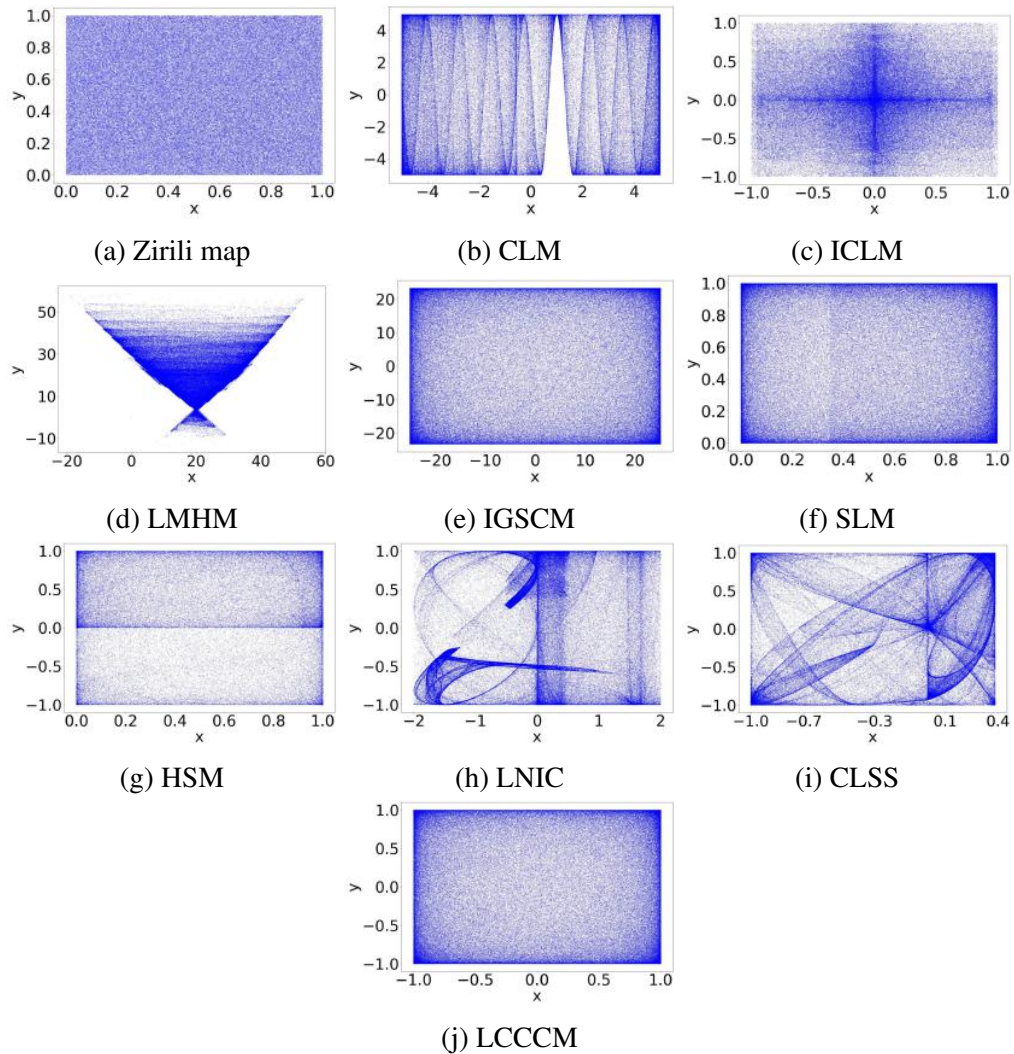


Figure 3.3: Phase diagrams (x and y).

3.3.3 Lyapunov exponent

The LE of ZM and other existing maps, as listed in Table 2.1, are exhibited in Figure 3.4. LE_x and LE_y represent the LEs associated with the x and y variables, respectively. From the Figure 3.4, it is visible that the LE of ZM are positive and high as compared to other maps except IGSCM. Some maps shown in Figure 3.4 have negative LEs also. The LEs of ZM are high and positive as well. Since the LEs are positive for both the variable, the ZM is a hyper-chaotic map. Thus it can be concluded that the ZM is extremely sensitive to initial conditions. The larger the LE, the faster this divergence happens. Thus ZM is chaotic, complex, unpredictable and hence suitable for integration into IEAs.

3.3.4 Permutation entropy

Figure 3.5 illustrates the PE of the ZM alongside other existing chaotic maps listed in Table 2.1. As shown in the Figure 3.5, the ZM consistently exhibits values near 1 across the specified range of control parameters. This suggests that the ZM demonstrates highly complex or chaotic behavior, making it a strong candidate for applications requiring randomness or unpredictability, such as cryptography or secure communications.

3.3.5 Sample entropy

Figure 3.6 shows the SE of the ZM compared to other chaotic maps listed in Table 2.1. As shown in Figure 3.6, the ZM consistently achieves high values of SE around 2.5 across the evaluated range of control parameters, suggesting that the ZM exhibits pronounced chaotic behavior. Thus it can be concluded that ZM is a strong candidate for applications requiring high unpredictability, including cryptography and secure communications.

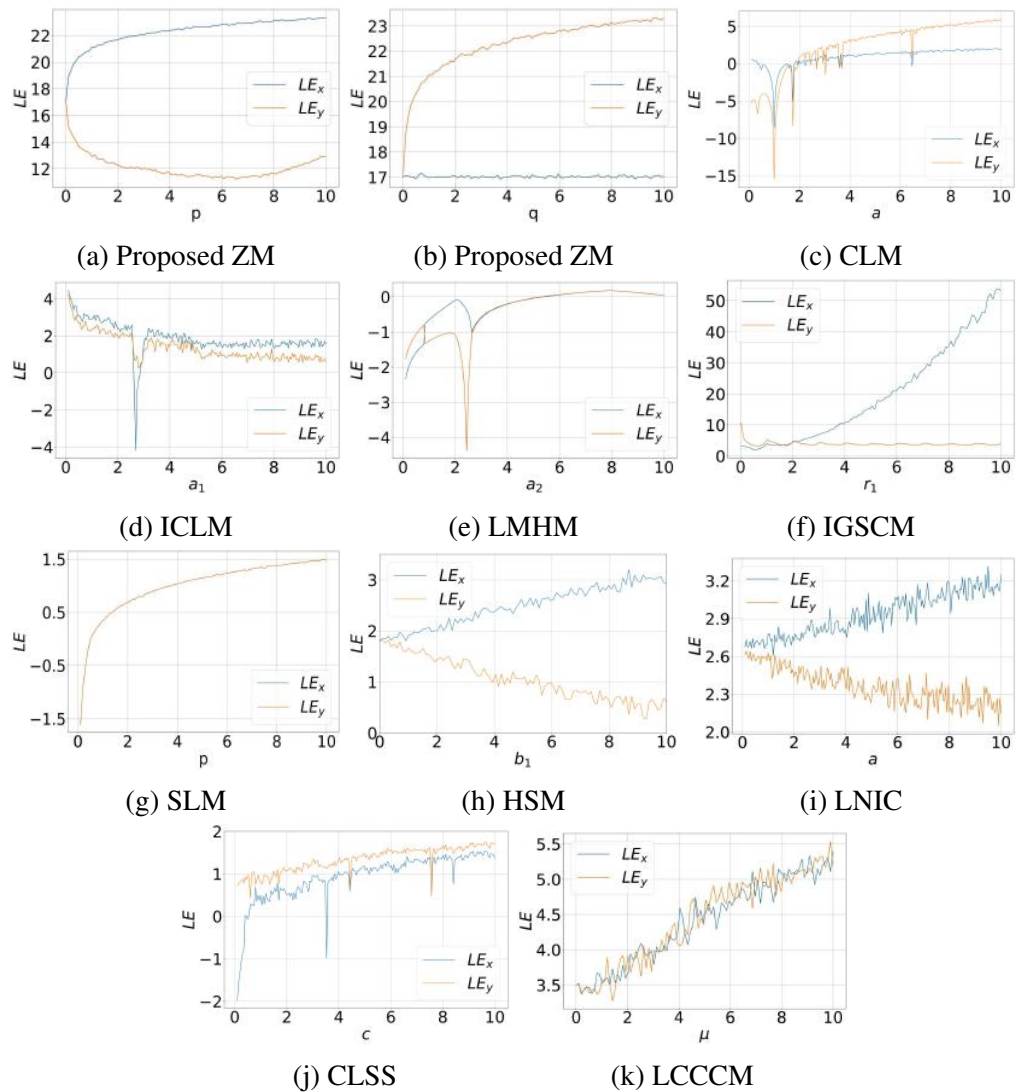


Figure 3.4: Lyapunov exponent diagram of Zirili and others maps.

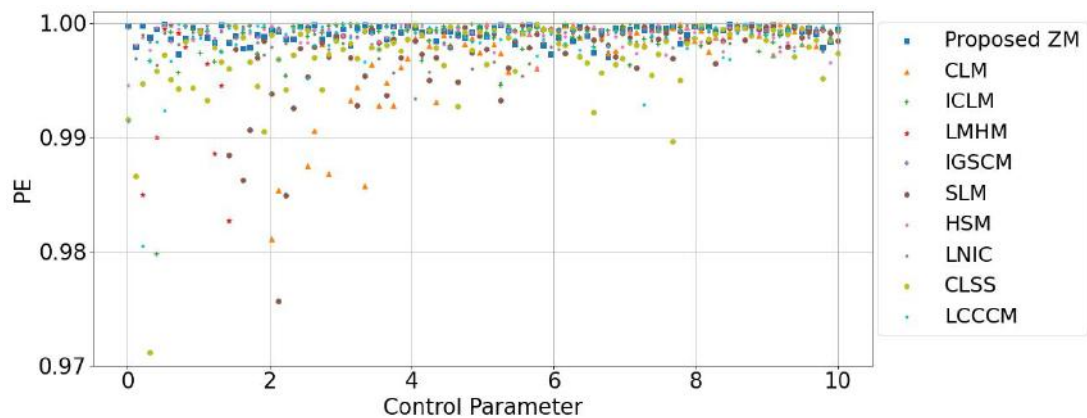


Figure 3.5: Permutation entropy of Zirili map.

34

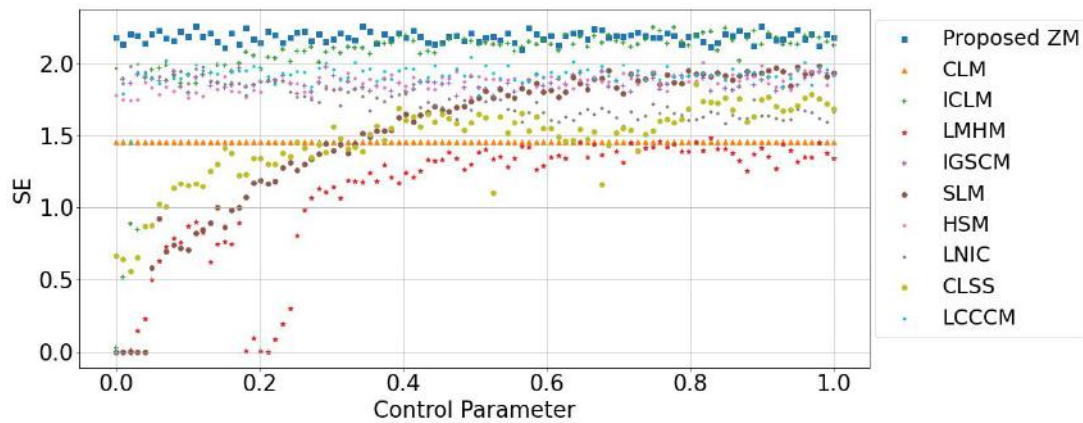


Figure 3.6: Sample entropy of Zirili map.

3.4 Application of map in image encryption

This section delves into the development of IEA. The algorithm is termed as ZM-IEA. The ZM-IEA involves generation of sequences utilizing ZM, MCDPM and CCT. The steps of ZM-IEA are displayed in Figure 3.7. Further, the formation of sequences, diffusion and confusion operations are described in section 3.4.1, 3.4.2 and 3.4.3, respectively.

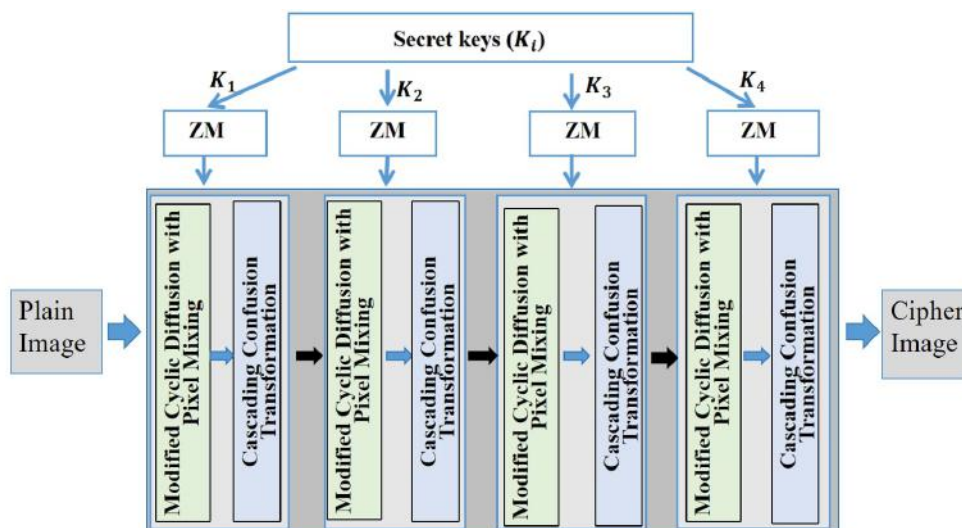


Figure 3.7: Image encryption algorithm leveraging Zirili Map.

3.4.1 Obtaining secret key and chaotic sequence

The secret key is an essential component of a cryptosystem, which ensures that messages may only be encrypted and decrypted using a particular key. If the key size is less than 2^{100} , the key can be obtained using a brute-force attack. So, to thwart such threats, the key space must have a size greater than 2^{100} [110]. In this study, we have used a key K consisting of 64 hexadecimal numbers equivalent to 256-bits. Hence, the size of key space is 2^{256} , enough to prevent brute-force attacks.

The hexadecimal key is divided into eight parts, and the corresponding integer is stored as $\{I_i : 1 \leq i \leq 8\}$ using (3.4.1):

$$I_i = \text{hexodec}(K_{8(i-1)+1:8i}), \quad 1 \leq i \leq 8 \quad (3.4.1)$$

where, $\text{hexodec}(\bullet)$ is the function to convert hexadecimal numbers into decimal numbers. The values of I_i are modified using (3.4.2) and used to generate the ZM's initial values and control parameters.

$$\begin{cases} x_0 = \frac{1}{e} \left(\frac{I_1}{10^9} + \sin \left(\frac{\pi}{2} I_j \right) \right) \bmod 1 \\ y_0 = \frac{1}{e} \left(\frac{I_2}{10^9} + \sin \left(\frac{\pi}{2} I_j \right) \right) \bmod 1 \\ p = \frac{1}{e} \left(\frac{I_3}{10^9} + \sin \left(\frac{\pi}{2} I_j \right) \right) \bmod 10 \\ q = \frac{1}{e} \left(\frac{I_4}{10^9} + \sin \left(\frac{\pi}{2} I_j \right) \right) \bmod 10 \end{cases} \quad \text{for } j = 5, 6, 7, 8 \quad (3.4.2)$$

The initial values and control parameters obtained for $j = 5$ are stored as $K_1 = \{x_0, y_0, p, q\}$. Similarly, for other values of j , the initial seeds are calculated and stored as $\{K_k, k = 1, 2, 3, 4\}$. Each K_k is used to iterate the ZM for $(M + M \times N)$ times. To eliminate the transitory impact, the first M values are removed. The obtained sequences x and y are modified and used in ZM-IEA. The chaotic sequence of size $M \times N$ is used in the further steps of the ZM-IEA, i.e., to disturb pixel placements and change pixel values.

3.4.2 Modified Cyclic Diffusion with Pixel Mixing

The pixel values provide vital information about the image, and attackers may retrieve the image by analysing statistical features, even if the locations of the pixels are completely modified. To avoid this, a robust method for modification of the pixel values is required. In order to apply the diffusion process, firstly a matrix V of the size of $M \times N$ is obtained using chaotic sequence y (3.4.3).

$$V = \lfloor y_i \times 10^{10} \rfloor, 0 \leq i \leq (M \times N) - 1 \quad (3.4.3)$$

where $\lfloor \bullet \rfloor$ represents the floor operation, the array V is reshaped into a matrix of size $M \times N$.

The MCDPM ensures information's security and robustness of IEA. The plain image is divided into four blocks, and then MCDPM is applied to enhance the randomness in the cipher images. The method introduces localised diffusion by dividing the image into blocks, which helps in achieving high randomness and unpredictability. The use of neighbouring pixel values, both horizontally and vertically, in the diffusion process increases the dependency between adjacent pixels, making the relationship between the plain image and the encrypted image more complex and resistant to several attacks. The multi-dimensional relationships in the Algorithm 3.1 help quickly propagate small changes in the plain-text throughout the encrypted image, ensuring high sensitivity to initial conditions. The method leverages multiple dependencies between neighbouring pixels and chaotic values that improve the unpredictability, making it resistant to common cryptographic attacks such as statistical, differential and brute-force attacks. We have applied the $\text{mod}(\bullet, 256)$ operation to keep the resultant pixel values in range $[0, 255]$. The proposed MCDPM can be applied to the blocks, leveraging parallel computing to save time for high-resolution images. A bit of modification in the value of a single pixel results in a significant adjustment in the pixel values of the whole image.

Figure 3.8 illustrates the use of MCDPM, using the matrix of size (8×8) . The MCDPM is described in (3.4.4).

$$C_{i,j} = \begin{cases} (P_{i,j} + V_{i,j} + P_{i+1,j} + P_{i,j+1}) \bmod 256, & i = 0, j = 0; \\ (P_{i,j} + C_{i,j-1} + V_{i,j}) \bmod 256, & i = 0, 0 < j < BN; \\ (P_{i,j} + C_{i-1,j} + V_{i,j}) \bmod 256, & 0 < i < BM, j = 0; \\ (P_{i,j} + C_{i,j-1} + C_{i-1,j} + V_{i,j}) \bmod 256, & 0 < i < BM, 0 < j < BN, i \neq j; \\ (P_{i,j} + C_{i-1,j-1} + V_{i,j}) \bmod 256, & 0 < i < BM, 0 < j < BN, i = j. \end{cases} \quad (3.4.4)$$

Where BM and BN represent the height and width of the block of the plain image P , respectively. V represents chaotic matrix block of size $(BM \times BN)$. C is a block of the diffused array obtained after the MCDPM process.

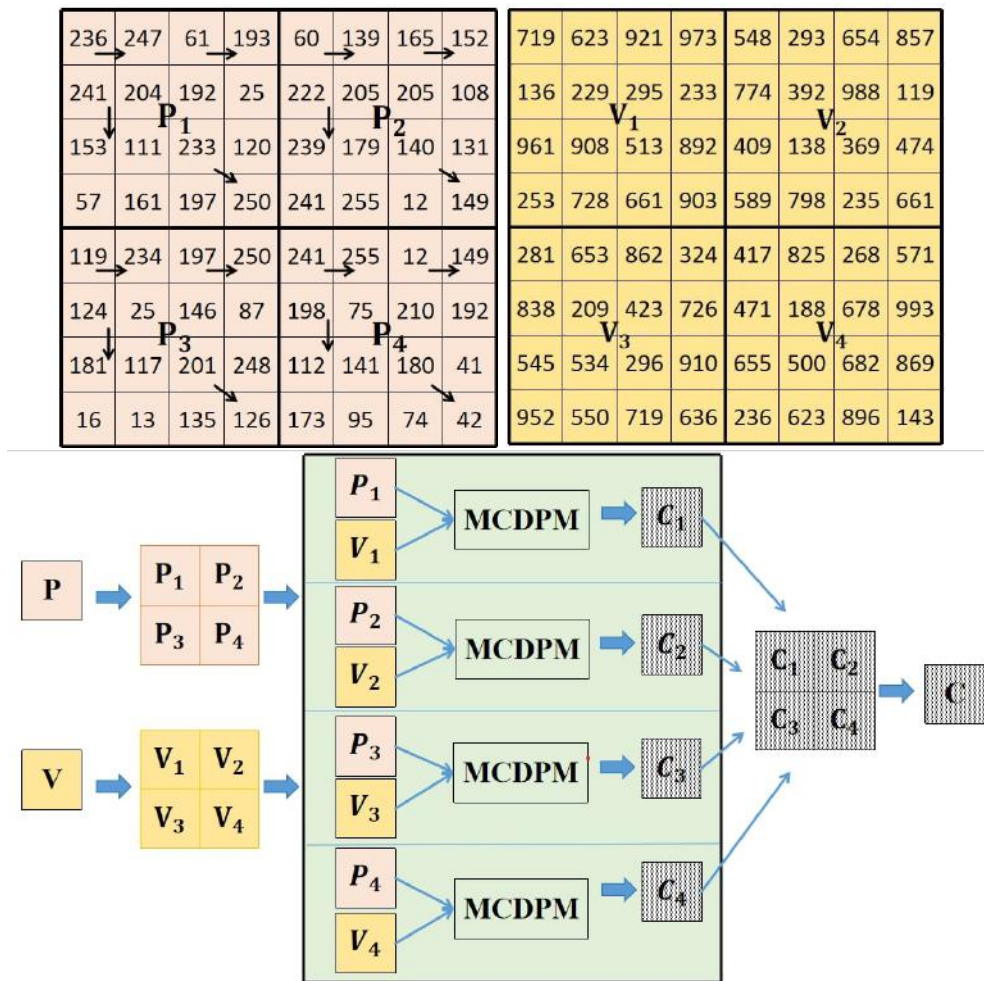


Figure 3.8: Illustration of Modified Cyclic Diffusion with Pixel Mixing.

Algorithm 3.1: Steps for applying Modified Cyclic Diffusion with Pixel Mixing.

Input : Plain image P , chaotic sequence V

Output: Diffused image C

- 1 Divide the P into four blocks i.e., P_1, P_2, P_3, P_4 .
 - 2 Divide the V into four blocks i.e., V_1, V_2, V_3, V_4 .
 - 3 Compute C_1 by substituting values of block pair (P_1, V_1) in (3.4.4).
 - 4 Compute C_2 by substituting values of block pair (P_2, V_2) in (3.4.4).
 - 5 Compute C_3 by substituting values of block pair (P_3, V_3) in (3.4.4).
 - 6 Compute C_4 by substituting values of block pair (P_4, V_4) in (3.4.4).
 - 7 Concatenate the blocks (C_1, C_2, C_3, C_4) to obtain diffused image C .
-

Furthermore, the MCDPM is exhibited in Algorithm 3.1 and Figure 3.8. The elements of array C are to be permuted using CCT. Once the confusion and diffusion stages are over, all the essential information in the image becomes permanently irretrievable.

3.4.3 Cascading Confusion Transformation

The CCT is designed to disrupt the spatial arrangement of image pixels. This process significantly reduces the correlation between adjacent pixels in the confused image. To initiate this process, sequences are initially generated using ZM (3.2.1), as described in Section 3.4.1. After iterating ZM (3.2.1), the chaotic sequence, x of length $(M \times N)$, is obtained. The chaotic sequence x is sorted row-wise and column-wise in ascending order and is stored in SX_r and SX_c . The new position of the element of sequence x in the sorted sequences SX_r and SX_c is stored in the argument sequences Arg_r and Arg_c , respectively. These argument sequences Arg_r and Arg_c are used to shuffle the pixels of the plain image P as shown in Figure 3.9 and Algorithm 3.2. In the first step of the confusion process, the columns of the plain image are swapped, followed by the clockwise circular shift of the rows. The second step involves swapping the matrix rows and clockwise shifting the columns. All the pixels of the plain image are shuffled, resulting in a complex cipher image. The output matrix is stored as a new permuted matrix T . The matrix T is the obtained final cipher image.

The first round of encryption uses K_1 , MCDPM and CCT operations. Similarly, the

Algorithm 3.2: Cascading Confusion Transformation (CCT).

Input : Diffused image C , chaotic sequences x .

Output: Permutated matrix T

```

1  $x = \text{reshape}(x, M \times N)$ ;
2 Sort  $x$  row-wise,  $SX_r = \text{row\_sort}(x)$ , Sort  $x$  column-wise,  $SX_c = \text{col\_sort}(x)$ ;
3 Store location of elements of  $SX_r$  in  $x$  in  $Arg_r$  and  $Arg_c$ :  $Arg_r = \text{arg}(SX_r)$ ,  $Arg_c$ 
  =  $\text{arg}(SX_c)$ ;
4 Function  $\text{SwapColumns}(C, i, j)$ ;
5   for  $r = 1$  to  $M$  do
6   |   Swap  $C[r, i]$  and  $C[r, j]$ ;
7   end
8 Function  $\text{Circular-shift-Rows}(C, Arg_r)$ ;
9   Circular shift rows of  $C$  in clockwise direction using the elements of row
    in  $Arg_r$ ;
10 Function  $\text{SwapRows}(C, i, j)$ ;
11   for  $cs = 1$  to  $N$  do
12   |   Swap  $C[i, cs]$  and  $C[j, cs]$ ;
13   end
14 Function  $\text{Circular-shift-Columns}(C, Arg_c)$ ;
15   Circular shift columns of  $C$  in clockwise direction using elements of
    columns in  $Arg_c$ ;
16 Store the resulting matrix as  $T$ ;

```

40

MCDPM and CCT operations are performed for K_2 , K_3 , and K_4 . The obtained cipher image after the last step is random and possesses no information about the plain image. Since the ZM-IEA uses four rounds of encryption and four different initial seeds in each round, the IEA is complex and highly sensitive.

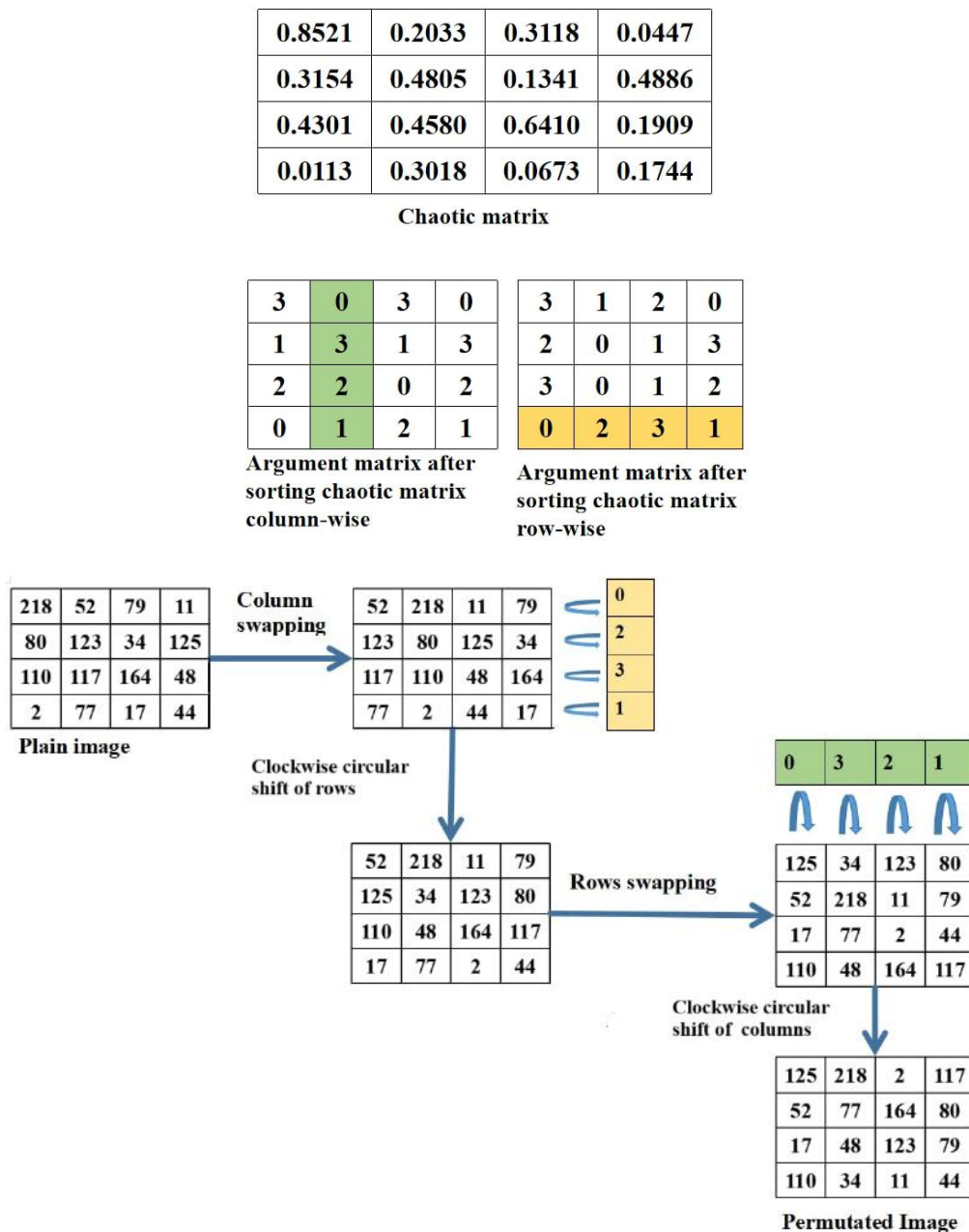


Figure 3.9: Cascading Confusion Transformation (CCT).

Since the proposed ZM-IEA is symmetric, it uses the same key in the encryption and decryption operations. As encryption and decryption processes are inherently re-

versible, the decryption process entails executing the inverse operations of the encryption process.

3.5 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed ZM-IEA, we performed a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and resilience are compared to various algorithms regarding information entropy, NPCR, UACI, correlation coefficient and execution time.

3.5.1 Information entropy analysis

Table 3.1 presents the information entropy values of cipher images generated by the proposed ZM-IEA and other existing algorithms. The entropy values for images encrypted using ZM-IEA are consistently close to the ideal value of 8, which indicates a high level of randomness. This suggests that the ZM-IEA effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it poses a challenge before an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the ZM-IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the plain image content.

Table 3.1: Information entropy values of the cipher images obtained using ZM-IEA and other existing IEAs.

Image/IEA	ZM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9993	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9992	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9968	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9999	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9998	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9998	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9998	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9998	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9993	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9970	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9994	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9993	7.9992	7.9992	7.9992	7.9991
bridge256	7.9976	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9993	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9970	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9993	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

42

3.5.2 Differential attack

Table 3.2 and Table 3.3 present a comparative analysis of NPCR and UACI values for various encrypted images using different IEAs. The results clearly demonstrate that the proposed ZM-IEA consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related algorithms often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the ZM-IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that ZM-IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

Table 3.2: NPCR values of the ZM-IEA and other existing IEAs.

Image/IEA	ZM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.6044	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.6025	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.6246	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6101	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6203	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.6116	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6156	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.6164	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.5979	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.6155	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.5972	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6216	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.6330	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.6262	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.6155	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

Table 3.3: UACI values of the ZM-IEA and other existing IEAs.

Image/IEA	ZM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.4568	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.5148	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.3081	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.4411	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4569	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.4546	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.4365	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.4624	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.4339	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.6601	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.4831	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.3836	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.5105	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.3970	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.4041	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

3.5.3 Histogram analysis

Figure 3.10 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining the Figure 3.10, it becomes clear that a significant trans-

formation occurs in the statistical distribution of pixel intensities. In case of the plain images, the histograms display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 3.10(d-f)). These patterns can often reveal information about the image content, making plain images vulnerable to statistical attacks. While, the histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the ZM-IEA has effectively randomized the pixel values across the entire gray-scale range (Figure 3.10(j-l)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the histograms of the cipher image confirm that the IEA has successfully obscured the plain image information. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

3.5.4 Correlation Coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 3.4. As observed from the Table 3.4, plain images exhibit very high correlation coefficients, with values close to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the encryption process has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of the IEA in reducing statistical information.

In addition, the pixel intensity distribution is illustrated in Figure 3.11. For the plain images shown in Figure 3.11(a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 3.11(d-f), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

44

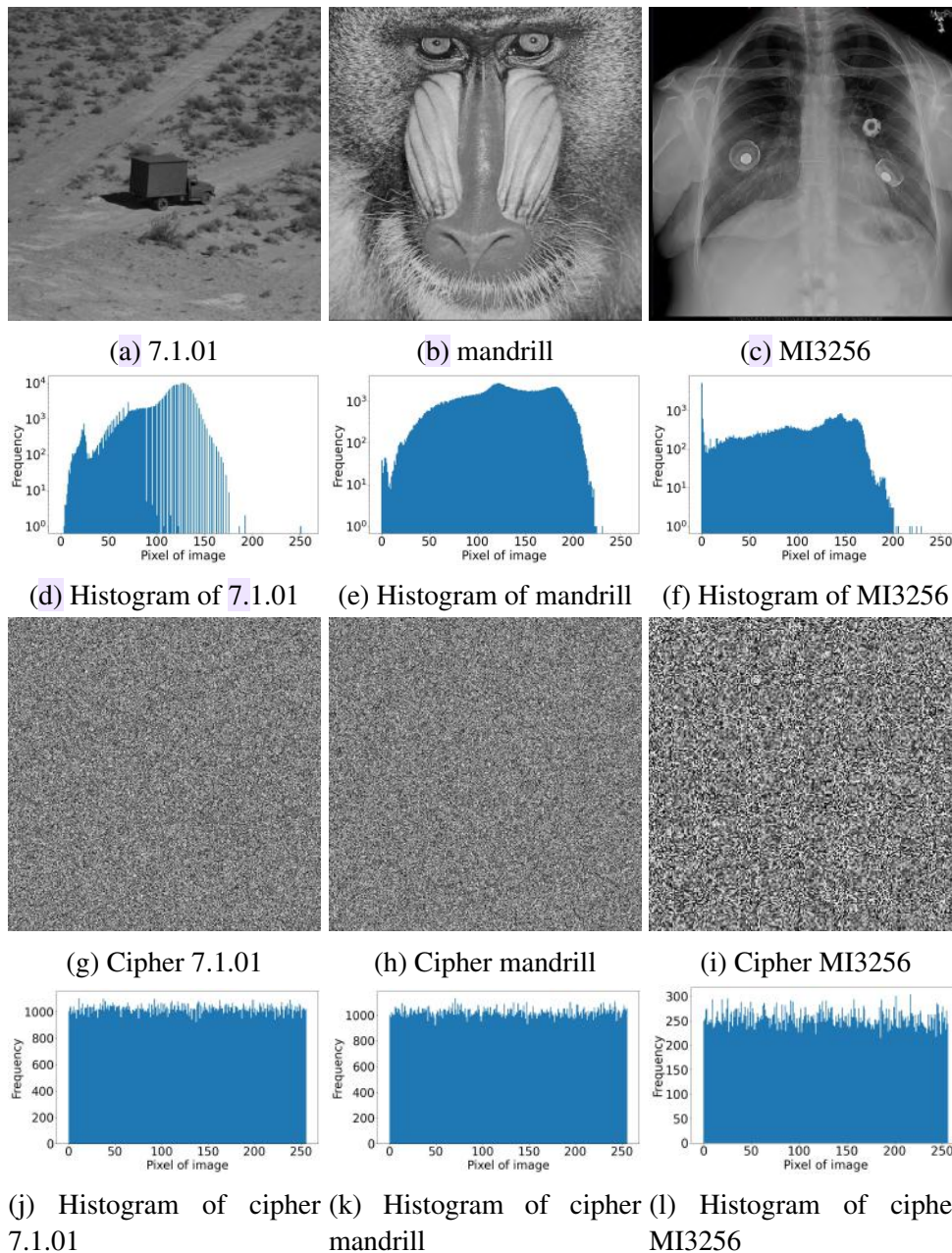


Figure 3.10: Histogram of plain and encrypted images

Table 3.4: Comparison of correlation coefficient values of ZM-IEA with algorithms available in the literature.

Image	Plain image	ZM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]	
7.1.01	HD	0.9630	0.0001	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD	0.9192	0.0039	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD	0.8995	-0.0058	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD	0.8625	-0.0023	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD	0.7669	-0.0083	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD	0.7202	-0.0003	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD	0.9784	-0.0170	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD	0.9795	-0.0055	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD	0.9405	0.0036	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085

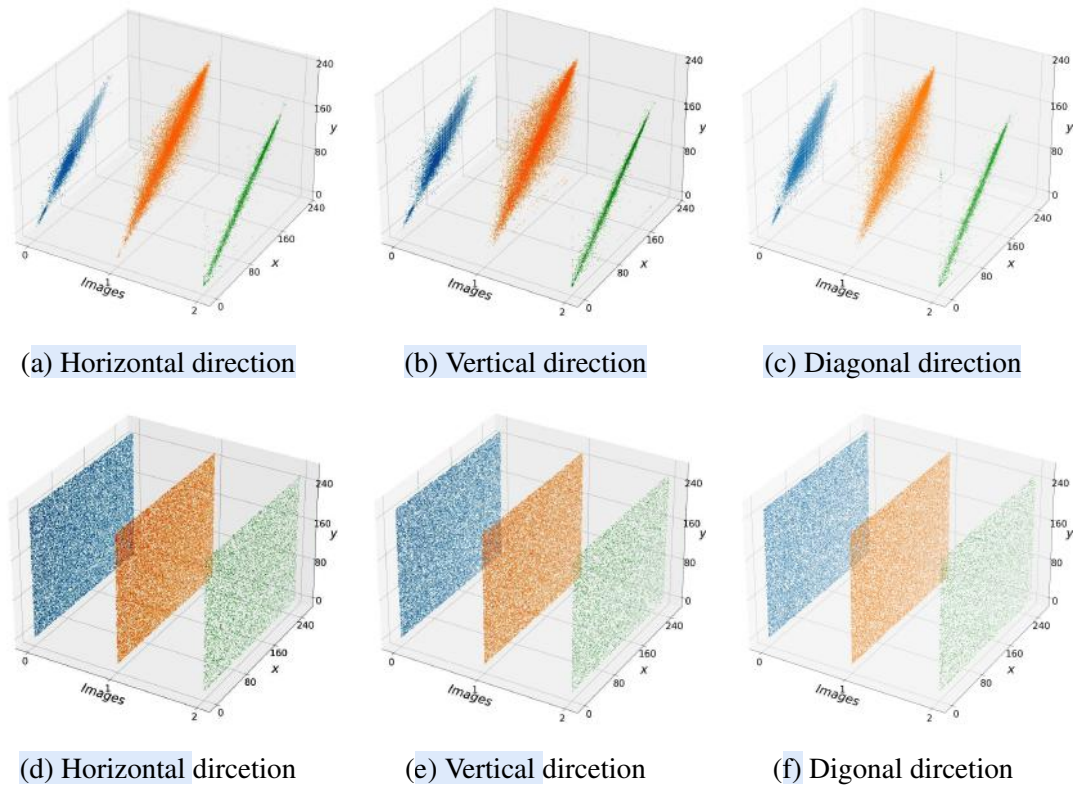


Figure 3.11: Pixel distribution of plain and cipher images

3.5.5 Resistance to classical attacks

The robustness of proposed ZM-IEA against chosen-plaintext attacks is established through Equation (2.3.8). This operation is visually represented in Figure 3.12. By examining Figure 3.12(a),(b), it is clear that (2.3.8) holds, suggesting that the ZM-IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 3.12(a) and Figure 3.12(b). The resulting NPCR value between these two images is 99.5960%, further reinforcing the ZM-IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed ZM-IEA is also expected to be resilient against other classical attacks.

3.5.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in

46

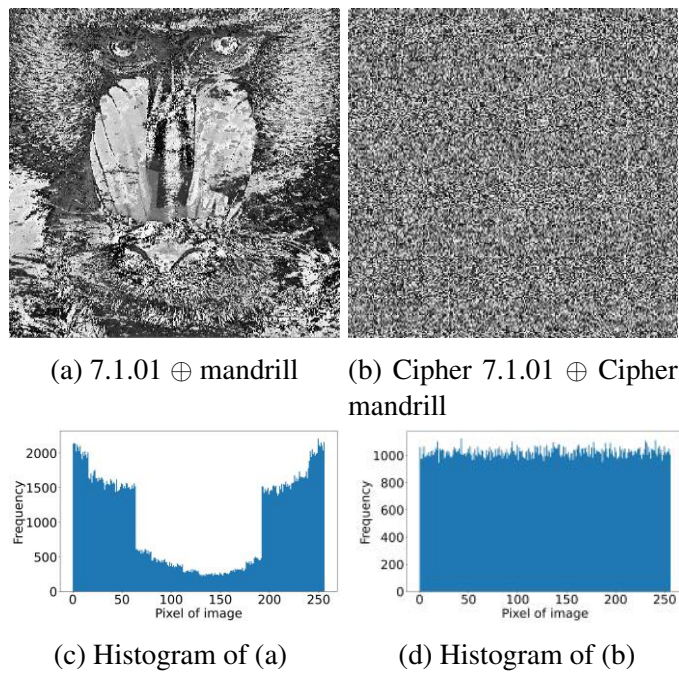


Figure 3.12: Resistance to classical attacks

Figure 3.13(a). The corresponding decrypted image of the occluded images is shown in the Figure 3.13(b). The decrypted image retains most of the original visual content, indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that ZM-IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.

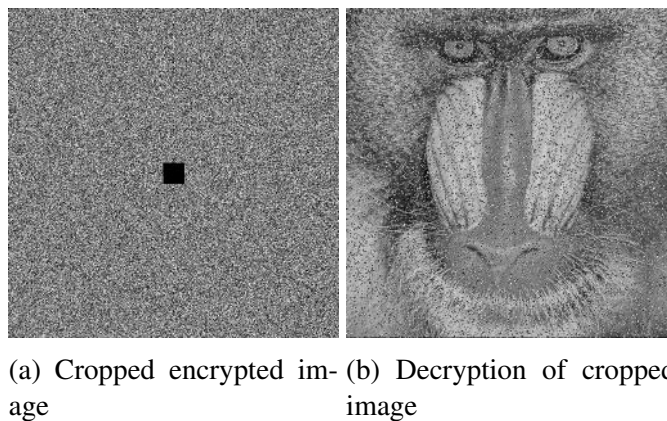


Figure 3.13: Representation of ZM-IEA's resistance to cropping attack

3.5.7 Noise attack

To assess the resilience of decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 3.14(a), while the corresponding decrypted image is shown in Figure 3.14(b). Despite the presence of noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption algorithms can effectively tolerate such distortions. These results confirm that ZM-IEA is robust against noise attacks and suitable for secure image transmission over noisy communication channels.

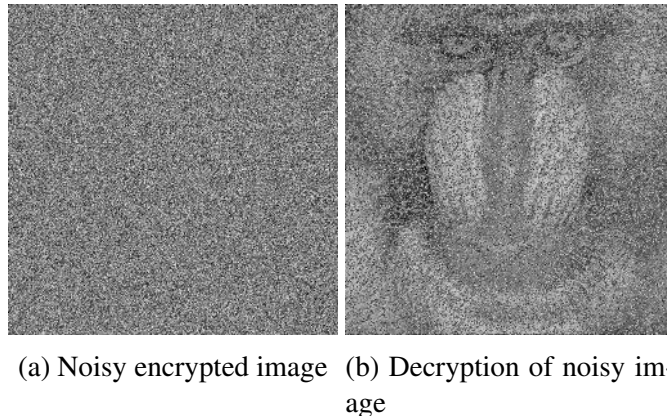


Figure 3.14: Representation of ZM-IEA's resistance to Noise attack

3.5.8 Randomness test

Table 3.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the ZM-IEA. As shown in the Table 3.5, the cipher image successfully passes all the randomness tests, indicating that the ZM-IEA effectively introduces randomness in the encrypted images.

3.5.9 Execution time analysis

The execution time of the proposed ZM-IEA is presented in Table 3.6. For a comprehensive performance evaluation, these results are compared with the execution times

Table 3.5: Randomness test results for ZM-IEA.

Test name	p-value	Result
Frequency Test	0.7581	Successful
Run Test	0.9759	Successful
Run Test (Longest Run of Ones)	0.0966	Successful
Block Frequency Test	0.8831	Successful
Universal Statistical Test	0.4049	Successful
Linear Complexity Test	0.9643	Successful
Serial Test	0.4639	Successful
Binary Matrix Rank Test	0.6028	Successful
Non-overlapping Template Matching Test	0.6529	Successful
Overlapping Template Matching Test	0.0133	Successful
Approximate Entropy Test	0.5559	Successful
Random Excursion Test	0.1758	Successful
Random Excursion Variant Test	0.5849	Successful
Cumulative Sums	0.3829	Successful
Discrete Fourier Transform Test	0.9123	Successful

of other encryption algorithms available in the literature. This comparison highlights the efficiency of the proposed ZM-IEA in terms of computational speed. As shown in Table 3.6, the ZM-IEA shows higher execution time compared to other algorithms available in literature, it offers enhanced robustness and superior security features. This trade-off between time and performance indicates that while ZM-IEA may require more processing time, it compensates with greater resilience against several attacks.

Table 3.6: Comparison of execution time (in seconds) of the ZM-IEA with algorithms available in the literature.

Image/IEA	ZM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	16.97	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	14.74	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	3.90	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

3.6 Summary

This chapter proposes the hyper-chaotic Zirili map along with novel confusion and diffusion operations. An IEA is developed leveraging the map and operations. The performance of proposed ZM-IEA is rigorously evaluated using a diverse set of gray-scale images to ensure its applicability across different visual content. Comprehensive experimental analyses are conducted to assess the algorithm's robustness against multiple types of attacks, including statistical, differential, and brute-force attacks. The results

confirm that the IEA effectively disrupts the inherent correlations in image data, ensuring high security. Furthermore, the corresponding decryption algorithm reconstructs the plain image content, demonstrating the algorithm's reliability and lossless recovery capability.

Chapter 4

Coupled Kaplan-Yorke-Logistic map with application in Image Encryption

Coupling refers to the phenomenon where two or more systems influence each other's behavior through mutual interaction [13]. The coupled nonlinear systems exhibit rich and complex chaotic characteristics [111]. The process of coupling chaotic systems enables researchers to control, enhance, or suppress chaos, thereby tailoring the system behavior to specific needs. This chapter presents a coupled chaotic map. Section 4.1 describes the background details required for the chapter. Section 4.2 proposes the coupled Kaplan-Yorke-Logistic map (KYLM). In Section 4.3, we have presented the analysis of KYLM utilising BD, PD, LE, PE, and SE. Section 4.4 proposes the IEA leveraging KYLM termed as KYLM-IEA. The KYLM-IEA employs simultaneous confusion and diffusion operation to disrupt the plain image. Section 4.5 describes the analysis of KYLM-IEA utilising several key metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 4.6 summarizes the chapter.

4.1 Background

This section describes the Kaplan-Yorke map and Logistic map. These maps are the utilised in the development of Coupled KYLM.

4.1.1 Kaplan-Yorke map

The Kaplan–Yorke map [112] is a 2D discrete-time chaotic map. The map involves one parameter and the Cosine term. Utilising the given initial points (x_0, y_0) , the map can be iterated to obtain sequence x and y . The map is given in (4.1.1).

$$\begin{aligned} x_{i+1} &= \text{mod}(2x_i, 0.99995) \\ y_{i+1} &= ky_i + \cos(4\pi x_i) \end{aligned} \quad (4.1.1)$$

here, $\text{mod } 0.99995$ is the modulo operator with real arguments. For the Kaplan-Yorke map, the PD, BD, and LE are exhibited in Figure 4.1. The PD reveals patterns and the LE of the map is very low and often negative, indicating weak dynamics. Similarly, the BD does not display rich and complex behavior. It can be concluded that its overall chaotic properties are relatively limited.

4.1.2 Logistic map

Logistic map is 1D dynamic non-linear equation exhibiting complex chaotic characters [15]. The mathematical expression for the map is given in (4.1.2).

$$x_{i+1} = \mu x_i(1 - x_i) \quad (4.1.2)$$

where $\mu \in (0, 4]$ is the control parameter. x_i is i^{th} term of the sequence. The produced chaotic sequence is pseudo-random, non-periodic, and unexpected for the proper selection of bifurcation parameter μ . The map displays bifurcations as μ increases, transitioning from periodic behaviour to chaos. For the Logistic map, the BD and LE are shown in Figure 4.2. The BD exhibits chaotic behavior in a narrow range of the control parameter, while the corresponding LE is negative and low, indicating the presence of

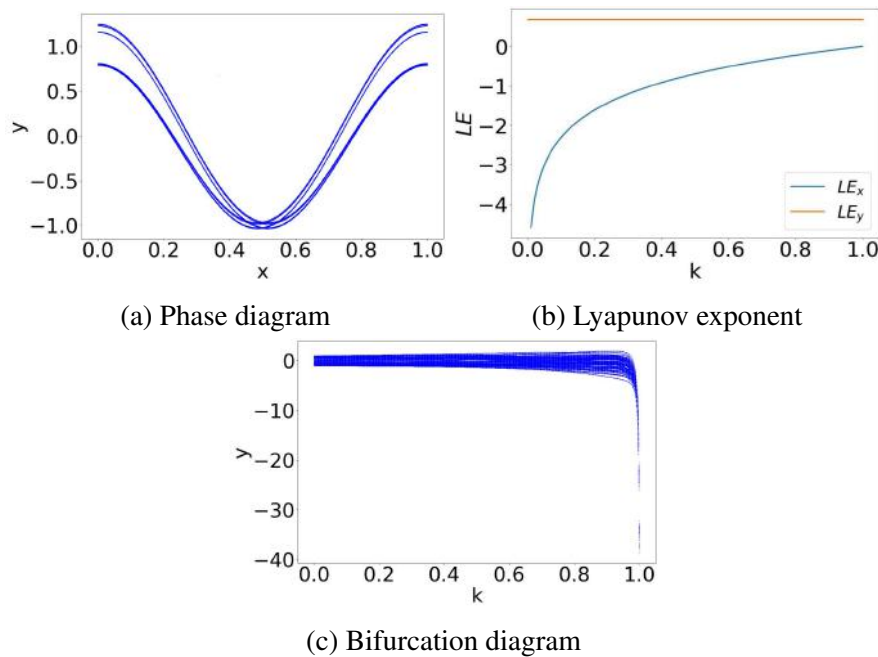


Figure 4.1: Diagrams related to Kaplan-Yorke map.

weak chaotic dynamics.

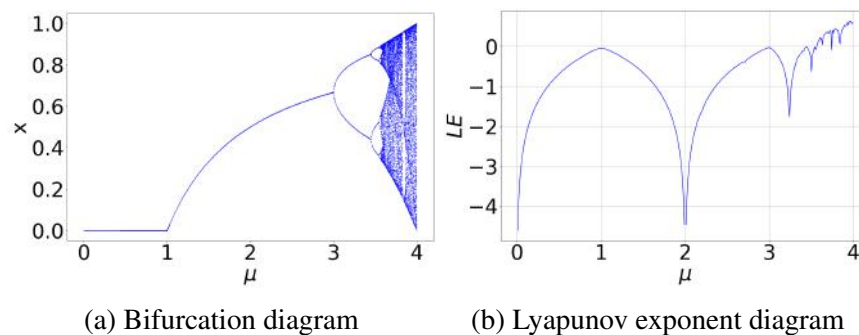


Figure 4.2: Logistic map

4.2 Proposed coupled Kaplan-Yorke-Logistic map

The Kaplan-Yorke map and Logistic map exhibit limited chaotic behaviour and narrow chaotic range of control parameter. To address these issues, we aim to develop a chaotic map with superior chaotic characteristics. Through coupling, we've significantly enhanced the distribution of chaotic trajectories, sensitivity to initial values and control parameters, and unpredictability of the map. The proposed map is a hybrid map that emerges from the fusion of two distinct maps: the Kaplan-Yorke map and

54

the Logistic map. The KYLM exhibits a high level of chaotic behaviour owing to its incorporation of non-linear components and utilisation of features from multiple maps. The map demonstrates hyper-chaotic behaviour within a broad parameter space, uniform output distribution and high values of LE. This novel map is 2D discrete and characterised by a pair of control parameters (μ, ω) . The proposed map is given in (4.2.1):

$$\begin{aligned}x_{i+1} &= \text{mod}(2x_i + \mu y_i(1 - y_i), 1) \\y_{i+1} &= \text{mod}(\omega y_i + \cos(4\pi x_{i+1}), 1)\end{aligned}\tag{4.2.1}$$

where, x_i , and y_i represent the values of the sequences x , and y at i^{th} - iteration. The control parameters μ , and ω are in the range $[0, \infty)$. The modular operation $\text{mod}(\bullet, 1)$ is used to adapt the sequences x and y in the range $(0, 1)$. For experimental purposes, the values of control parameters are set in $[0, 10]$.

4.3 Analysis of the Kaplan-Yorke-Logistic map

The chaotic behavior of the KYLM is comprehensively investigated by employing a range of tools, including BD to visualize the transition between periodic and chaotic regimes, PD to depict the map's state space trajectories, LE to quantify the rate of divergence of nearby trajectories and confirm chaotic dynamics, PE to measure the complexity of the time series based on ordinal patterns, and SE to assess the irregularity and unpredictability of the map's temporal evolution. These tests are performed and the results are discussed in the subsequent sections.

4.3.1 Bifurcation diagram

Figure 4.3 illustrates the BD of the KYLM with respect to the control parameters μ and ω , one varying within the interval $[0, 10]$, while keeping the other parameter fixed and using initial conditions $x_0 = 0.55$ and $y_0 = 0.03$. These diagrams reveal that the KYLM exhibits significant ergodicity across a broad range of control parameter values. Furthermore, the BD highlight the high sensitivity of the KYLM to variations

in its control parameters. Even small changes in μ or ω result in different dynamic behaviors indicating high chaotic dynamics. Thus, it can be concluded that KYLM is well-suited for integration into IEAs.

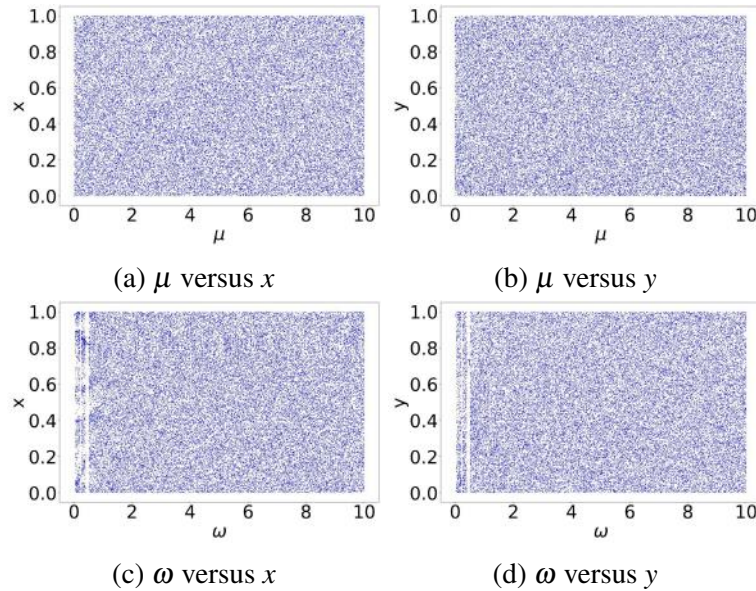


Figure 4.3: Bifurcation diagram of the KYLM.

4.3.2 Phase diagram

The PD of the KYLM and other maps, as listed in Table 2.1, are exhibited in Figure 4.4. The PD are plotted using the initial values as KYLM $((x_0, y_0, \mu, \omega) = (0.55, 0.03, 3.3571, 5))$, CLM $((x_0, y_0, a, a_1) = (0.5, 0.8, 5, 5))$, ICLM $((x_0, y_0, a, a_1) = (0.3, 0.1, 0.1, 0.1))$, LMHM $((x_0, y_0, \beta, k_1, k_2, \rho_1, k) = (0.5, 0.8, 0.1, 1, 0.1, 100, 0.7))$, IGSCM $((x_0, y_0, r_1, r_2) = (0.21, 0.31, 25, 23.3))$, SLM $((x_0, y_0, \Gamma, p) = (0.3, 0.4, 4, 3.6))$, HSM $((x_0, y_0, b_1, b_2, \omega) = (0.3, 0.6, 5, 1.57, 10))$, LNIC $((x_0, y_0, a, a_1) = (0.9, 0.6, 1, 1))$, CLSS map $((x_0, y_0, c) = (0.3, 0.6, 0.5))$, LCCCM $((x_0, y_0, \mu, p_1) = (0.6, 0.9, 5, 8.78))$. The KYLM's PD demonstrates a uniform distribution throughout the phase space. This indicates that the state trajectories of the KYLM do not concentrate in specific regions but are instead evenly dispersed across the entire region. In contrast, the PD of other maps display non-uniform distributions. This observation suggests that the proposed maps offer enhanced resistance to phase space reconstruction attacks.

56

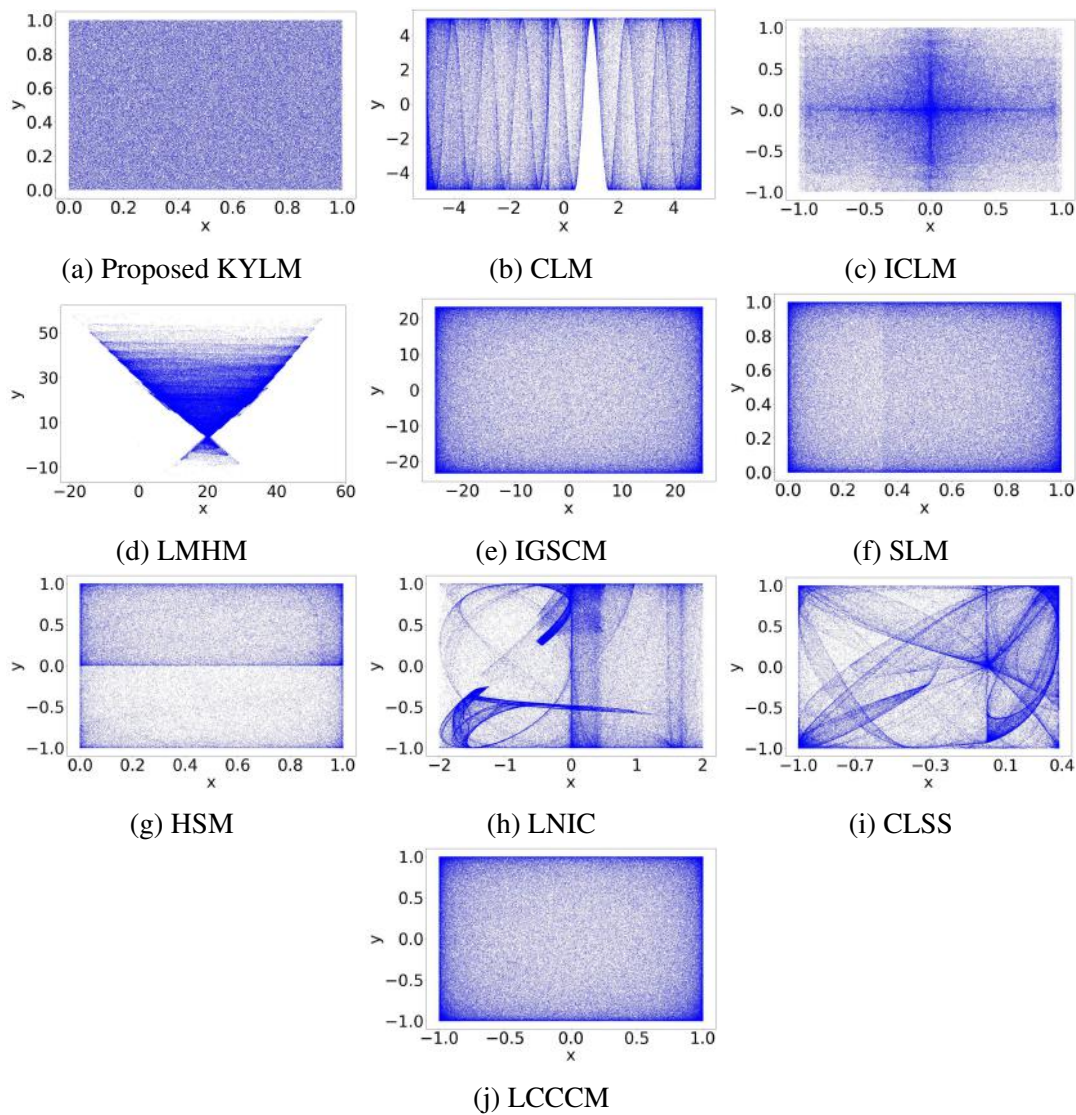


Figure 4.4: Phase diagrams (x and y).

4.3.3 Lyapunov exponent

The LE of KYLM and other maps, as listed in Table 2.1, are exhibited in Figure 4.5. LE_x and LE_y represent the LEs associated with the x and y variables, respectively. From the Figure 4.5, it is visible that the LEs of KYLM map are positive and high as compared to other maps except IGSCM. Thus it can be concluded that the KYLM is extremely sensitive to initial conditions. The larger the LE, the faster this divergence happens. Thus KYLM is hyper-chaotic, complex, unpredictable and hence suitable for integration into IEAs.

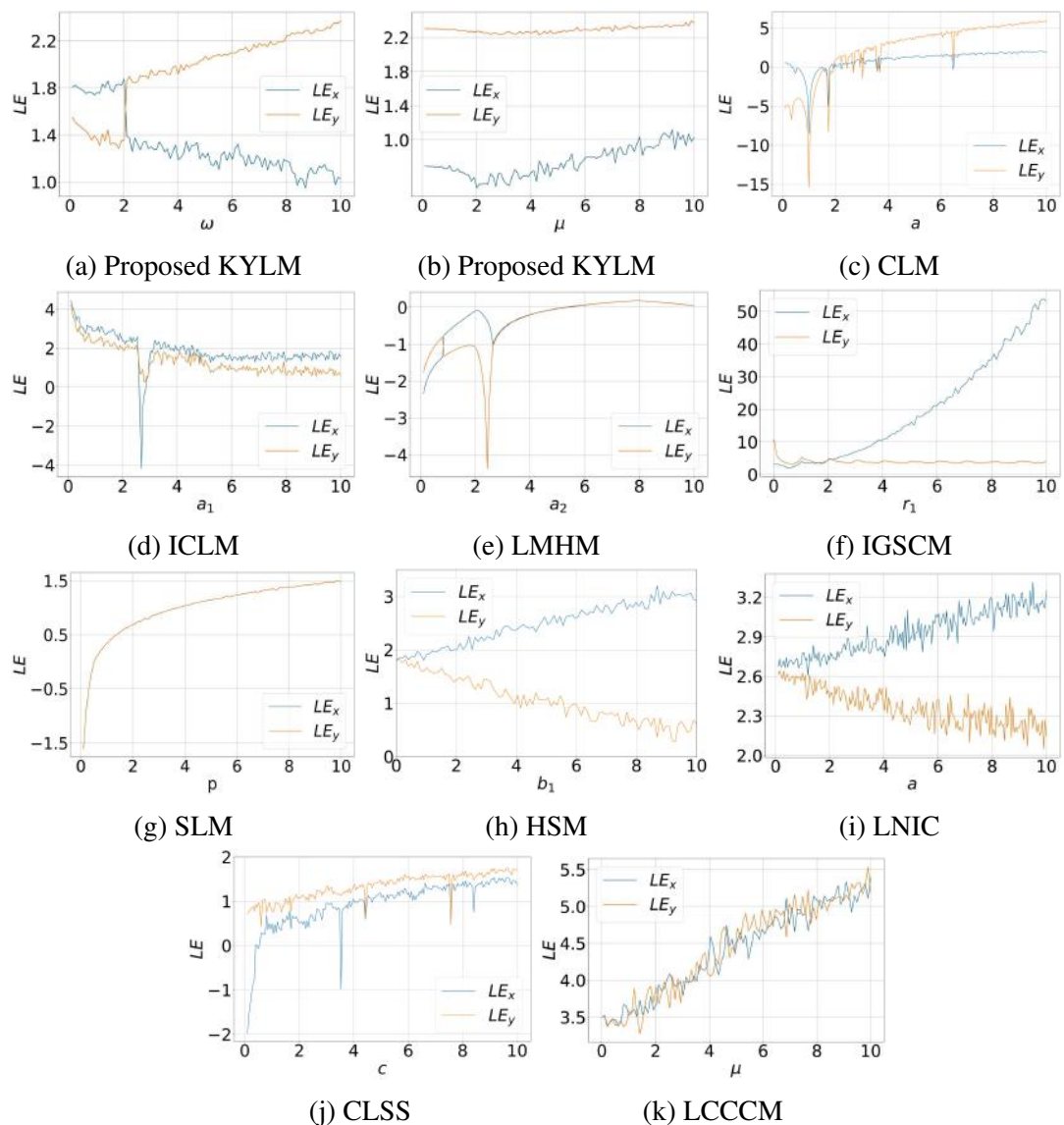


Figure 4.5: Lyapunov exponent diagram of Kaplan-Yorke-Logistic and others maps.

58

4.3.4 Permutation entropy

Figure 4.6 illustrates the PE of the KYLM alongside other chaotic maps listed in Table 2.1. As shown in the Figure 4.6, the KYLM consistently exhibits values near 1 across the specified range of control parameters. This suggests that the KYLM demonstrates highly complex or chaotic behavior, making it a strong candidate for applications requiring randomness or unpredictability, such as cryptography or secure communications.

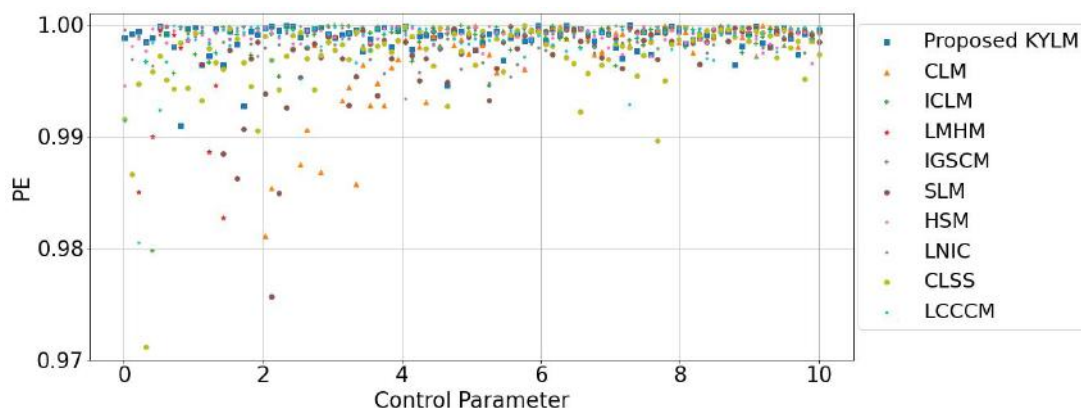


Figure 4.6: Permutation entropy of KYLM.

4.3.5 Sample entropy

Figure 4.7 shows the SE of the KYLM compared to other chaotic maps listed in Table 2.1. As shown in Figure 4.7, the KYLM consistently achieves high values of SE around 2 across the evaluated range of control parameters, suggesting that the KYLM exhibits pronounced chaotic behavior. It can be inferred that KYLM is a strong candidate for applications requiring high unpredictability, including cryptography and secure communications.

4.4 Application of map in image encryption

This section explores the KYLM-IEA that utilises the *SHA3 – 512*, simultaneous confusion and diffusion, and KYLM. The steps involved in IEA are the generation of

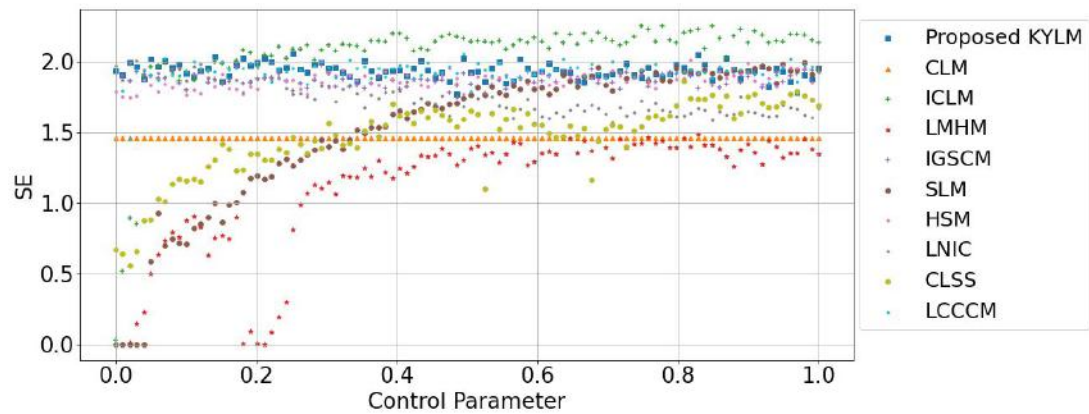


Figure 4.7: Sample entropy of KYLM.

a sequence and the simultaneous confusion and diffusion of plain image pixels. The sequence generation procedure is defined in Section 4.4.1. Similarly, simultaneous confusion and diffusion procedures are briefly described in Section 4.4.2. The steps of the KYLM-IEA are shown in Figure 4.8.

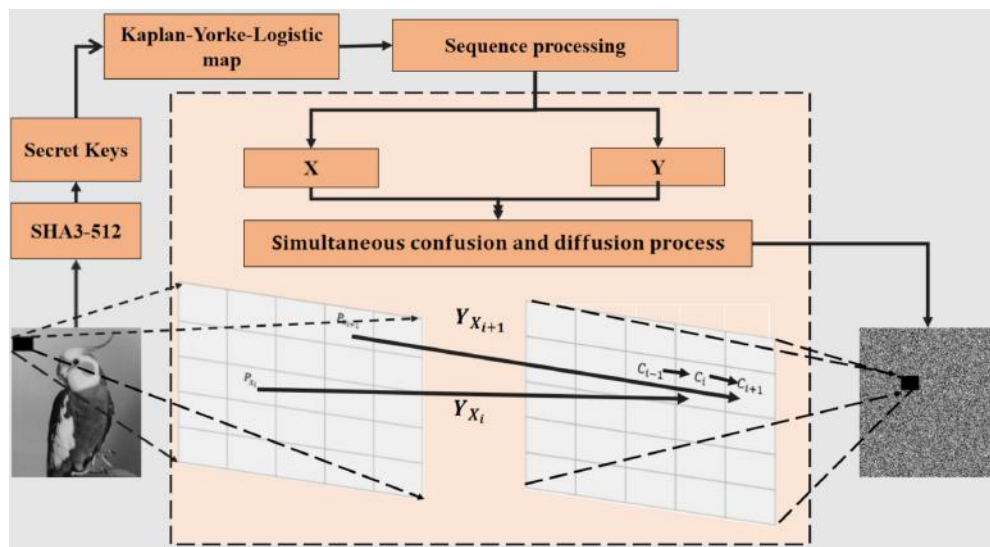


Figure 4.8: Image encryption algorithm leveraging KYLM (KYLM-IEA).

4.4.1 Sequence generation

In the encryption and decryption processes utilising chaotic maps, sequences from these chaotic maps undergo modifications to enhance their suitability for encryption operations. This adaptation ensures the resulting sequences possess valuable properties

60

to secure encryption and decryption processes. To perform this, the KYLM needs specific initial values and control parameters. These parameters play a critical role in shaping the behaviour of the chaotic map, influencing the generation of the sequence. The generated sequences undergo modification and are then used in KYLM-IEA. The initial values and parameters crucial for the KYLM are derived from a hash value. The hash values are obtained from the plain image using *SHA3 – 512*. Using SHA, we get different hash values for different plain images and, hence, different initial values and control parameters. To ensure robust protection against a wide range of brute-force attacks, the cryptographic algorithm requires a key space of size 2^{100} [113]. In our proposed KYLM-IEA, the encryption key denoted as K is derived from the *SHA3 – 512* hash function, resulting in a key length of 512 bits. Hence, the key space has a size of 2^{512} , which is sufficient to resist brute-force attacks.

The *SHA3 – 512* hash function generates the key as follows: $K = \text{SHA3} - 512(P)$, where the input data P is the plain image. Consequently, the key becomes closely tied to the plain image, enhancing security and resilience against plaintext/ciphertext attacks. In the hash value K , each hexadecimal number is of 4 bits. The obtained hash value K is divided into parts and converted into decimals using (4.4.1). The initial keys and control parameters are as given in (4.4.1).

$$\begin{cases} x_0 = \frac{\text{hex2dec}(K_{1:25})}{2^{100}}, \\ y_0 = \frac{\text{hex2dec}(K_{26:50})}{2^{100}}, \\ \omega = 10 \left(\frac{\text{hex2dec}(K_{51:75})}{2^{100}} \right), \\ \mu = 10 \left(\frac{\text{hex2dec}(K_{76:100})}{2^{100}} \right), \\ \text{initial_pixel} = \text{mod}(\text{hex2dec}(K_{101:128}), 256) \end{cases} \quad (4.4.1)$$

where, x_0 , y_0 are the initial values and ω , and μ are the control parameters. The *initial_pixel* represents the initial pixel value to be used in the simultaneous confusion and diffusion process.

With these values, KYLM is iterated for $500 + M \times N$. The obtained sequences x and y are modified and applied in the IEA. The first 500 terms from each sequence x and

y are removed to avoid transient effects. Then, the sequence $x = \{x_1, x_2, \dots, x_{M \times N}\}$ is sorted in ascending order and its arguments are stored in X . Further, the sequence y is modified as given in (4.4.2) and stored in Y .

$$Y_i = \text{mod}(\lfloor y_i \times 10^{10} \rfloor, 256), i = 0, 1, 2, \dots, (M \times N) - 1 \quad (4.4.2)$$

Where $\lfloor \bullet \rfloor$ is the floor function, and $\text{mod}(\bullet, 256)$ sets the numbers in range $[0, 255]$. The Algorithm 4.1 describes the sequence generation process. The forthcoming section will detail the utilisation of sequences X and Y in both the simultaneous confusion and diffusion steps.

Algorithm 4.1: Sequence generation for KYLM.

Input : plain image P .

Output: X, Y

- 1 Input gray plain image P of size $M \times N$. $K = \text{SHA3} - 512(P)$.
 - 2 Convert K into decimals using Equation (4.4.1).
 - 3 Obtain values: $x_0, y_0, \omega, \mu, \text{initial_pixel}$
 - 4 Iterate KYLM for $500 + M \times N$ and store x and y .
 - 5 Sort x in ascending order and store its arguments in X .
 - 6 Modify y using (4.4.2) and store as Y .
 - 7 Output: X, Y
-

4.4.2 Simultaneous confusion and diffusion process

In the intriguing world of chaos-based IEAs, implementing a confusion-diffusion framework is a popular method. This framework operates in two vital stages: confusion and diffusion, both pivotal in the encryption process. During the confusion stage, the locations of the pixels in the image are systematically altered using a secret key. This procedure alters the spatial configuration of the image, rendering it incomprehensible to anyone without appropriate authorization. The secret key plays a crucial role in this intricate process of pixel repositioning, ensuring robust encryption. In the diffusion step, the image's pixel values are modified by utilising crucial secret keys. For this stage, it is necessary to perform accurate changes in the pixel values and effectively disperse the encrypted data throughout the image. The diffusion method ensures that the encrypted information is deeply integrated into the image's visual features by spread-

62

ing the secret key's impact across the pixels. The distinguishing characteristic of the KYLM-IEA is its capacity to perform the confusion and diffusion phases concurrently. Rather than sequentially completing these processes, they work together in synergy, enhancing the encryption strength and effectiveness of the algorithm. The simultaneous execution of this process improves the security of the encryption by introducing additional levels of complexity and unpredictability, hence increasing the difficulty of decryption. In the technique of simultaneous confusion and diffusion, the i^{th} encrypted image pixel is associated with the X_i^{th} plain image pixel, the X_i^{th} element of the chaotic sequence, and the previous cipher image pixel. The adjacent cipher pixels are obtained from nonadjacent plain pixels. As a result, both the position and content of a pixel in plain image may be changed at the same time. The steps of the IEA are shown below:

1. Load a gray-scale image P of size $M \times N$, where M and N are the height and width of the plain image, respectively.
2. Convert the P into the 1D array.
3. Set the cipher image as C with the first pixel as $C_0 = initial_pixel$.
4. Apply the simultaneous confusion and diffusion process on the plain image using the sequences X and Y as given in (4.4.3).

$$C_i = P_{X_i} \oplus Y_{X_i} \oplus C_{i-1}, \quad 1 \leq i \leq ((M \times N) - 1) \quad (4.4.3)$$

and \oplus denotes bit-wise XOR operation.

5. The obtained cipher image C is has $(M \times N)$ number of pixels. The cipher image C is reshaped into a size equal to the size of the P . Hence, C is the final encrypted image

Since the proposed KYLM-IEA is symmetric, it uses the same key in the encryption and decryption operations. As encryption and decryption processes are inherently reversible, the decryption process entails executing the inverse operations of the encryption process.

4.5 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed KYLM-IEA, we performed a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and resilience are compared to various algorithms regarding information entropy, NPCR, UACI, correlation coefficient and execution time.

4.5.1 Information entropy analysis

Table 4.1 presents the information entropy values of cipher images generated by the proposed KYLM-IEA and other existing algorithms. The entropy values for images encrypted using KYLM-IEA are consistently close to the ideal value of 8, which indicates a high level of randomness. This suggests that the KYLM-IEA effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it makes it significantly more difficult for an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the KYLM-IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the plain image content.

Table 4.1: Comparison of information entropy values of the KYLM-IEA with algorithms available in the literature.

Image	KYLM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9993	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9994	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9993	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9998	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9998	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9998	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9998	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9998	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9993	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9970	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9993	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9993	7.9992	7.9992	7.9992	7.9991
bridge256	7.9973	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9994	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9975	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9993	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

64

4.5.2 Differential attack

Table 4.2 and Table 4.3 present a comparative analysis of NPCR and UACI values for various encrypted images obtained using different encryption algorithms. The results clearly demonstrate that the proposed KYLM-IEA consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related algorithms often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the KYLM-IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that KYLM-IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

Table 4.2: Comparison of NPCR values of KYLM-IEA with algorithms available in the literature.

Image	KYLM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.6277	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.6174	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.6368	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6099	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6058	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.6230	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6099	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.6063	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.6010	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.6048	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.6021	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6231	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.6155	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.6216	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.6048	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

Table 4.3: Comparison of UACI values of the KYLM-IEA with algorithms available in the literature.

Image	KYLM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.4622	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.4846	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.5513	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.4268	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4015	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.4728	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.4904	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.5095	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.5017	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.3871	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.4845	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.4565	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.5346	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.4132	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.4521	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

4.5.3 Histogram analysis

Figure 4.9 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining Figure 4.9, it becomes clear that a significant transformation occurs in the statistical distribution of pixel intensities following the IEA. In the case of the plain images, the histograms typically display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 4.9(a-c)). These patterns can often reveal information about the image content, making plain images vulnerable to statistical analysis and attacks.

The histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the IEA has effectively randomized the pixel values across the entire gray-scale range (Figure 4.9(d-f)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the cipher image histograms confirms that the IEA has successfully obscured the plain image information. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

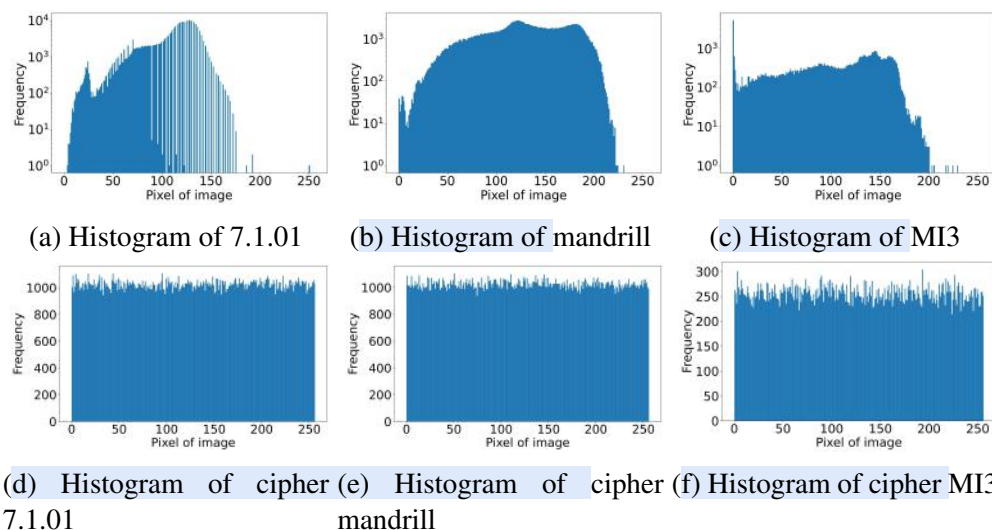


Figure 4.9: Histogram of plain and cipher images obtained using KYLM-IEA.

4.5.4 Correlation coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 4.4. As observed from the Table 4.4, plain images exhibit very high correlation coefficients, with values close to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the encryption process has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of IEA in reducing statistical information.

In addition, the pixel intensity distribution is illustrated in Figure 4.10. For the plain images shown in Figure 4.10(a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 4.10(d-f), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

Table 4.4: Comparison of correlation coefficient values of KYLM-IEA with algorithms available in the literature.

Image	Plain images	KYLM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	HD 0.9630	0.0072	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD 0.9192	-0.0008	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD 0.8995	-0.0006	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD 0.8625	0.0061	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD 0.7669	-0.0049	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD 0.7202	-0.0144	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD 0.9784	-0.0006	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD 0.9795	0.0141	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD 0.9405	-0.0178	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085

4.5.5 Resistance to classical attacks

The robustness of proposed KYLM-IEA against chosen-plaintext attacks is established through Equation (2.3.8). This operation is visually represented in Figure 4.11. By examining Figure 4.11(a),(b), it is clear that Equation (2.3.8) holds, suggesting that the KYLM-IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 4.11(a) and Figure 4.11(b). The resulting NPCR value between these two images is

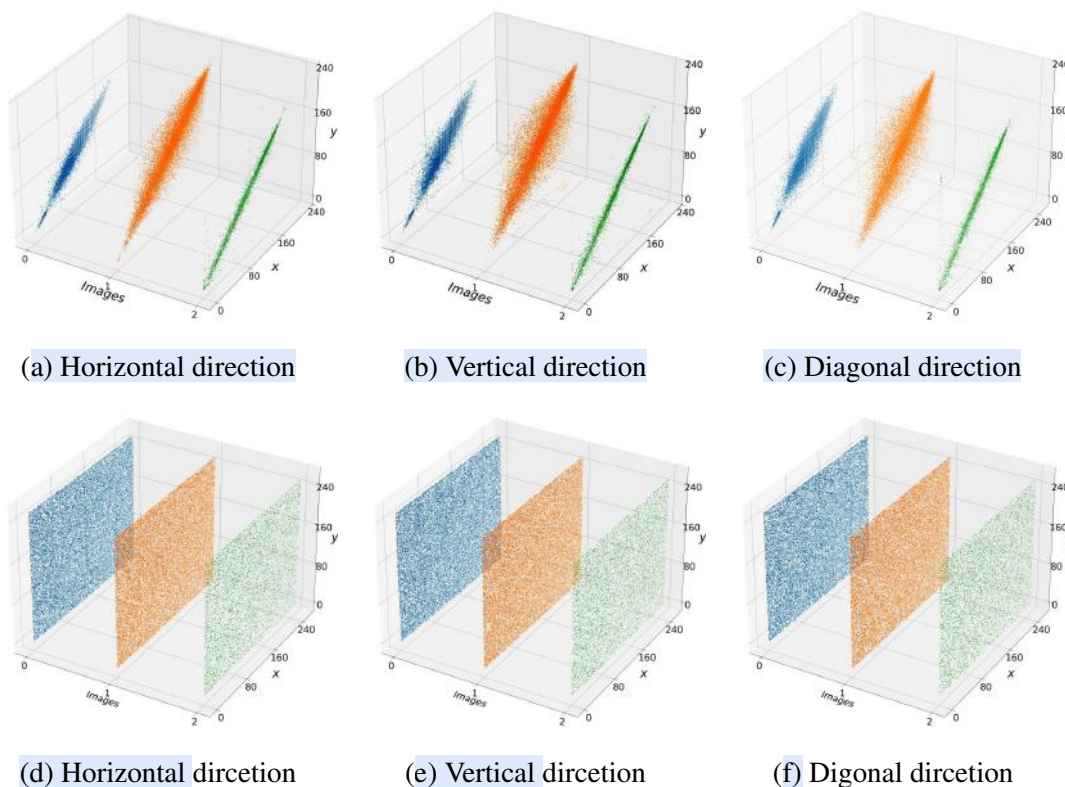


Figure 4.10: Pixel distribution of plain and cipher images obtained using KYLM-IEA.

99.6196%, further reinforcing the KYLM-IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed KYLM-IEA is also expected to be resilient against other classical attacks.

4.5.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in Figure 4.12(a). The corresponding decrypted image of the occluded images is shown in the Figure 4.12(b). The decrypted image retains most of the original visual content, indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that the KYLM-IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.

68

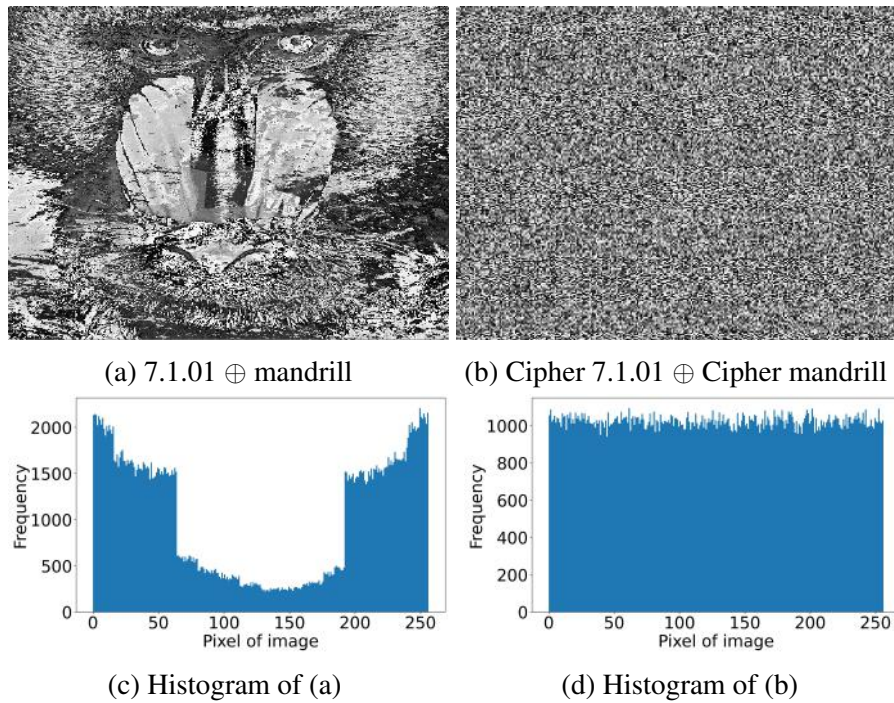


Figure 4.11: Resistance to classical attacks

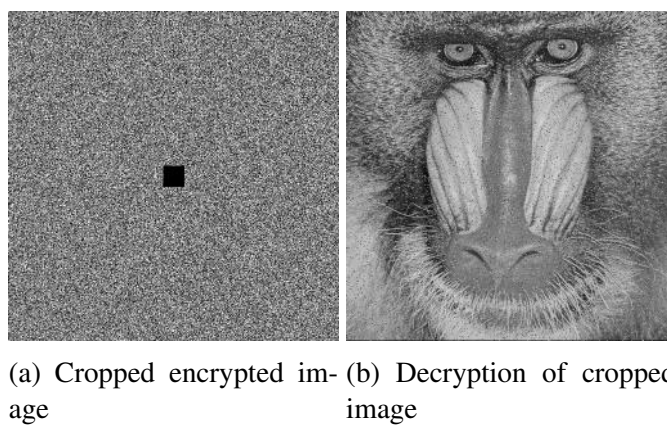
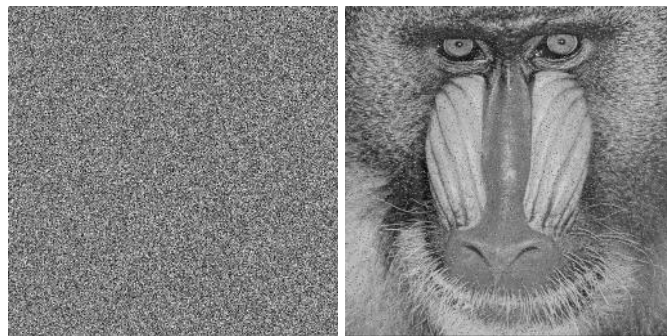


Figure 4.12: Representation of KYLM-IEA's resistance to cropping attacks.

4.5.7 Noise attack

To assess the resilience of the decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 4.13(a), while the corresponding decrypted image is shown in Figure 4.13(b). Despite the presence of noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption scheme can effectively tolerate such distortions. These results confirm that the KYLM-IEA is robust against noise attacks and suitable for secure image transmission over noisy communication channels.



(a) Noisy encrypted image (b) Decryption of noisy image

Figure 4.13: Representation of KYLM-IEA's resistance to Noise attack.

4.5.8 NIST randomness test

Table 4.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the KYLM-IEA. As shown in the Table 4.5, the cipher image successfully passes all the randomness tests, indicating that the KYLM-IEA effectively introduces randomness in the encrypted images.

70

Table 4.5: Randomness test results for KYLM-IEA.

Test name	p-value	Result
Frequency Test	0.0268	Successful
Run Test	0.4782	Successful
Run Test (Longest Run of Ones)	0.9653	Successful
Block Frequency Test	0.9626	Successful
Universal Statistical Test	0.3604	Successful
Linear Complexity Test	0.9930	Successful
Serial Test	0.1274	Successful
Binary Matrix Rank Test	0.5633	Successful
Non-overlapping Template Matching Test	0.3178	Successful
Overlapping Template Matching Test	0.6222	Successful
Approximate Entropy Test	0.3841	Successful
Random Excursion Test	0.1757	Successful
Random Excursion Variant Test	0.0692	Successful
Cumulative Sums	0.0392	Successful
Discrete Fourier Transform Test	0.9853	Successful

4.5.9 Execution time analysis

The execution time of the proposed IEA and related IEAs available in literature is presented in Table 4.6. From the Table 4.6, it is observed that the KYLM-IEA executes in a very short time, demonstrating high computational efficiency. Thus it can be concluded that the KYLM-IEA is fast enough to be applied in a real-world problem.

Table 4.6: Comparison of execution time (in seconds) of the KYLM-IEA with algorithms available in the literature.

Image	KYLM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	0.74	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	0.75	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	0.18	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

4.6 Summary

This chapter proposes the hyper-chaotic coupled Kaplan-Yorke-Logistic map. The proposed map is integrated into an IEA. The performance of the proposed KYLM-IEA is rigorously evaluated using a diverse set of gray-scale images to ensure its applicability across different visual content. Comprehensive experimental analyses are conducted to assess the algorithm's robustness against multiple types of attacks, including statistical, differential, and brute-force attacks. The results confirm that the IEA effec-

tively disrupts the inherent correlations in image data, ensuring high security. Furthermore, the corresponding decryption algorithm reconstructs the plain image content, demonstrating the algorithm's reliability and lossless recovery capability.

Chapter 5

SHIELD map with application in Image Encryption

This chapter introduces a novel chaotic SHIELD map and demonstrates its application within an IEA. The proposed SHIELD map is formulated by combining the exponential function, sine function, and logistic map. In Section 5.1, we have discussed the background details required for the chapter. The SHIELD map is proposed in Section 5.2. A detailed analysis of the SHIELD map is presented in Section 5.3 in terms of BD, PD, LE, PE, and SE. Section 5.4 proposes the encryption algorithm leveraging the SHIELD map termed as SHIELD-IEA. The SHIELD-IEA utilises chaotic sequences generated by the SHIELD map along with Two-step confusion and Dynamic Diffusion Operation to disrupt plain image. The Two-step confusion operation utilises bit-level shuffling and Fisher-Yates shuffling operation. In Section 5.5, SHIELD-IEA is analysed using several key metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 5.6 summarizes the chapter.

74

5.1 Background

The exponential function is one of the most fundamental nonlinear functions in mathematics, defined as:

$$f(x) = e^x \quad (5.1.1)$$

where $e \approx 2.718$ is Euler's constant. The exponential function is strictly increasing and exhibits rapid growth as x increases. A key property is that small variations in x can lead to disproportionately large differences in $f(x)$, for positive x . This inherent sensitivity directly supports chaotic behaviour by amplifying small deviations in initial conditions.

When applied within bounded transformations such as the modulo operation, the exponential function introduces irregularity and unpredictability in the system's state transitions.

The sine function is defined as:

$$f(x) = \sin(x), \quad (5.1.2)$$

which is a bounded periodic function in range $[-1, 1]$. The oscillatory nature of the sine function introduces smooth fluctuations, allowing the system to alternate between growth and decay in a non-linear manner. Unlike the exponential function, which promotes unbounded divergence, the sine function provides bounded oscillations that enrich the complexity of trajectories without leading to instability that escapes the desired range.

The periodicity of sine function introduces repetitive non-linear modulation. In chaotic system design, this oscillatory modulation contributes to irregular switching behaviours, increases entropy, and strengthens unpredictability in state evolution.

5.2 Proposed SHIELD map

The SHIELD map is non-linear due to the inclusion of an exponential and Sine function along with Logistic map. The inclusion of exponential term introduces rapid growth or decay, while the sine component adds oscillatory behaviour to the map. The inclusion of Logistic map (4.1.2) with other non-linear terms increases the complexity of map. The SHIELD map is given in (5.2.1).

$$\begin{aligned} x_{i+1} &= \text{mod} \left(y_i + \rho x_i e^{\sin(\omega + \mu y_i (1 - y_i)(x_i - y_i))}, 1 \right) \\ y_{i+1} &= \text{mod} \left(x_{i+1} + \mu y_i e^{\sin(\omega + \rho(x_{i+1}^2 - y_i^2))}, 1 \right) \end{aligned} \quad (5.2.1)$$

where μ , ρ , ω are control parameters. The modulo operation ensures that the variables x_{i+1} , and y_{i+1} remain bounded between 0 and 1. The parameters $\omega \in [0, 2\pi]$, $\mu \in [0, \infty)$ and $\rho \in [0, \infty)$ provide flexibility in controlling the map's dynamics. For experimental purposes, the values of μ and ρ are set in the $[0, 10]$ range and $\omega = 1.57$. Depending on their values, the map may transition between different regimes of behaviour, such as stability, periodicity, and chaos.

Furthermore, the analysis of SHIELD is compared with existing maps shown in Table 2.1. The analysis and results are exhibited in the forthcoming sections.

5.3 Analysis of the SHIELD map

The chaotic behavior of the SHIELD is comprehensively investigated by employing a range of tools, including BD to visualize the transition between periodic and chaotic regimes, PD to depict the map's state space trajectories, LE to quantify the rate of divergence of nearby trajectories and confirm chaotic dynamics, PE to measure the complexity of time series based on ordinal patterns, and SE to assess the irregularity and unpredictability of the map's temporal evolution. These tests are performed and the results are discussed in the subsequent sections.

76

5.3.1 Bifurcation diagram

Figure 5.1 exhibits the BD of the SHIELD map with respect to the control parameters μ , ρ , and ω one varying within the interval, while keeping the other parameter fixed and using initial conditions $x_0 = 0.9$ and $y_0 = 0.6$. These diagrams reveal that the SHIELD map exhibits significant ergodicity across a broad range of control parameter values. Furthermore, the BD highlights sensitivity of the SHIELD to variations in its control parameters. Even small changes in parameter values result in different dynamic behavior indicating its suitability for integration into IEAs.

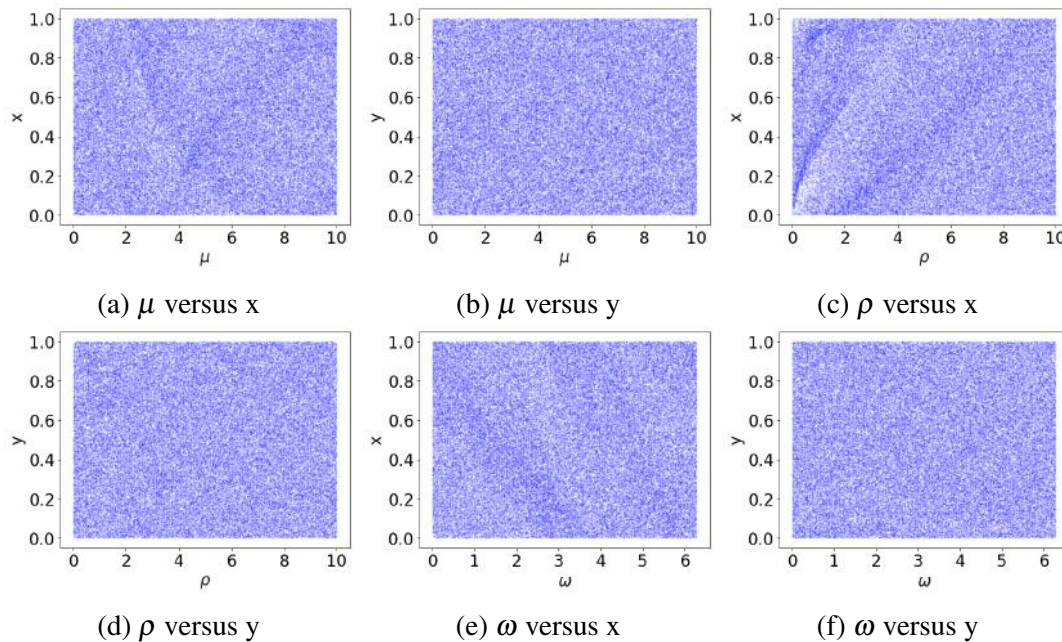


Figure 5.1: Bifurcation diagram of SHIELD map.

5.3.2 Phase diagram

The PD of the SHIELD and other maps, as listed in Table 2.1, are exhibited in Figure 5.2. The PD are plotted using the initial values as: SHIELD $((x_0, y_0, \mu, \rho, \omega) = (0.9, 0.6, 10, 10, 1.57))$, CLM $((x_0, y_0, a, a_1) = (0.5, 0.8, 5, 5))$, ICLM $((x_0, y_0, a, a_1) = (0.3, 0.1, 0.1, 0.1))$, LMHM $((x_0, y_0, \beta, k_1, k_2, \rho_1, k) = (0.5, 0.8, 0.1, 1, 0.1, 100, 0.7))$, IGSCM $((x_0, y_0, r_1, r_2) = (0.21, 0.31, 25, 23.3))$, SLM $((x_0, y_0, \Gamma, p) = (0.3, 0.4, 4, 3.6))$, HSM $((x_0, y_0, b_1, b_2, \omega) = (0.3, 0.6, 5, 1.57, 10))$, LNIC $((x_0, y_0, a, a_1) = (0.9,$

0.6, 1, 1)), CLSS map $((x_0, y_0, c) = (0.3, 0.6, 0.5))$, LCCCM $((x_0, y_0, \mu, p_1) = (0.6, 0.9, 5, 8.78))$. The SHIELD map demonstrates a uniform distribution throughout the region. This indicates that the state trajectories of the SHIELD map do not concentrate in specific regions but are instead evenly dispersed across the entire region. In contrast, the PD of other maps display non-uniform distributions. Thus, it can be inferred that SHIELD map offer enhanced resistance to phase space reconstruction attacks.

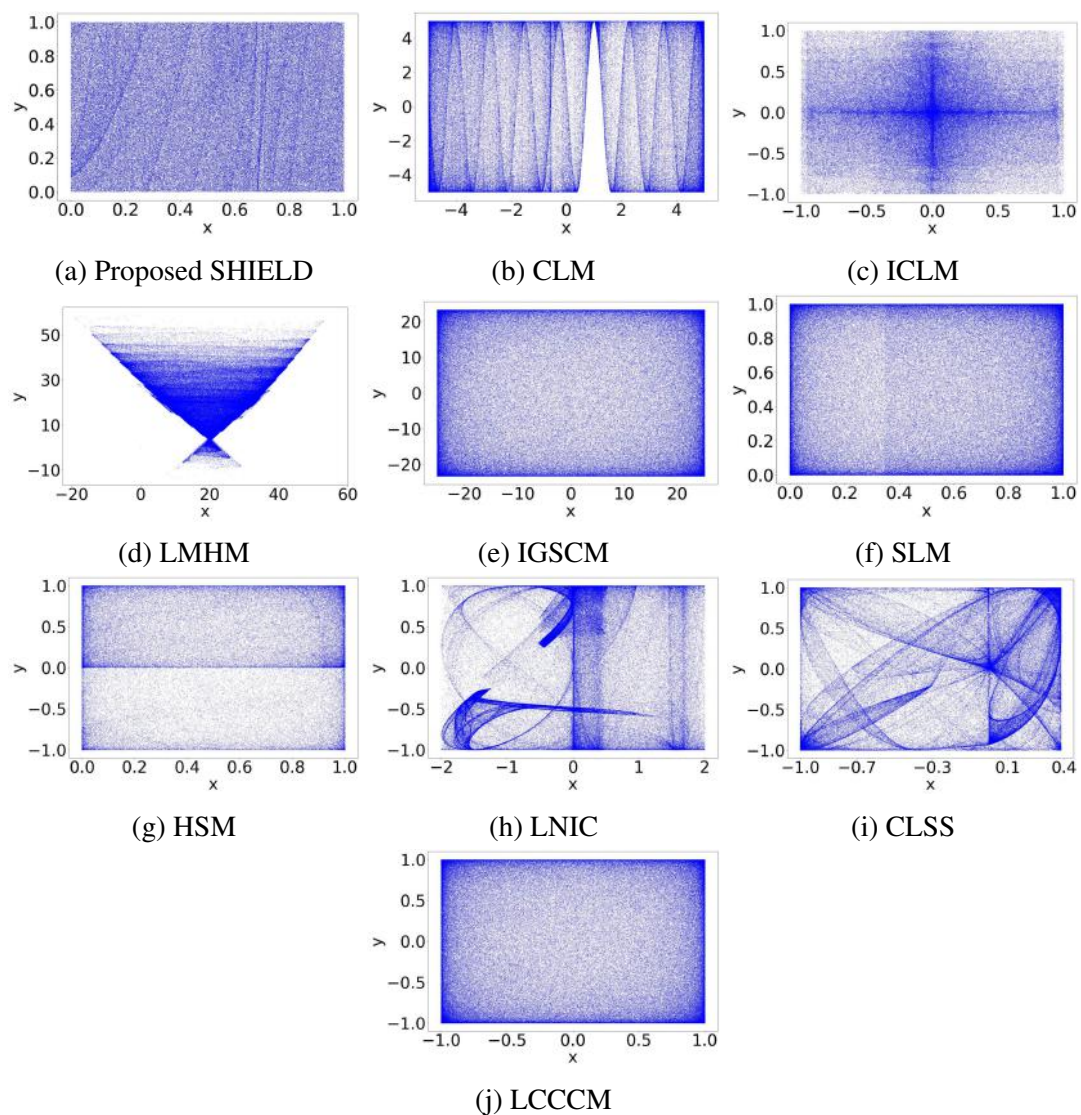


Figure 5.2: Phase diagrams (x and y).

78

5.3.3 Lyapunov exponent

The LE of the SHIELD and other maps, as listed in Table 2.1, are exhibited in Figure 5.3. LE_x and LE_y represent the LEs associated with the x and y variables, respectively. From the Figure 5.3, it is visible that the exponents of SHIELD maps are positive and high as compared to other maps except IGSCM. The larger the LE, the faster this divergence happens. Thus, it can be concluded that the SHIELD map is extremely sensitive to initial conditions, chaotic, unpredictable and hence suitable for integration into IEAs.

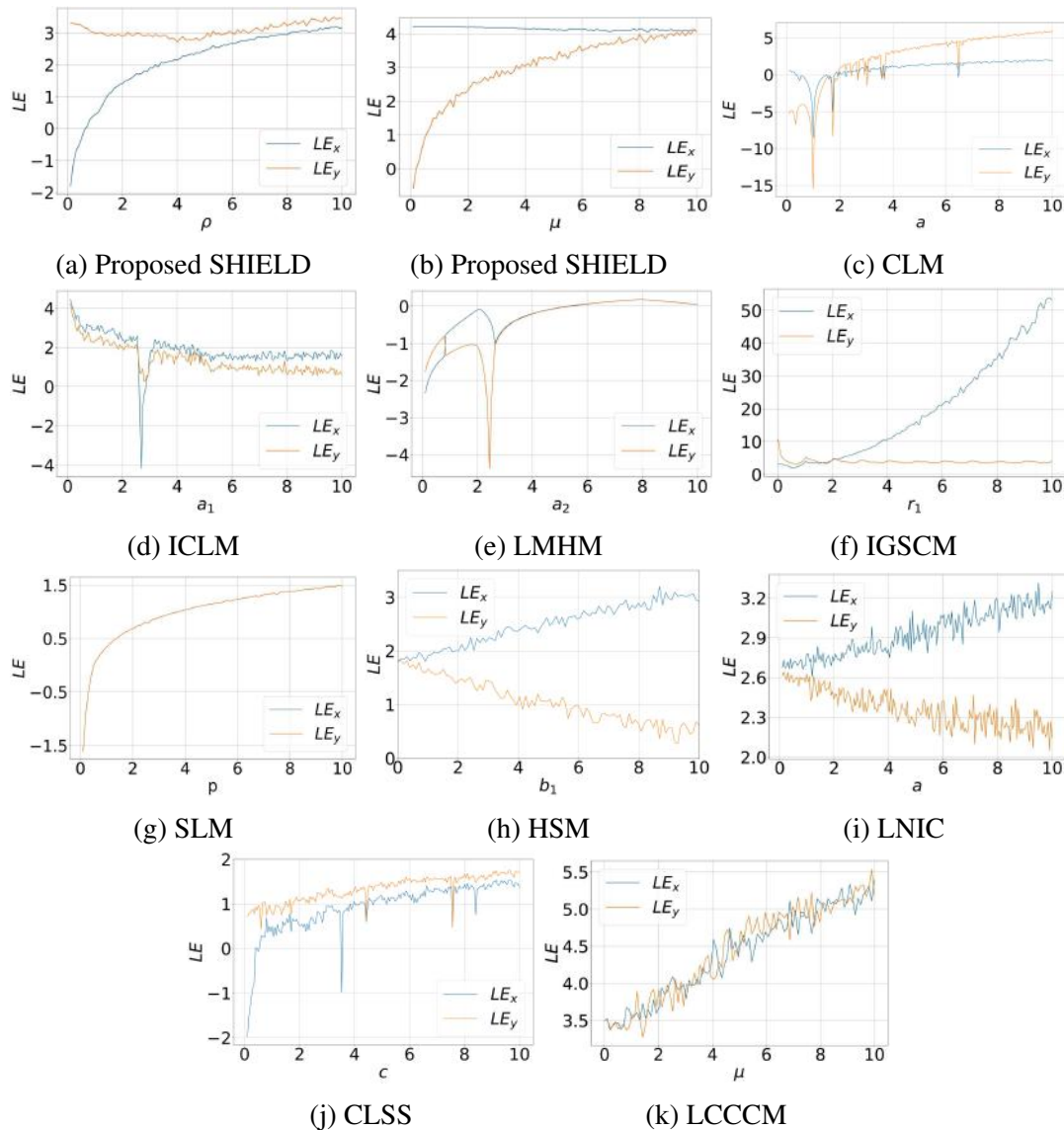


Figure 5.3: Lyapunov exponent spectrum of SHIELD map and other maps. .

5.3.4 Permutation entropy

Figure 5.4 illustrates the PE of the SHIELD map along with other chaotic maps listed in Table 2.1. As shown in the Figure 5.4, the SHIELD map consistently exhibits values near 1 across the specified range of control parameters. This suggests that the SHIELD map demonstrates complex chaotic behavior, making it a strong candidate for applications requiring unpredictability, such as cryptography or secure communications.

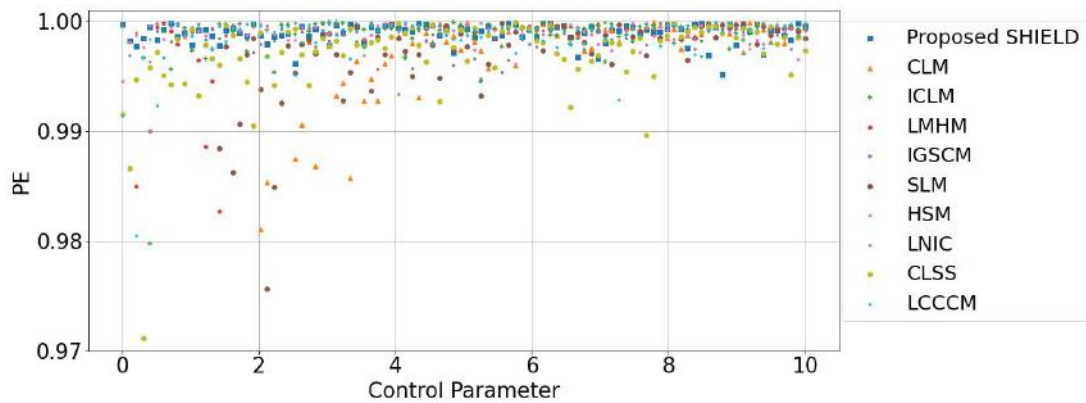


Figure 5.4: Permutation entropy of SHIELD map

5.3.5 Sample entropy

Figure 5.5 shows the SE of the SHIELD map compared to other chaotic maps listed in Table 2.1. As shown in Figure 5.5, the SHIELD map consistently achieves high values of SE around 2 across the evaluated range of control parameters, suggesting that the SHIELD map exhibits pronounced chaotic behavior. Thus the SHIELD map is a strong candidate for applications requiring high unpredictability, including cryptography and secure communications.

5.4 Application of the map in image encryption

This section outlines the SHIELD-IEA for encrypting an image of size $M \times N$. The SHIELD-IEA incorporates several key processes: secret key generation, two-step confusion operation, and dynamic diffusion operations, as described in subsections 5.4.1, 5.4.2 and 5.4.3, respectively. These methods collectively enhance the SHIELD-IEA

80

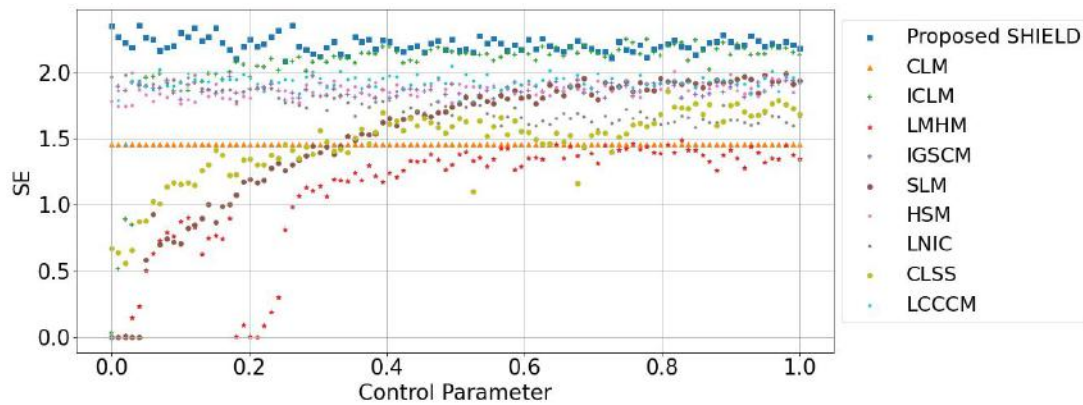


Figure 5.5: Sample entropy of SHIELD map

robustness by ensuring high randomness, reducing predictability, and providing strong resistance against cryptographic attacks.

5.4.1 Secret key generation method

The secret key plays a significant role in the encryption algorithm because it ensures the confidentiality of the data by enabling secure encryption and decryption processes. The algorithm would be vulnerable to attacks without a well-generated and protected key. The secret key K is derived from the plain image using the SHA3-512 hash function. The resulting hash key is converted into a 512-bit binary number which is large enough to resist Brute-Force attacks. These bits are transformed to produce the initial values and control parameters using Algorithm 5.1, which are then used in the SHIELD-IEA.

The outputs of Algorithm 5.1 include $key1$, $key2$, α , and β . The generated keys $key1$ and $key2$ are used as the initial seeds for the SHIELD at different steps of SHIELD-IEA. The parameters α and β are used as initial value in the diffusion process.

5.4.2 Two-step confusion operation

This section outlines the steps involved in the two-step confusion process, which incorporates bit-level shuffling and Fisher-Yates shuffling techniques. The sequences produced by the SHIELD map are modified and applied to scramble the pixel values

Algorithm 5.1: Computation of initial values and parameters for SHIELD-IEA.

Input : Hash value K .

Output: $key1, key2, \alpha, \beta$.

- 1 **Step 1: Convert hash slices to Integers:** $IS_0 \leftarrow bintodec(K_{0:63}),$
 $IS_1 \leftarrow bintodec(K_{64:127}), IS_2 \leftarrow bintodec(K_{128:191}),$
 $IS_3 \leftarrow bintodec(K_{192:255}), IS_4 \leftarrow bintodec(K_{256:319}),$
 $IS_5 \leftarrow bintodec(K_{320:383}), IS_6 \leftarrow bintodec(K_{384:447}),$
 $IS_7 \leftarrow bintodec(K_{448:511});$
 - 2 **Step 2: Compute $key1$ parameters:**
 $[x_0, y_0, \rho, \mu, \omega] = \left[\frac{IS_0}{2^{64}}, \frac{IS_1}{2^{64}}, 100 \times \frac{IS_2}{2^{64}}, 100 \times \frac{IS_3}{2^{64}}, 2\pi \times \frac{IS_1 \oplus IS_3}{2^{64}} \right];$
 - 3 $key1 = [x_{01}, y_{01}, \rho_1, \mu_1, \omega_1]$
 - 4 **Step 3: Compute $key2$ parameters:**
 $[x_0, y_0, \rho, \mu, \omega] = \left[\frac{IS_4}{2^{64}}, \frac{IS_5}{2^{64}}, 100 \times \frac{IS_6}{2^{64}}, 100 \times \frac{IS_7}{2^{64}}, 2\pi \times \frac{IS_5 \oplus IS_7}{2^{64}} \right];$
 - 5 $key2 = [x_{02}, y_{02}, \rho_2, \mu_2, \omega_2]$
 - 6 **Step 4: Compute additional values:** $\alpha = \frac{IS_0 + IS_5}{2^{61}}$
 $\beta = \text{mod} \left(\left\lfloor \frac{IS_1 + IS_6}{2^{30}} \right\rfloor, 256 \right);$
 - 7 **Output:** $key1, key2, \alpha, \beta;$
-

of the image as per the process.

Bit-level shuffling operation

Bit-level shuffling offers enhanced security and data obfuscation by rearranging individual bits in the data-set, making it harder for unauthorized users to detect patterns or extract useful information.

A new bit-level shuffling is proposed in which the bits of the whole sample are shuffled using the sequences obtained by SHIELD map. The proposed bit-level shuffling has greater randomness as it shuffles a larger pool of bits, creating a more complex and less predictable pattern that increases security and obfuscation. In this method, the 8-bit binary representations of the pixel values are concatenated into a single stream of bits. This long stream is then shuffled using the chaotic sequence generated by the SHIELD map. After shuffling, the bits are divided into chunks of 8 to convert them back into individual integers. Furthermore, the flowchart of the operation is exhibited in Figure 5.6.

82

For the bit-level shuffling, two sequences $X1$ and $Y1$ generated by applying $key1$ on the SHIELD map, are combined using (5.4.1).

$$SX_i = 10X1_i + Y1_i, 0 \leq i \leq 8L. \quad (5.4.1)$$

After the modification, the sequence SX is sorted in ascending order. Once the sorting is complete, the corresponding indices associated with the elements of the original sequence are recorded and stored in $S1$. This guarantees that the sequence is organized systematically while also retaining the original positions of each element for reference. The arguments are used to shuffle the bits as described in Algorithm 5.2. The proposed bit-level shuffling disrupts direct associations between input and output bits, making it more challenging for attackers to identify patterns. This method redistributes bits across various positions, hindering correlation predictions and enhancing security and randomness by dispersing the statistical structure. Furthermore, it improves diffusion, ensuring that small input modifications lead to widespread and unpredictable output variations. After bit-level shuffling, the bits are reconstituted into integers and further scrambled using the Fisher-Yates shuffling.

Algorithm 5.2: Bit-Level Shuffling operation.

Input : Plain image (P), $S1$.

Output: Bit-level shuffled image (BSA).

- 1 $M \times N = \text{size}(P)$
 - 2 Convert each byte sample value of image data into a binary stream and store it in bin_image of size $8L$.
 - 3 Initialize $shuff_bin \leftarrow []$
 - 4 **for** $i \leftarrow 0$ **to** $8(M \times N) - 1$ **do**
 - 5 $temp = S1[i]$
 - 6 $shuff_bin[temp] \leftarrow bin_image[i]$
 - 7 **end**
 - 8 Convert the shuffled bit stream $shuff_bin$ of size $8 \times M \times N$ into bytes and store it in BSA of size $M \times N$.
 - 9 **Output** BSA
-

Fisher-Yates shuffling

In 1938, Ronald Fisher and Frank Yates introduced a technique for generating random permutations of finite sets, now known as the Fisher-Yates shuffle [114]. This

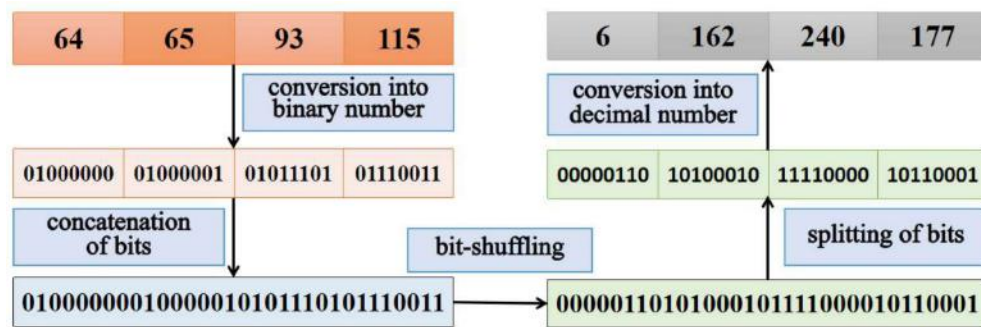


Figure 5.6: Bit-level shuffling operation.

method comprises two variants: the classical and the modern approach. The original Fisher-Yates shuffle is particularly notable for its unbiased nature, ensuring that every permutation is equally likely while requiring only a time complexity proportional to the number of items being shuffled and no additional storage space. The modern version of the Fisher-Yates shuffle, however, refines this concept into an in-place algorithm. Instead of creating a shuffled copy of an array, it rearranges the elements directly within the original array, thereby improving efficiency. Like the classical version, it maintains linear time complexity and avoids the need for extra storage. Nonetheless, the quality of the shuffle in both versions depend on the randomness of index generation process [115].

The image pixels obtained after bit level shuffling operation are reshuffled leveraging Fisher-Yates shuffling. The *key2* is used to iterate the SHIELD, and the obtained sequences are *X2* and *Y2*. The sequence *X2* is sorted and the arguments are stored as *SEQ*. The *SEQ* sequence is used to shuffle the image pixels and the steps are described in Algorithm 5.3. The impact of two-step confusion results in a highly randomized and unpredictable sequence of integers. Bit-level shuffling applied to the entire sample at once, alters the internal structure of each number by rearranging its bits in a randomized manner. This transformation disrupts any inherent numerical patterns, ensuring that even before positional shuffling, the values themselves are significantly altered. Following this, the Fisher-Yates algorithm further randomizes the sequence by shuffling the positions of these transformed integers. The method guarantees maximum entropy within individual numbers while maintaining a uniformly randomized order. It also guarantees that the final data-set exhibits no statistical correlation between the

84

original and shuffled sequences. The obtained shuffled array is used in the diffusion step, as described in next section.

Algorithm 5.3: Fisher-Yates shuffling algorithm.

Input : BSA, SEQ (argument sequence obtained after sorting $X2$)

Output: Shuffled image (SA)

```

1 function Fisher_Yates_Shuffle ( $BSA, SEQ$ )
2  $L \leftarrow \text{size}(BSA)$ 
3 for  $i \leftarrow 0$  to  $M \times N - 1$  do
4    $j \leftarrow SEQ[i];$ 
5   Swap  $BSA[i]$  with  $BSA[j]$ 
6 end
7  $SA \leftarrow BSA$ 
8 Output  $SA$ 

```

5.4.3 Dynamic diffusion operation

The original pixel values of plain image may contain important information that can reveal the underlying content, allowing attackers to reconstruct the image by analysing statistical patterns, even when the pixel value locations are fully rearranged. This vulnerability highlights the need for a robust approach to protect multimedia content from multiple types of statistical attacks. To achieve such security, a strong diffusion operation is required to substantially modify the pixel values. Diffusion operation ensures that changing even a small part of the plaintext results in a significant and widespread change in the ciphertext.

The proposed dynamic diffusion operation ensures strong security through its complexity. The algorithm involves improved sine-tangent map [116], recursive structure, and modular arithmetic. The improved sine-tangent map adds another layer of security to the IEA as it enhances the sensitivity to initial conditions (control parameters). Its sensitivity to initial conditions ensures that small changes in inputs lead to different results. The recursive structure, where each value depends on the previous one, adds an extra layer of protection by making it harder for attackers to isolate individual values. The $\text{mod}(\bullet, 256)$ operation restricts the output to $[0, 255]$. Overall, this makes the algorithm resistant to several attacks and well-suited for applications requiring unpre-

dictability. The diffusion operation is described in (5.4.2).

$$C_i = \begin{cases} SA_0 \oplus SY_0 \oplus \text{mod} \left(\left\lfloor 10^{10} \times \sin \left(\alpha \times \tan \left(3 \times \left(\frac{\beta}{255} \right)^2 - 1.5 \right) \right) \right\rfloor, 256 \right), & i = 0; \\ SA_i \oplus SY_i \oplus \text{mod} \left(\left\lfloor 10^{10} \times \sin \left(\alpha \times \tan \left(3 \times \left(\frac{CA_{i-1}}{255} \right)^2 - 1.5 \right) \right) \right\rfloor, 256 \right), & 1 \leq i \leq (M \times N - 1). \end{cases} \quad (5.4.2)$$

where SA , SY , and C represent shuffled image, chaotic sequence, and cipher image. $\lfloor \bullet \rfloor$ and \oplus represent floor and bit-wise XOR operation, respectively. The sequence SY is obtained by modifying $Y2$ using (5.4.3).

$$SY_i = \text{mod} (\lfloor Y2_i \times 10^5 \rfloor, 256), 0 \leq i \leq (M \times N - 1) \quad (5.4.3)$$

This SHIELD-IEA ensures the redistribution of pixel values so that correlations between adjacent image pixels are eliminated, enhancing the overall security of an encrypted image. By doing so, the encrypted output is significantly more resistant to cryptanalysis and reverse engineering attempts, preserving the confidentiality of the multimedia content.

The steps of SHIELD-IEA are described as follows:

1. Insert the plain image P of size $M \times N$.
2. Calculate the hash value K of the P using the hash function SHA3-512.
3. Insert the hash value K in the Algorithm 5.1 to get the required initial values and control parameters for the SHIELD-IEA ($key1$, $key2$, α , β).
4. The SHIELD is iterated using $key1$. The sequences obtained are $X1$ and $Y1$. These are modified for bit-level shuffling, and $S1$ is obtained.
5. The P and $S1$ is inserted into Algorithm 5.2 and the BSA is obtained.
6. The SHIELD is iterated again using $key2$. The sequences obtained are $X2$ and $Y2$.
7. $X2$ is sorted and output stored as SEQ and BSA are inserted into Algorithm 5.3 to accomplish Fisher-Yates shuffling.

86

8. Diffuse the obtained image in Step 7 using the diffusion operation given in (5.4.2). C is the obtained cipher image of size $M \times N$.

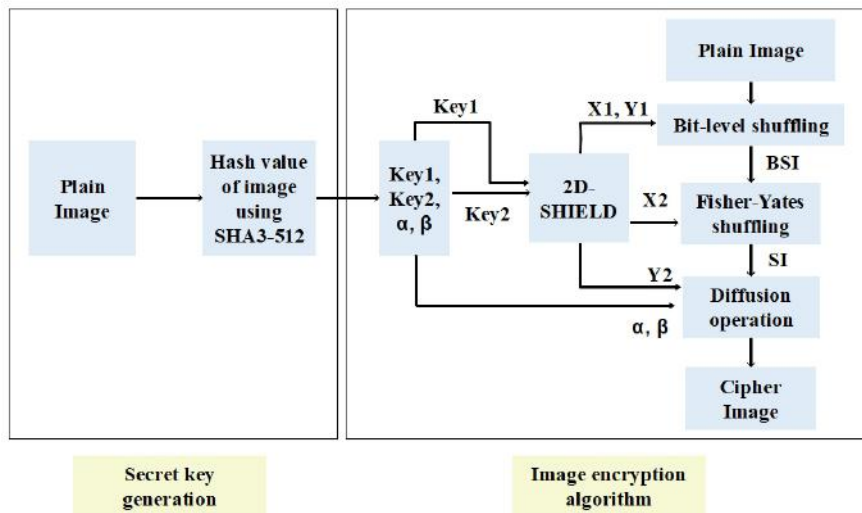


Figure 5.7: Image encryption algorithm (SHIELD-IEA).

Since the proposed SHIELD-IEA is symmetric, it uses the same key in the encryption and decryption operations. As encryption and decryption processes are inherently reversible, the decryption process entails executing the inverse operations of the encryption process.

5.5 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed SHIELD-IEA, we performed a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and resilience are compared to various algorithms regarding information entropy, NPCR, UACI, correlation coefficient, execution time.

5.5.1 Information entropy analysis

Table 5.1 presents the information entropy values of cipher images generated by the proposed SHIELD-IEA and other existing algorithms. The entropy values for images encrypted using SHIELD-IEA are consistently close to the ideal value, which

indicates a high level of randomness. This suggests that the SHIELD-IEA effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it makes it significantly more difficult for an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the SHIELD-IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the plain image content.

Table 5.1: Comparison of information entropy values of the SHIELD-IEA with algorithms available in the literature.

Image	SHIELD-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9993	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9993	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9970	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9998	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9998	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9998	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9998	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9998	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9993	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9977	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9993	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9993	7.9992	7.9992	7.9992	7.9991
bridge256	7.9967	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9993	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9971	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9993	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

5.5.2 Differential attack

Table 5.2 and Table 5.3 present a comparative analysis of NPCR and UACI values for various encrypted images using different IEAs. The results clearly demonstrate that the proposed SHIELD-IEA consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related IEAs often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the SHIELD-IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that SHIELD-IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

5.5.3 Histogram analysis

Figure 5.8 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining Figure 5.8, it becomes clear that a significant transfor-

88

Table 5.2: Comparison of NPCR values of SHIELD-IEA with algorithms available in the literature.

Image	SHIELD-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.6140	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.6021	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.5941	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6092	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6005	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.6165	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6140	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.6078	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.6174	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.5941	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.6059	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6216	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.6189	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.5743	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.5834	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

Table 5.3: Comparison of UACI values of the SHIELD-IEA with algorithms available in the literature.

Image	SHIELD-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.5615	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.4316	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.4612	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.4782	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4598	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.5060	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.5078	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.4628	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.5276	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.4155	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.5434	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.4063	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.4482	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.3902	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.4330	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

mation occurs in the statistical distribution of pixel intensities following the IEA. In the case of the plain images, the histograms typically display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 5.8(a-c)). These patterns can often reveal information about the image content, making plain images vulnerable to statistical analysis and attacks.

The histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the IEA has effectively randomized the pixel values across the entire grayscale range (Figure 5.8(d-f)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the cipher image histograms confirms that the IEA has successfully obscured the plain image information. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

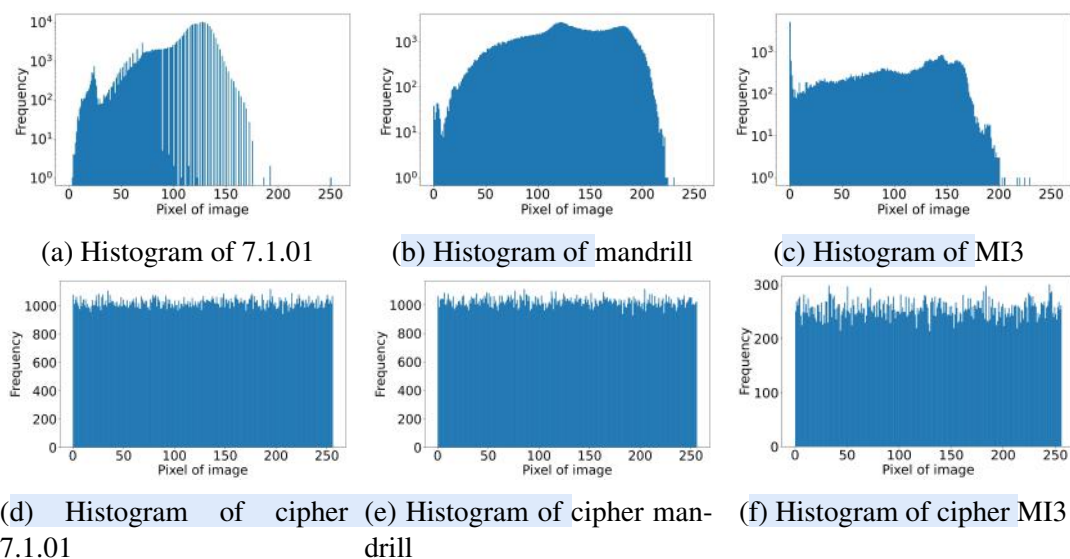


Figure 5.8: Histogram of plain and cipher images

5.5.4 Correlation Coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 5.4. As observed from the Table 5.4, the plain images exhibit very high correlation coefficients, with values close

90

to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the encryption process has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of the IEA in reducing statistical information.

In addition, the pixel intensity distribution is illustrated in Figure 5.9. For the plain images shown in Figure 5.9(a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 5.9(d-f), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

Table 5.4: Comparison of correlation coefficient values of SHIELD-IEA with algorithms available in the literature.

Image	Plain images	SHIELD-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	HD 0.9630	0.0008	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD 0.9192	-0.0047	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD 0.8995	-0.0032	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD 0.8625	0.0031	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD 0.7669	0.0093	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD 0.7202	0.0031	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD 0.9784	0.0102	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD 0.9795	-0.0032	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD 0.9405	-0.0043	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085

5.5.5 Resistance to classical attacks

The robustness of proposed SHIELD-IEA against chosen-plaintext attacks is established through Equation (2.3.8). This operation is visually represented in Figure 5.10. By examining Figure 5.10(a),(b), it is clear that (2.3.8) holds, suggesting that the SHIELD-IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 5.10(a) and Figure 5.10(b). The resulting NPCR value between these two images is 99.6127%, further reinforcing the SHIELD-IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed SHIELD-IEA is also expected to be resilient against other classical attacks.

10

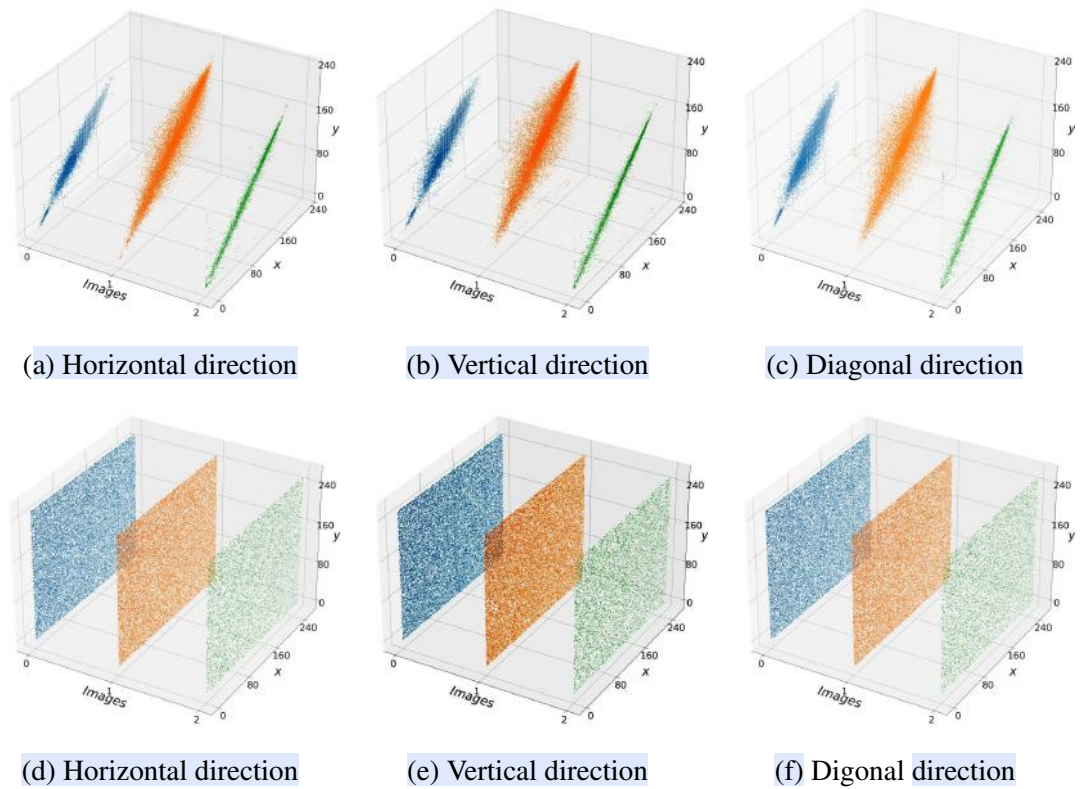


Figure 5.9: Pixel distribution of plain and cipher images obtained using SHIELD-IEA.

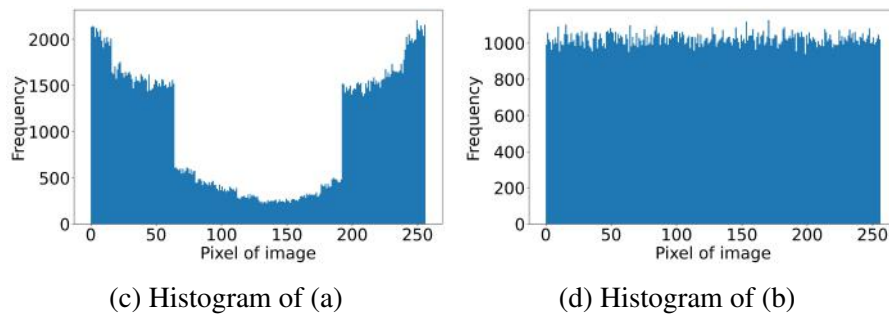
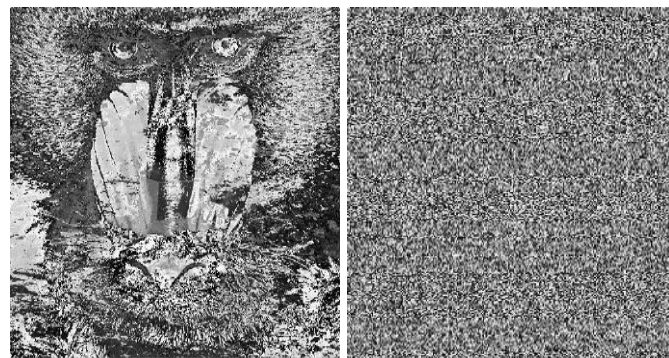
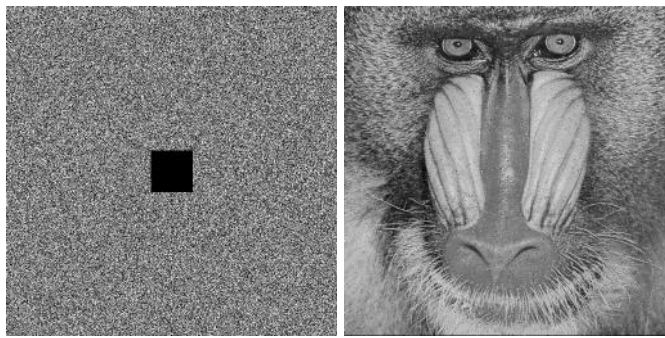


Figure 5.10: Resistance to classical attacks



(a) Cropped encrypted image (b) Decryption of cropped image

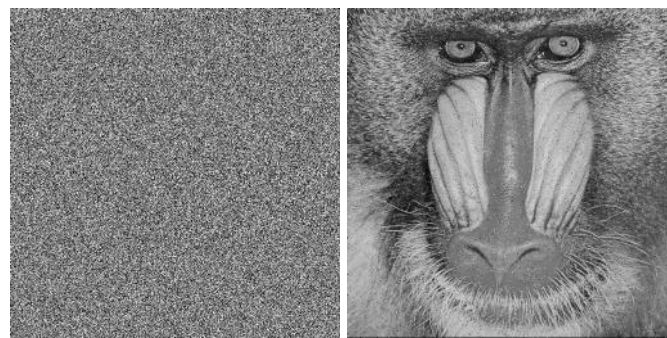
Figure 5.11: Representation of SHIELD-IEA's resistance to cropping attack

5.5.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in Figure 5.11(a). The corresponding decrypted image of the occluded images is shown in the Figure 5.11(b). The decrypted image retains most of the original visual content, indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that the SHIELD-IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.

5.5.7 Noise attack

To assess the resilience of the decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 5.12(a), while the corresponding decrypted image is shown in Figure 5.12(b). Despite the presence of noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption scheme can effectively tolerate such distortions. These results confirm that the SHIELD-IEA is robust against noise attacks and suitable for secure image transmission over noisy communication channels.



(a) Noisy encrypted image (b) Decryption of noisy image

Figure 5.12: Representation of SHIELD-IEA's resistance to Noise attack

5.5.8 NIST randomness test

Table 5.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the SHIELD-IEA. As shown in the Table 5.5, the cipher image successfully passes all the randomness tests, indicating that the SHIELD-IEA effectively introduces randomness in the encrypted images.

Table 5.5: Randomness test results for SHIELD-IEA.

Test name	p-value	Result
Frequency Test	0.8274	Successful
Run Test	0.7054	Successful
Run Test (Longest Run of Ones)	0.9357	Successful
Block Frequency Test	0.3088	Successful
Universal Statistical Test	0.8083	Successful
Linear Complexity Test	0.1872	Successful
Serial Test	0.8531	Successful
Binary Matrix Rank Test	0.4353	Successful
Non-overlapping Template Matching Test	0.6616	Successful
Overlapping Template Matching Test	0.6069	Successful
Approximate Entropy Test	0.6922	Successful
Random Excursion Test	0.5969	Successful
Random Excursion Variant Test	0.3750	Successful
Cumulative Sums	0.8411	Successful
Discrete Fourier Transform Test	0.2188	Successful

5.5.9 Execution time analysis

The execution time of the proposed IEA and other IEAs available in literature is presented in Table 5.6. The execution time for SHIELD-IEA is comparatively higher than that of IEAs available in literature [60, 46, 59, 82, 33, 86, 87, 88], it offers enhanced robustness and superior security features. This trade-off between time and performance indicates that while SHIELD-IEA may require more processing time, it compensates with greater resilience against several attacks.

Table 5.6: Comparison of execution time (in seconds) of the SHIELD-IEA with algorithms available in the literature.

Image	SHIELD-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	13.95	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	14.44	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	3.46	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

5.6 Summary

This chapter proposes chaotic SHIELD map to overcome the limitations of the maps available in literature. The analysis exhibits that the SHIELD map possesses wide chaotic range of control parameter, uniform output distribution, positive and high LEs, along with high sample and PE values. The proposed map is integrated into an IEA along with the two-step confusion and dynamic diffusion operation. The performance of the proposed SHIELD-IEA is rigorously evaluated using a diverse set of gray-scale images to ensure its applicability across different visual content. Comprehensive experimental analyses are conducted to assess the algorithm's robustness against multiple types of attacks, including statistical, differential, and brute-force. The results confirm that the IEA effectively disrupts the inherent correlations in image data, ensuring high security. Furthermore, the corresponding decryption algorithm reconstructs the plain image content, demonstrating the algorithm's reliability and lossless recovery capability.

Chapter 6

Modified chaotic maps with application in Image Encryption

In this chapter, we propose two IEAs constructed using modified chaotic maps. These maps are derived from the existing $e\pi$ map [33]. The proposed maps are named the 2D Sine $e\pi$ map (SEPM) and 3D Non-linear Sine hyper-chaotic map (NLS). Section 6.1 describes the background required for the chapter. In Section 6.2, SEPM and NLS are discussed. The analysis of proposed modified maps is presented in Section 6.3 in terms of BD, PD, LE, PE, and SE. Section 6.4 proposes the encryption algorithms utilising modified maps. In Section 6.5, we have discussed the analysis of the IEA utilising metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 6.6 summarizes the chapter.

6.1 Background

This section delves into the details of the existing $e\pi$ map and the fractal sorting matrix (FSM). In addition, the generation of higher order FSM is exhibited using an example.

6.1.1 $e\pi$ map

In 2022, Erkan et al. introduced a 2D chaotic map, referred to as the $e\pi$ map [33]. The map was designed to generate sequences with strong chaotic properties, which are crucial for applications such as image encryption and secure communications. The map used e and π numbers, both of which are transcendental and irrational. These constants are well known for their non-repeating decimal expansions, making them excellent candidates for enhancing the diversity and complexity of chaotic maps. The $e\pi$ map is given in (6.1.1).

$$\begin{aligned} x_{i+1} &= \text{mod}(x_i^{\pi^3} e^4 + u e^{10} y_i, 1) \\ y_{i+1} &= \text{mod}(y_i^{\pi^3} e^4 + u \pi^9 x_{i+1}^2, 1) \end{aligned} \quad (6.1.1)$$

Here, x_i and y_i represent the i^{th} state variables, u is a control parameter that influences the behavior of map, and the modulo operation ensures that the outputs x_{i+1} and y_{i+1} remain within the interval $[0,1)$. The map involve high-order powers of π and e , which significantly amplify the non-linearity and sensitivity to initial conditions of the map.

6.1.2 Fractal Sorting Matrix

Definition 6.1.1. Sorting Matrix: Consider the elements of a matrix \mathbf{A} which are positive integers from the set $\{1, 2, \dots, N^2\}$, and the elements of \mathbf{A} at any two different positions are different. The matrix \mathbf{A} is called a sorting matrix.

Definition 6.1.2. Consider the matrix \mathbf{A} that satisfies the following properties:

1. The elements within matrix \mathbf{A} exhibit variation, spanning from small to large or vice-versa in an irregular manner.
2. The order of the elements in matrix \mathbf{A} has a self-similar form.
3. \mathbf{A} can be produced by iteration, and an infinite matrix \mathbf{A} can be produced through an infinite number of iterations.

Then, \mathbf{A} is called the FSM [82].

According to Definition 6.1.2, a class of FSM construction method with the base of a square matrix is described. The formula used to iterate the matrix is given in (6.1.2).

$$\begin{aligned} \mathbf{A}_0^n &= [\mathbf{A}_{i,j}^n] \\ \mathbf{A}_{i,j}^n &= (2^{2n} + 1)^{-1} \times \mathbf{A}^{n-1} + \mathbf{A}^{n-1}(i, j) \end{aligned} \quad (6.1.2)$$

where $\mathbf{A}_{i,j}^n$ represents the sub-block at the i^{th} row and j^{th} column of \mathbf{A}^n , and $\mathbf{A}^{n-1}(i, j)$ represents the element at i^{th} row and j^{th} column of \mathbf{A}^{n-1} .

We take a square matrix of order two, $\mathbf{A}^1 \in \mathbb{R}^{2 \times 2}$, consisting of elements 1, 2, 3 and 4. To obtain FSM \mathbf{A}^* , the steps are as given below .

1. $\mathbf{A}_0^2 \in \mathbb{R}^{4 \times 4}$ is a 4-order square matrix obtained by iterating over \mathbf{A}^1 with formula given in (6.1.2).

$$\mathbf{A}_0^2 = \begin{bmatrix} \mathbf{A}_{1,1}^2 & \mathbf{A}_{1,2}^2 \\ \mathbf{A}_{2,1}^2 & \mathbf{A}_{2,2}^2 \end{bmatrix} \quad (6.1.3)$$

2. We can obtain the FSM by sorting the matrix \mathbf{A}_0^2 from small to large as follows:

$$\mathbf{A}^2 = \text{order}(\mathbf{A}_0^2) \quad (6.1.4)$$

where $\text{order}(\bullet)$ is a function to sort the matrix from small to large according to the elements of the matrix.

3. $\mathbf{A}_0^n \in \mathbb{R}^{2^n \times 2^n}$ is a square matrix obtained by iterating over $\mathbf{A}^{n-1} \in \mathbb{R}^{2^{n-1} \times 2^{n-1}}$ with formula given in (6.1.2).

$$\mathbf{A}_0^n = \begin{bmatrix} \mathbf{A}_{1,1}^n & \mathbf{A}_{1,2}^n & \cdots & \mathbf{A}_{1,2^n}^n \\ \mathbf{A}_{2,1}^n & \mathbf{A}_{2,2}^n & \cdots & \mathbf{A}_{2,2^n}^n \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{2^n,1}^n & \mathbf{A}_{2^n,2}^n & \cdots & \mathbf{A}_{2^n,2^n}^n \end{bmatrix} \quad (6.1.5)$$

4. Similar to the step 2, we obtain \mathbf{A}^n as follows:

$$\mathbf{A}^n = \text{order}(\mathbf{A}_0^n) \quad (6.1.6)$$

98

Through the above steps, we can obtain the FSM $A^* = A^n$, combined with actual needs and the appropriate number of iterations.

To explain the definition of the FSM, we give an example as follows.

Example Construct the initial matrix as follows:

$$A^1 = \begin{bmatrix} 3 & 1 \\ 2 & 4 \end{bmatrix} \quad (6.1.7)$$

and applying the iterative steps given above, the FSM can be obtained as follows:

$$A^2 = \begin{bmatrix} 11 & 9 & 3 & 1 \\ 10 & 12 & 2 & 4 \\ 7 & 5 & 15 & 13 \\ 6 & 8 & 14 & 16 \end{bmatrix} \quad (6.1.8)$$

$$A^3 = \begin{bmatrix} 43 & 41 & 35 & 33 & 11 & 9 & 3 & 1 \\ 42 & 44 & 34 & 36 & 10 & 12 & 2 & 4 \\ 39 & 37 & 47 & 45 & 7 & 5 & 15 & 13 \\ 38 & 40 & 46 & 48 & 6 & 8 & 14 & 16 \\ 27 & 25 & 19 & 17 & 59 & 57 & 51 & 49 \\ 26 & 28 & 18 & 20 & 58 & 60 & 50 & 52 \\ 23 & 21 & 31 & 29 & 55 & 53 & 63 & 61 \\ 22 & 24 & 30 & 32 & 54 & 56 & 62 & 64 \end{bmatrix} \quad (6.1.9)$$

As shown in Example, the elements in the FSM produced by iteration are irregularly ordered and self-similar. By iterating A^1 once, we can obtain an FSM A^2 , whose top-left block with size 2×2 of A^2 is iterated from the element '3' at position (1,1) in A^1 , bottom-left block from '2', top-right block from '1' and bottom-right block from '4'. By iterating twice, we can obtain an FSM A^3 . We can intuitively see that the size of the matrix increases as the iteration number increases.

6.2 Proposed Sine $e\pi$ map and Non-Linear Sine hyper-chaotic map

In this section, we have described the modified SEPM and NLS. Since these formulations are developed using Euler number e and π , we have used the numerical values of the e and π , rounded up to 4 decimal digits.

6.2.1 Sine $e\pi$ map

The map is constructed using existing $e\pi$ map and transcendental functions. The non-linearity is further amplified by the use of irrational exponents like π^3 and e^{10} , which contribute to rapid state divergence and sensitive dependence on initial conditions. The SEPM is a 2D discrete-time, and hyper-chaotic dynamical map that demonstrates complex and unpredictable behavior across a broad range of the control parameter $u \in (0, \infty)$. The map is given in (6.2.1).

$$\begin{aligned} x_{i+1} &= \text{mod} (x_i^{\pi^3} e^4 - u^2 e^{10} y_i \sin(x_i), 1) \\ y_{i+1} &= \text{mod} (y_i^{\pi^3} e^4 - u^2 \pi^9 x_{i+1}^2, 1) \end{aligned} \quad (6.2.1)$$

where, x_i and y_i are i^{th} terms of the sequence, and $u \in (0, \infty)$ is control parameter. The operation $\text{mod } 1$ ensures that all values are constrained to the interval $[0,1)$, introducing discontinuity and boundedness.

6.2.2 Non-Linear Sine hyper-chaotic Map

The NLS is pseudo-random, non-periodic, and exhibits complex chaotic behaviour. In order to include a good amount of non-linearity, we integrated the trigonometric function along with the irrational constants, i.e., π and e . Further, to obtain the bound-

100

edness, the mod 1 operation is utilized. The map is given in (6.2.2).

$$\begin{aligned}x_{i+1} &= \text{mod} (e^4 x_i^{\pi^3} + e^9 u^2 y_i \sin x_i, 1) \\y_{i+1} &= \text{mod} (\pi^9 u^2 x_{i+1}^2 + e^4 y_i^{\pi^3} + u^2 z_i, 1) \\z_{i+1} &= \text{mod} (\pi^9 u^2 \sin x_{i+1} + e^9 z_i^{\pi^3}, 1)\end{aligned}\tag{6.2.2}$$

where $p = e^9$, $q = e^4$, $r = \pi^9$, $s = \pi^3$ and, u is control parameter that can take values in the range $(0, \infty)$.

6.3 Analysis of Sine $e\pi$ map and Non-Linear Sine hyper-chaotic Map

This section discusses the chaotic dynamics of the proposed SEPM and NLS maps.

6.3.1 Bifurcation diagram

Figure 6.1 illustrate the BD of SEPM with respect to the control parameter u and using initial conditions $x_0 = 0.3$ and $y_0 = 0.6$.

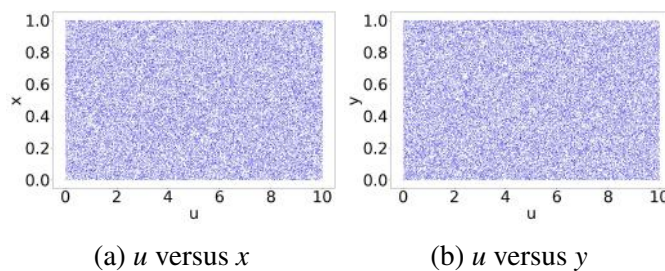


Figure 6.1: Bifurcation diagram of SEPM map.

Figure 6.2 illustrate the BD of the NLS with respect to the control parameter u and using initial conditions $x_0 = 0.3$, $y_0 = 0.4$, and $z_0 = 0.9$.

These diagrams reveal that both the maps exhibits significant ergodicity across a broad range of control parameter values. Furthermore, the BD highlight the high sensitivity of the maps to variations in its control parameters. Even small changes in u result in different chaotic regimes. This high sensitivity and complex dynamical be-

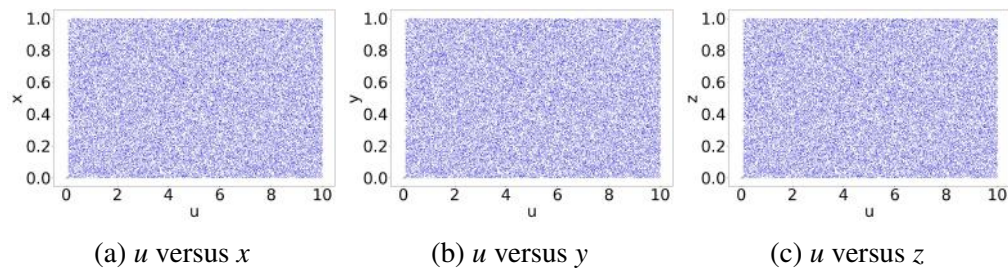


Figure 6.2: Bifurcation diagram of NLS map.

havior make the map particularly well-suited for integration into IEAs.

6.3.2 Phase diagram

The PD of the SEPM, NLS and other maps, as listed in Table 2.1, are exhibited in Figure 6.3. The PD are plotted using the initial values as SEPM $((x_0, y_0, u) = (0.3, 0.6, 0.4))$, NLS $((x_0, y_0, z_0, u) = (0.3, 0.4, 0.9, 0.8))$, CLM $((x_0, y_0, a, a_1) = (0.5, 0.8, 5, 5))$, ICLM $((x_0, y_0, a, a_1) = (0.3, 0.1, 0.1, 0.1))$, LMHM $((x_0, y_0, \beta, k_1, k_2, \rho_1, k) = (0.5, 0.8, 0.1, 1, 0.1, 100, 0.7))$, IGSCM $((x_0, y_0, r_1, r_2) = (0.21, 0.31, 25, 23.3))$, SLM $((x_0, y_0, \Gamma, p) = (0.3, 0.4, 4, 3.6))$, HSM $((x_0, y_0, b_1, b_2, \omega) = (0.3, 0.6, 5, 1.57, 10))$, LNIC $((x_0, y_0, a, a_1) = (0.9, 0.6, 1, 1))$, CLSS map $((x_0, y_0, c) = (0.3, 0.6, 0.5))$, LCCCM $((x_0, y_0, \mu, p_1) = (0.6, 0.9, 5, 8.78))$. The proposed map's PD demonstrates a uniform distribution throughout the region. This indicates that the state trajectories of the proposed maps do not concentrate in specific regions but are instead evenly dispersed across the entire region. In contrast, the PD of other maps display non-uniform distributions. Thus it can be inferred that proposed maps offer enhanced resistance to phase space reconstruction attacks.

6.3.3 Lyapunov exponent

The LE of the SEPM, NLS and other maps, as listed in Table 2.1, are exhibited in Figure 6.4. LE_x and LE_y represent the LEs associated with the x and y variables, respectively. From the Figure 6.4, it is visible that the LEs of SEPM and NLS maps are positive and high as compared to other maps. Thus it can be concluded that the maps are extremely sensitive to initial conditions. The larger the LE, the faster this

102

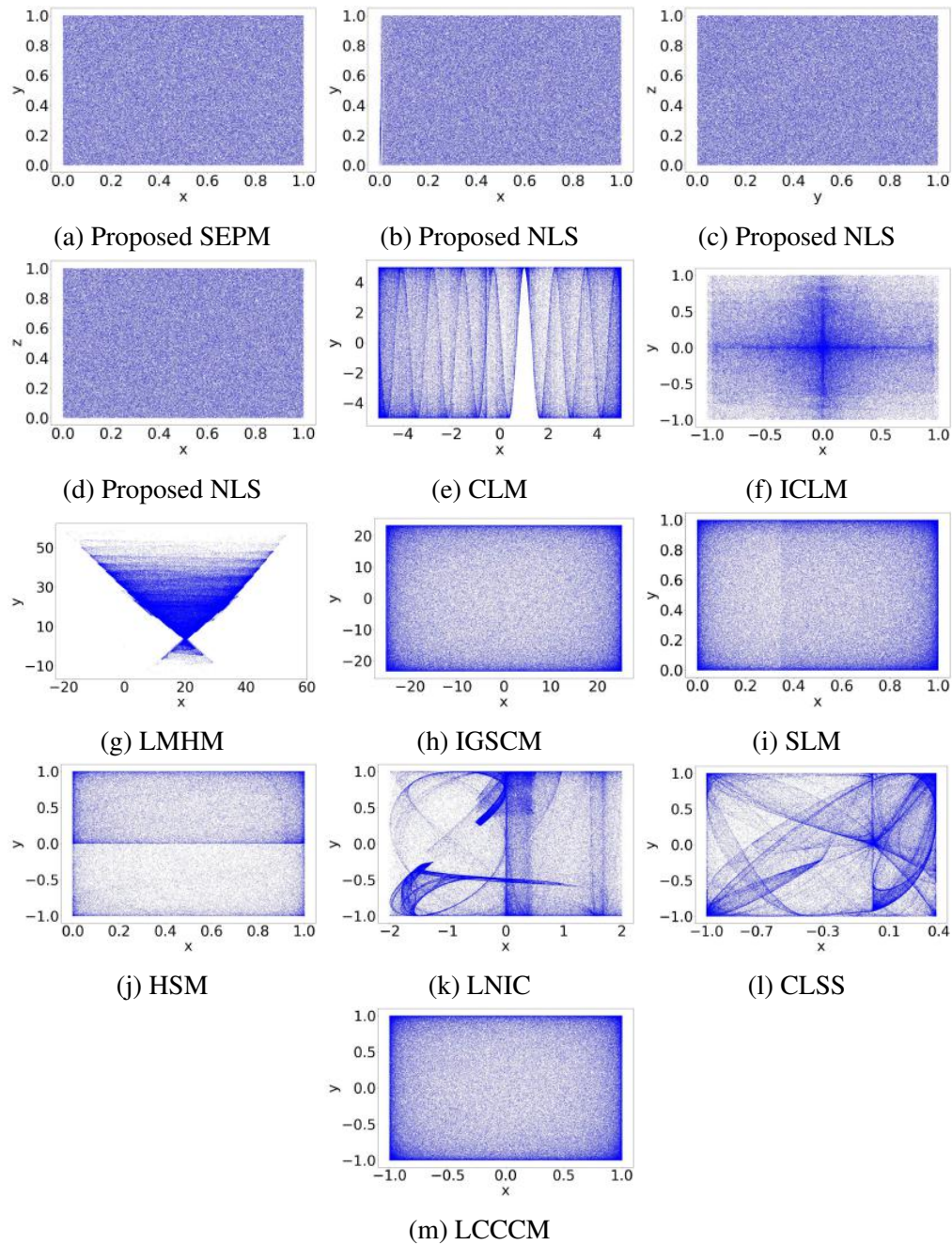


Figure 6.3: Phase diagrams (x and y).

divergence happens. Thus, a high positive LE is a hallmark of chaotic, complex, and unpredictable behavior suggesting its suitability for integration into IEAs.

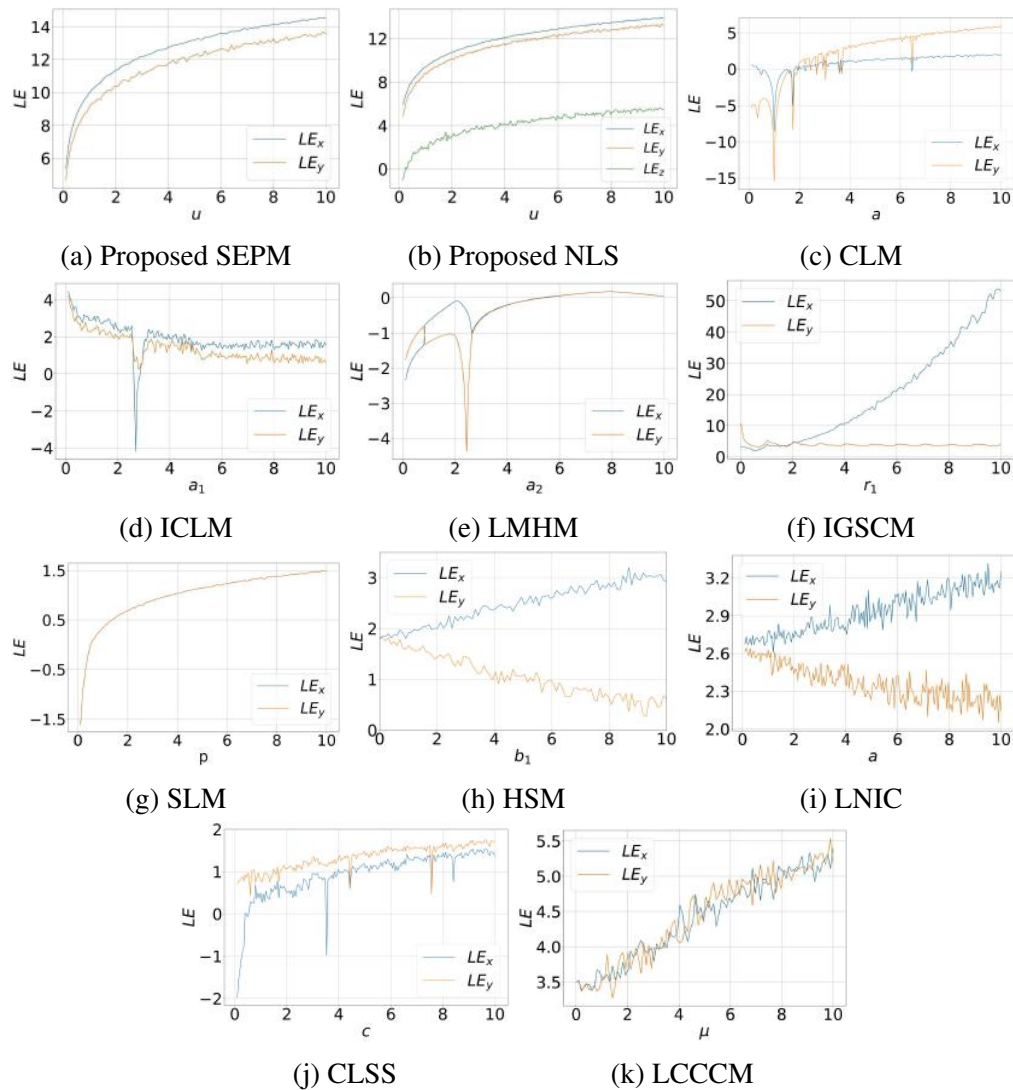


Figure 6.4: Lyapunov exponent diagram of SEPM, NLS and others maps.

6.3.4 Permutation entropy

Figure 6.5 illustrates the PE of SEPM, NLS alongside other chaotic maps listed in Table 2.1. As shown in the Figure 6.5, the SEPM and NLS consistently exhibit values near 1 across the specified range of control parameters. This suggests that the SEPM and NLS demonstrates highly complex or chaotic behavior, making it a strong candidate for applications requiring randomness or unpredictability, such as cryptography

104

or secure communications.

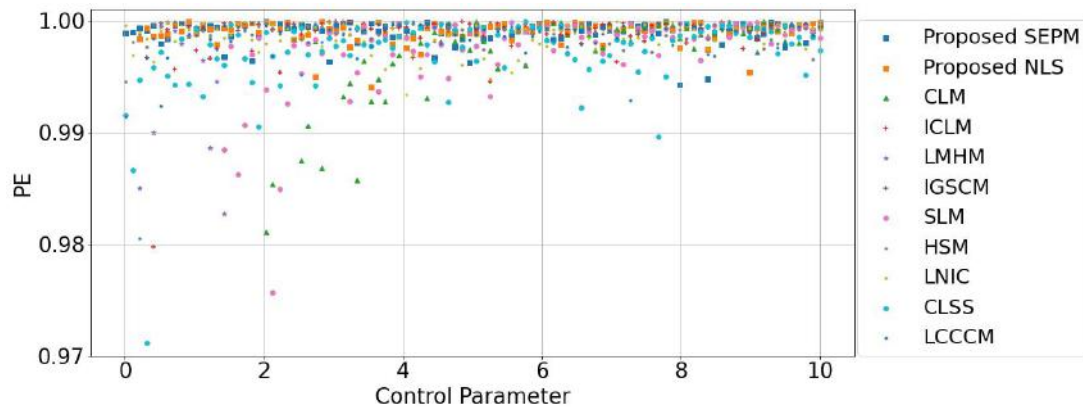


Figure 6.5: Permutation entropy of SEPM and NLS map.

6.3.5 Sample entropy

Figure 6.6 shows the SE of the SEPM and NLS compared to other chaotic maps listed in Table 2.1. As shown in Figure 6.6, the SEPM and NLS consistently achieves high values of SE around 2.5 across the evaluated range of control parameters, suggesting that the SEPM and NLS exhibits pronounced chaotic behavior. Thus, SEPM and NLS maps are a strong candidate for applications requiring high unpredictability, including cryptography and secure communications.

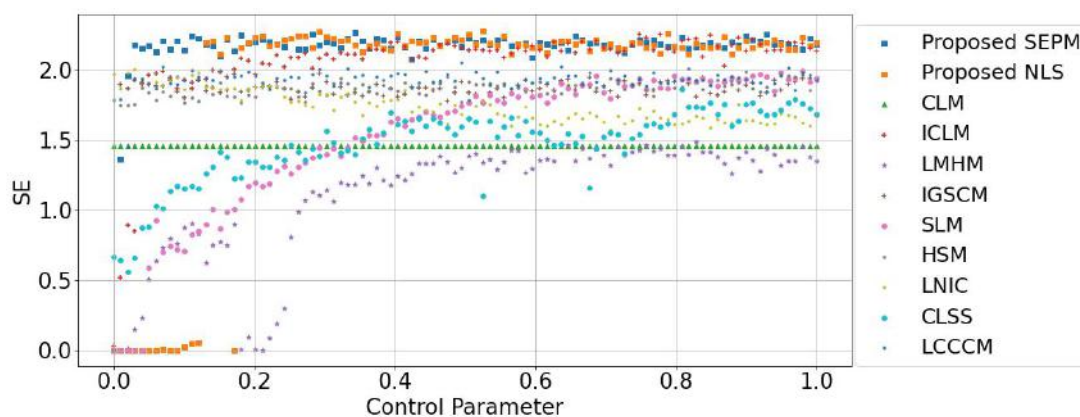


Figure 6.6: Sample entropy of SEPM and NLS map.

6.4 Application of maps in image encryption

This section presents the IEAs developed using the proposed chaotic maps SEPM and NLS. The IEA constructed with SEPM is termed as SEPM-IEA, whereas the one constructed with NLS is termed as NLS-IEA. The algorithms, driven by the chaotic sequences generated from the respective maps, are thoroughly elaborated to highlight their structure and contribution to the overall security of the IEAs. The IEA utilises maps along with FSM, and “Bit separation”.

The encryption process developed is applied to plain images P of size $M \times N$. We have obtained the hash value for the plain image P using the SHA3-256 algorithm that gives a hash string K consisting of 64 hexadecimal characters. The key is large enough to resist brute-force attacks. The string K is divided into four parts, each having 16 hexadecimal characters for calculating a_1, a_2, a_3 and a_4 , using (6.4.1).

$$a_k = \text{mod} \left(\frac{\text{hex2dec}(K_{16(k-1)+1:16k})}{10^6}, 1 \right), k = 1, 2, 3, 4. \quad (6.4.1)$$

All four a_k 's are used as control parameters and initial values for NLS to get sequences x, y , and z . Setting the control parameter and initial values as $x_0 = a_1, y_0 = a_2, z_0 = a_3, u = a_4$. NLS map produces three sequences x, y and z of size $\frac{M \times N}{2}$. The values in the sequences x, y , and z are transformed into 16-bit binary representations as shown in Figure 6.7. The obtained bits are employed to generate two separate 8-bit binary representations by extracting bits from even and odd positions. The procedure for generating 8-bit binary representation and hence decimal numbers is termed “Bit separation” and is shown via the diagram in Figure 6.7. The 8-bit binary values are subsequently transformed into their decimal equivalents.

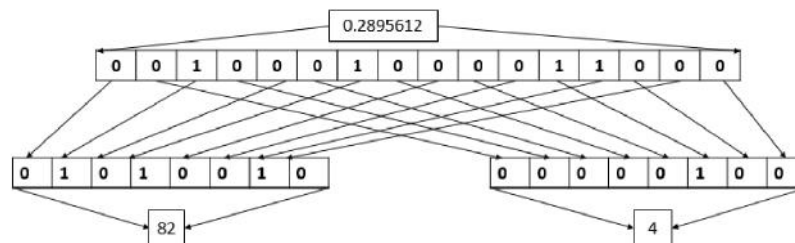


Figure 6.7: Bit separation process

106

The sequences x , y and z are transformed using the methods shown in Figure 6.7. We get six sequences x_{odd} , x_{even} , y_{odd} , y_{even} , z_{odd} , and z_{even} . Finally, the sequences x_{odd} , x_{even} , y_{odd} , y_{even} , z_{odd} , z_{even} are concatenated to produce three pseudo-random sequences of length $M \times N$ (same as image dimension) using (6.4.2).

$$\begin{aligned} X &= \text{Concatenate}(y_{even}, z_{odd}) \\ Y &= \text{Concatenate}(x_{even}, z_{even}) \\ Z &= \text{Concatenate}(x_{odd}, y_{odd}) \end{aligned} \quad (6.4.2)$$

The sequences X , Y , and FSM A^* are used in IEA. We have applied a diffusion process, confusion process, and simultaneous confusion and diffusion process to shift and modify the pixel values of the image P .

Initially, the plain image P undergoes a transformation into a 1D array denoted as C' . The sequence X is used to modify the pixels of the image C' using (6.4.3). The diffused pixels are stored in the C'' .

$$C''_k = X_k \oplus C'_k, k = 0, 1, 2, \dots, (M \times N) - 1 \quad (6.4.3)$$

where, X_k , C'_k represents the k^{th} element of the sequence X and C' respectively. \oplus represents bit-wise XOR operation. After diffusion of the image pixels, the pixels of the cipher image C'' are shifted using the FSM A^* . The $(A_k^*)^{th}$ pixel of the C'' is shifted to k^{th} location of the C''' .

$$C'''_k = C''_{(A_k^*)}, k = 0, 1, 2, \dots, (M \times N) - 1 \quad (6.4.4)$$

After the initial pixel confusion in the image C'' , further diffusion and confusion of the pixels in the resulting cipher image C''' are achieved using (6.4.5):

$$\begin{aligned} C_{W_0} &= Y_0 \oplus C'''_0 \\ C_{W_k} &= C_{k-1} \oplus C'''_k \oplus Y_k, k = 1, 2, \dots, (M \times N) - 1 \end{aligned} \quad (6.4.5)$$

Where Y_k shows the k^{th} element of Y . W is the argument sequence obtained by sorting Z . C represents the cipher image obtained after confusion and diffusion of the pixels

of the input image C''' . In this process $(k-1)^{th}$ element of C , k^{th} element of Y and k^{th} element of C''' are XOR-ed together to obtain the W_k^{th} element of C . This procedure is termed simultaneous confusion and diffusion. After reshaping the obtained cipher image C into the shape $M \times N$, we get the final cipher image.

The IEA developed using SEPM is termed as SEPM-IEA. Since SEPM is 2D map, two sequences x and y are obtained using the keys x_0 , y_0 and u . The third sequence z is obtained by using (6.4.6). The elements are added and modulus values are applied to set the values in the range $[0,1)$.

$$z = \text{mod}(x + y, 1) \quad (6.4.6)$$

The obtained three sequences are transformed using “Bit separation process” and follow same IEA to encrypt the plain images.

Since it is symmetric key cryptography, the secret keys used in the decryption algorithm are the same as encryption algorithm. The steps of encryption algorithm are reversed to obtain the decrypted image.

6.5 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed IEA, we performed a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and resilience are compared to various contemporary algorithms regarding information entropy, NPCR, UACI, correlation coefficient and execution time.

6.5.1 Information entropy analysis

Table 6.1 presents the information entropy values of cipher images generated by the proposed IEA and other existing algorithms. The entropy values for images encrypted using proposed IEAs are consistently close to the ideal value of 8, which indicates a high level of randomness. This suggests that the IEAs effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it makes it significantly more

108

difficult for an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the original image content.

Table 6.1: Comparison of information entropy values of the SEPM-IEA and NLS-IEA with algorithms available in the literature.

Image	SEPM-IEA	NLS-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9992	7.9993	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9995	7.9993	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9972	7.9971	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9998	7.9998	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9998	7.9998	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9998	7.9998	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9998	7.9998	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9998	7.9998	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9992	7.9993	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9968	7.9972	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9994	7.9993	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9992	7.9992	7.9992	7.9992	7.9991
bridge256	7.9970	7.9971	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9993	7.9992	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9996	7.9975	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9993	7.9992	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

6.5.2 Differential attack

Table 6.2 and Table 6.3 present a comparative analysis of NPCR and UACI values for various encrypted images using different encryption algorithms. The results clearly demonstrate that the proposed IEAs consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related algorithms often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

Table 6.2: Comparison of NPCR values of SEPM-IEA and NLS-IEA with algorithms available in the literature.

Image	SEPM-IEA	NLS-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.5930	99.6044	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.6006	99.6014	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.6414	99.5941	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6122	99.6045	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6100	99.6091	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.6114	99.5996	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6158	99.6220	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.6178	99.6095	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.6094	99.6262	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.6490	99.6216	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.6071	99.6151	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6017	99.6017	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.6178	99.6067	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.5789	99.6140	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.5991	99.6014	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

Table 6.3: Comparison of UACI values of the SEPM-IEA and NLS-IEA with algorithms available in the literature.

Image	SEPM-IEA	NLS-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.4429	33.4032	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.4976	33.4587	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.2972	33.6021	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.4574	33.4499	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4827	33.4948	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.4436	33.4132	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.4657	33.4748	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.4785	33.8263	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.3851	33.4439	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.5077	33.4210	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.4873	33.4987	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.4665	33.4732	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.4964	33.4821	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.5147	36.2339	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.4829	33.3446	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

6.5.3 Histogram analysis

Figure 6.8 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining the Figure 6.8, it becomes clear that a significant transformation occurs in the statistical distribution of pixel intensities following the IEA. In the case of the plain images, the histograms typically display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 6.8(a-c)). These patterns can often reveal information about the image content, making plain images vulnerable to statistical analysis and attacks.

The histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the IEA has effectively randomized the pixel values across the entire gray-scale range (Figure 6.8(d-i)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the cipher image histograms confirms that the IEA has successfully obscured the plain image information. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

6.5.4 Correlation Coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 6.4. As observed from the

110

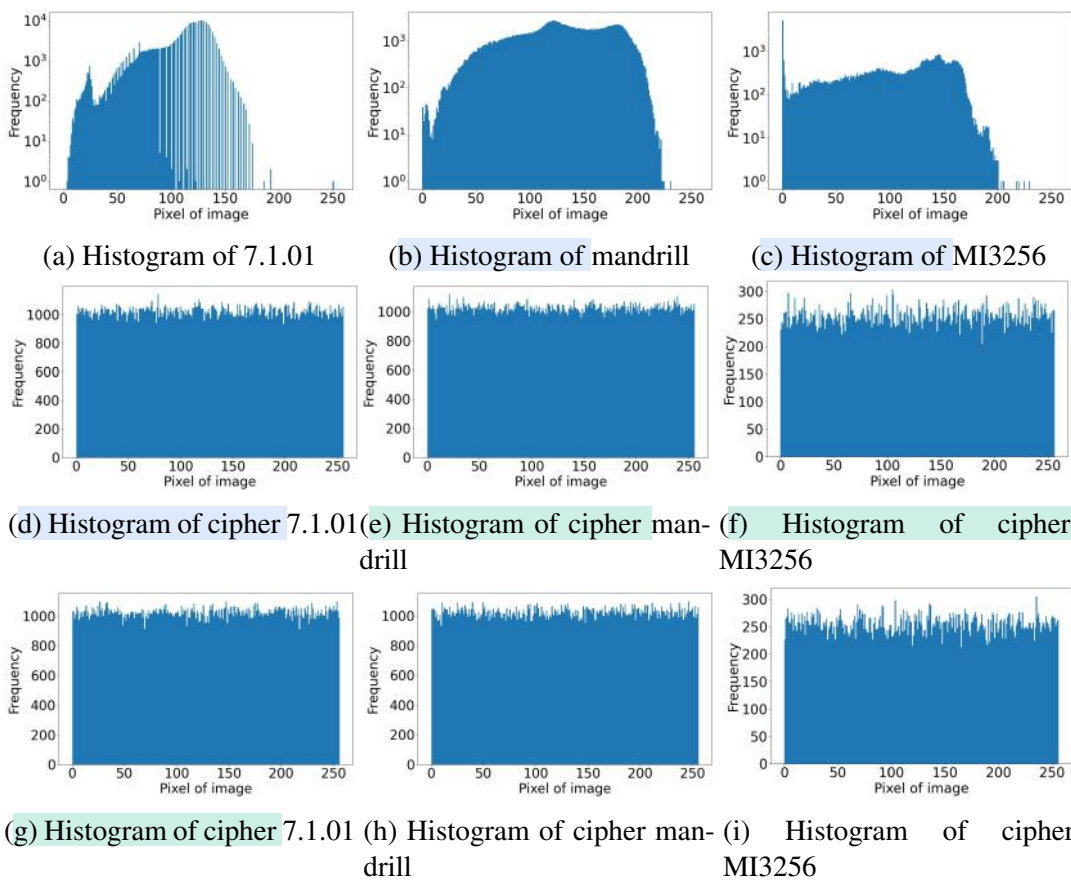


Figure 6.8: Histogram of plain and encrypted images: ((a)-(c)) Histogram of plain images, ((d)-(f)) Histogram of cipher images obtained using SEPM-IEA, ((g)-(i)) Histogram of cipher images obtained using NLS-IEA

Table 6.4, the plain images exhibit very high correlation coefficients, with values close to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the encryption process has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of the IEA in reducing statistical information.

In addition, the pixel intensity distribution is illustrated in Figure 6.9. For the plain images shown in Figure 6.9(a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 6.9(d-i), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

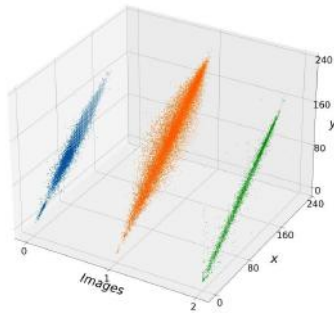
Table 6.4: Comparison of correlation coefficient values of SEPM-IEA and NLS-IEA with algorithms available in the literature.

Image	Plain images	SEPM-IEA	NLS-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	HD 0.9630	-0.0031	0.0060	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD 0.9192	-0.0071	-0.0087	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD 0.8995	-0.0057	0.0004	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD 0.8625	-0.0032	-0.0065	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD 0.7669	0.0031	-0.0035	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD 0.7202	-0.0040	0.0068	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD 0.9784	0.0049	0.0049	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD 0.9795	0.0024	0.0001	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD 0.9405	0.0084	-0.0095	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085

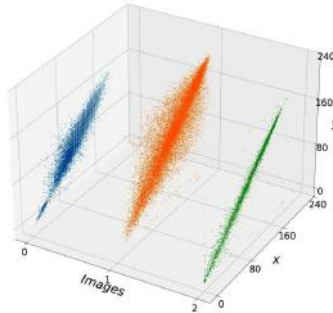
6.5.5 Resistance to classical attacks

The robustness of proposed IEAs against chosen-plaintext attacks is established through Equation (2.3.8). This operation is visually represented in Figure 6.10. By examining Figure 6.10(a-c), it is clear that (2.3.8) holds, suggesting that the IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 6.10(a) and Figure 6.10(b-c). The resulting NPCR value between these two images is 99.6036% (NLS-IEA) and 99.6055% (SEPM-IEA), further reinforcing the IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed IEA is also expected to be resilient against other classical attacks.

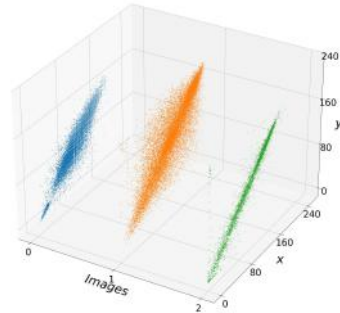
112



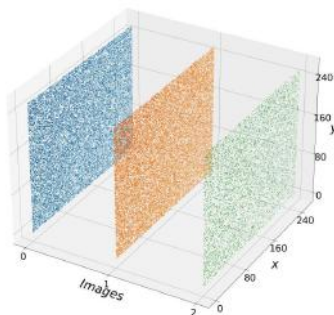
(a) Horizontal direction



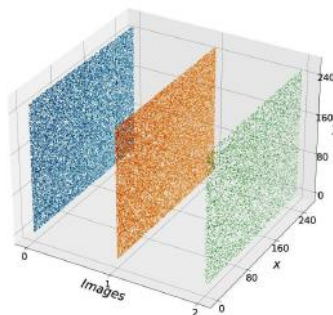
(b) Vertical direction



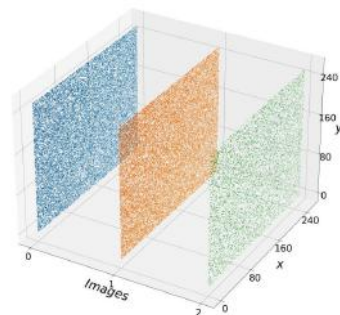
(c) Diagonal direction



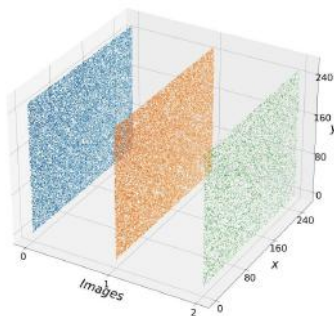
(d) Horizontal direction



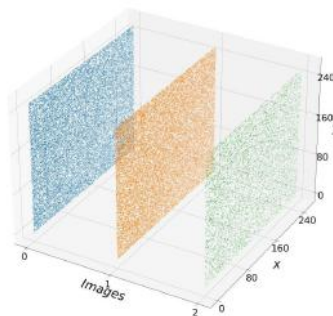
(e) Vertical direction



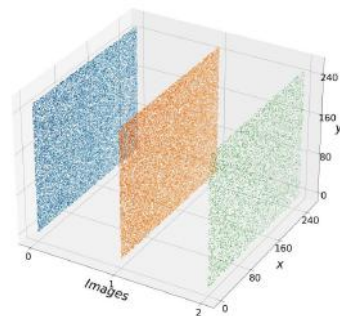
(f) Digonal direction



(g) Horizontal direction



(h) Vertical direction



(i) Digonal direction

Figure 6.9: Pixel distribution of plain and cipher images obtained using SEPM-IEA and NLS-IEA.

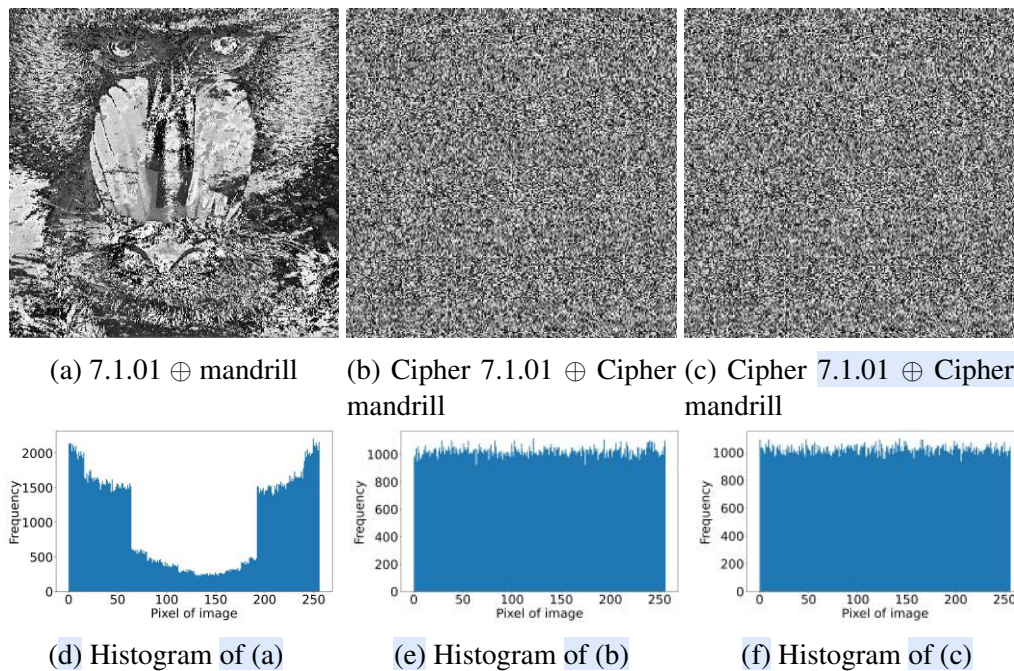


Figure 6.10: Resistance to classical attacks (a) Plain image, (b) SEPM-IEA, (c) NLS-IEA, (d-f) Corresponding histograms.

6.5.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in Figure 6.11(a),(c). The corresponding decrypted image of the occluded images is shown in the Figure 6.11(b),(d). The decrypted image retains most of the original visual content, indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that the IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.

6.5.7 Noise attack

To assess the resilience of the decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 6.12(a),(c), while the corresponding decrypted image is shown in Figure 7.10(b),(d). Despite the presence of

114

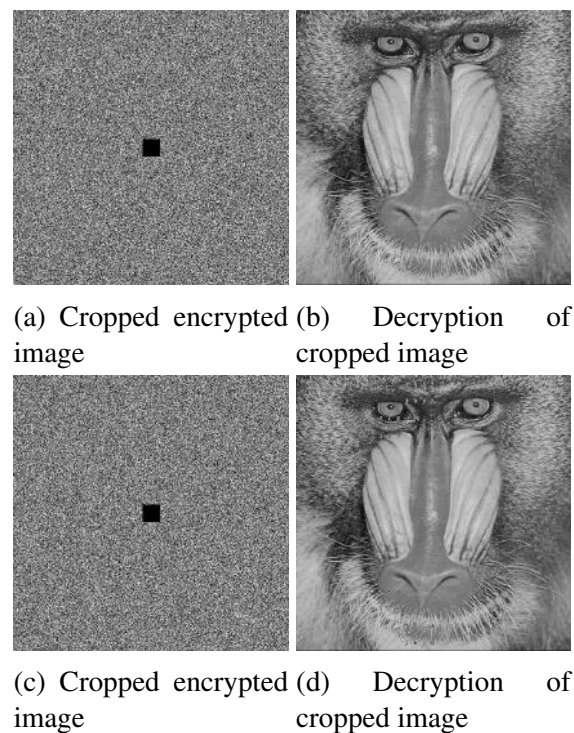


Figure 6.11: Representation of SEPM-IEA's and NLS-IEA's resistance to cropping attack

19 noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption scheme can effectively tolerate such distortions. These results confirm that the proposed IEAs are robust against noise attacks and suitable for secure image transmission over noisy communication channels.

6.5.8 NIST randomness test

Table 6.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the IEAs. As shown in the Table 6.5, the cipher image successfully passes all the randomness tests, indicating that the IEAs effectively introduce randomness in the encrypted images.

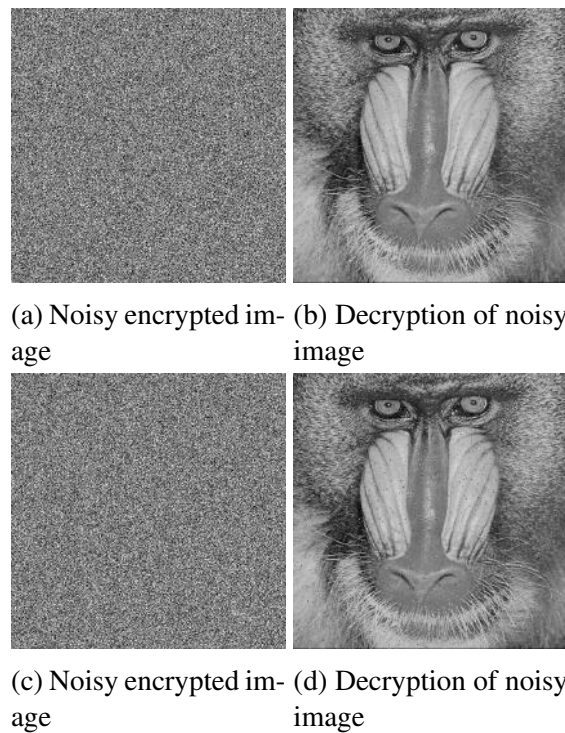


Figure 6.12: Representation of SEPM-IEA's and NLS-IEA's resistance to Noise attack

Table 6.5: Randomness test results for SEPM-IEA and NLS-IEA.

Test Name	SEPM-IEA		NLS-IEA	
	<i>p</i> -value	Result	<i>p</i> -value	Result
Frequency Test	0.6003	Successful	0.6980	Successful
Run Test	0.5617	Successful	0.4878	Successful
Run Test (Longest Run of Ones)	0.9322	Successful	0.4240	Successful
Block Frequency Test	0.3639	Successful	0.7064	Successful
Universal Statistical Test	0.8966	Successful	0.7889	Successful
Linear Complexity Test	0.6454	Successful	0.9385	Successful
Serial Test	0.9669	Successful	0.1919	Successful
Binary Matrix Rank Test	0.5513	Successful	0.9166	Successful
Non-overlapping Template Matching Test	0.3096	Successful	0.4525	Successful
Overlapping Template Matching Test	0.4262	Successful	0.2689	Successful
Approximate Entropy Test	0.7622	Successful	0.4249	Successful
Random Excursion Test	0.6262	Successful	0.0905	Successful
Random Excursion Variant Test	0.5693	Successful	0.2929	Successful
Cumulative Sums	0.4596	Successful	0.5281	Successful
Discrete Fourier Transform Test	0.0878	Successful	0.9707	Successful

116

6.5.9 Execution time analysis

The execution time of the proposed IEA is presented in Table 6.6. As shown in Table 6.6, the execution time for SEPM-IEA is lower, while for NLS-IEA is comparatively higher than that of IEAs available in literature, it offers enhanced robustness and superior security features. This trade-off between time and performance indicates that while proposed IEAs may require more execution time, it compensates with greater resilience against several attacks.

Table 6.6: Comparison of execution time (in seconds) of the SEPM-IEA and NLS-IEA with algorithms available in the literature.

Image	SEPM-IEA	NLS-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	8.07	8.36	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	5.10	5.65	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	1.26	1.81	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

6.6 Summary

In this chapter, we have proposed modified chaotic maps utilizing the existing $e\pi$ -map. The maps exhibit wide chaotic range of control parameter, uniform output distribution, positive and high LE along with high values of PE and SE. The modified maps are used in a IEA. The performance of proposed SEPM-IEA and NLS-IEA is rigorously evaluated using a diverse set of gray-scale images to ensure its applicability across different visual content. Comprehensive experimental analyses are conducted to assess the algorithm's robustness against multiple types of attacks, including statistical, differential, and brute-force. The results confirm that the SEPM-IEA and NLS-IEA effectively disrupt the inherent correlations in image data, ensuring high security. Furthermore, the corresponding decryption algorithm reconstructs the original image content, demonstrating the algorithm's reliability and lossless recovery capability.

Chapter 7

Magic Square Matrix based Fractal Sorting Matrix and its application in Image Encryption

This chapter discusses the development of IEA utilising magic square matrix-based FSM and Zirili–Logistic map (ZLM). Section 7.1 details the background required for the chapter. Section 7.2 describes the proposed ZLM developed by combining the functions such as exponential, sine and Zirili along with Logistic map. Section 7.3 analyses ZLM in terms of BD, PD, LE, PE, and SE. Section 7.4 describes proposed magic square matrix-based FSM. Section 7.5 proposes the IEA leveraging magic square matrix-based FSM and ZLM termed as ZLFSM-IEA. Section 7.6 discusses the analysis of IEA utilising the metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 7.7 summarizes the chapter.

118

7.1 Background

Magic square matrix is a matrix of dimension $n \times n$ with n^2 numbers arranged such that the sum of elements of each row, each column, diagonal, and anti-diagonal is equal to a fixed constant. The value of this fixed constant K can be calculated as $\frac{n(n^2+1)}{2}$ [117, 118, 119]. Mathematically, if $\mathbf{A} = [a_{ij}]$ is a magic square of order n , then

$$\begin{aligned} \text{Row sum : } \sum_{j=1}^n a_{ij} &= K \quad \forall i = 1, 2, 3, \dots, n \\ \text{Column sum : } \sum_{i=1}^n a_{ij} &= K \quad \forall j = 1, 2, 3, \dots, n \\ \text{Diagonal sum : } \sum_{i=1}^n a_{ii} &= K, \quad \sum_{i=1}^n a_{i, n-i+1} = K \quad \forall i = 1, 2, 3, \dots, n \end{aligned} \quad (7.1.1)$$

For example, matrix \mathbf{A} of dimension 3 given in (7.1.2) is a magic square with $K = 15$.

$$\mathbf{A} = \begin{bmatrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{bmatrix} \quad (7.1.2)$$

7.2 Proposed Zirili–Logistic map

The proposed 2D chaotic ZLM is a non-linear map that integrates multiple mathematical features to enhance chaotic complexity. The map leverages synergistic effects of function compositions, wherein Logistic non-linearity, trigonometric oscillations, and exponential amplification are interwoven with the Zirili function to yield irregular and unpredictable dynamics. The modular operation sets the map's output in the range $[0,1)$. Furthermore, the coupling between x and y components enhances cross-dimensional interaction, resulting in a richer chaotic structure than traditional maps. The map is given in (7.2.1).

$$\begin{aligned} x_{i+1} &= \text{mod}(\alpha \sin(\mu x_i(1-x_i)) + \beta e^{x_i^2 + 0.5(1-\cos(2x_i)) + y_i^2}, 1) \\ y_{i+1} &= \text{mod}(\alpha \sin(x_i^2 + 0.5(1-\cos(2x_i)) + y_i^2) + \beta e^{\mu y_i(1-y_i)}, 1) \end{aligned} \quad (7.2.1)$$

where x_i and y_i represent the i^{th} state of the variables. The control parameters α , β and μ lie in the range $[0, \infty)$. For experimental purposes, the values of control parameters are set in range $[0, 10]$.

7.3 Analysis of the Zirili–Logistic Map

The chaotic behavior of the ZLM is comprehensively investigated by employing a range of tools, including BD to visualize the transition between periodic and chaotic regimes, PD to depict the map's state space trajectories, LE to quantify the rate of divergence of nearby trajectories and confirm chaotic dynamics, PE to measure the complexity of the time series based on ordinal patterns, and SE to assess the irregularity and unpredictability of the map's temporal evolution. These tests are performed and the results are discussed in the subsequent sections.

7.3.1 Bifurcation diagram

Figure 7.1 illustrates the BD of ZLM with respect to the control parameters α , β and μ , one varying within the interval $[0, 10]$, while keeping the other parameters fixed and using initial conditions $x_0 = 0.5$ and $y_0 = 0.5$. These diagrams reveal that ZLM exhibits significant ergodicity across a broad range of control parameter values. Furthermore, the BD highlights sensitivity of ZLM to variations in its control parameters. Even small changes in control parameters result in different dynamic behaviors indicating high chaotic dynamics. Thus, it can be concluded that ZLM is well-suited for integration into IEAs.

7.3.2 Phase diagram

The PD of ZLM and other maps, as listed in Table 2.1, are exhibited in Figure 7.2. The PD are plotted using the initial values as ZLM $((x_0, y_0, \alpha, \beta, \mu) = (0.5, 0.5, 10, 10, 10))$, CLM $((x_0, y_0, a, a_1) = (0.5, 0.8, 5, 5))$, ICLM $((x_0, y_0, a, a_1) = (0.3, 0.1, 0.1, 0.1))$, LMHM $((x_0, y_0, \beta, k_1, k_2, \rho_1, k) = (0.5, 0.8, 0.1, 1, 0.1, 100, 0.7))$, IGSCM $((x_0, y_0, r_1, r_2) = (0.21, 0.31, 25, 23.3))$, SLM $((x_0, y_0, \Gamma, p) = (0.3, 0.4, 4, 3.6))$, HSM $((x_0,$

120

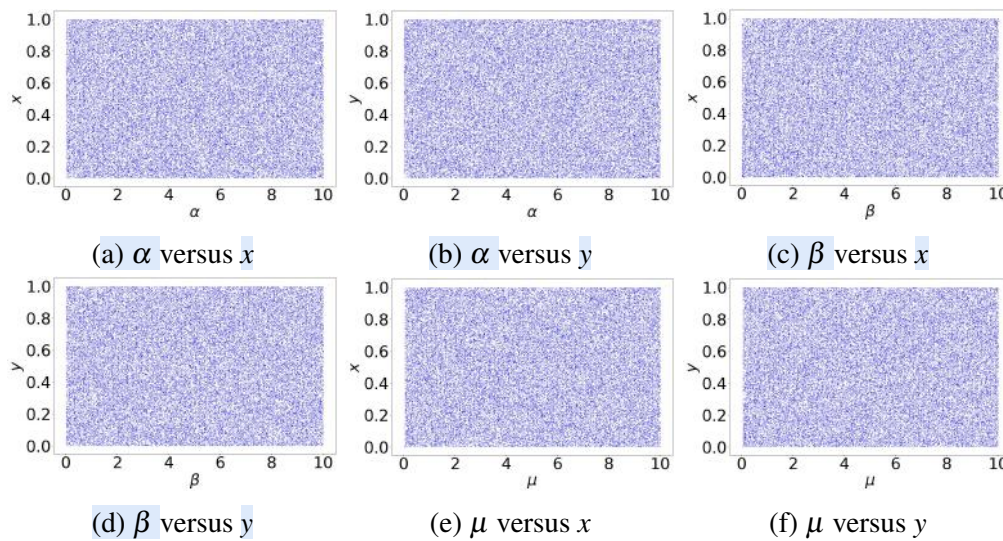


Figure 7.1: Bifurcation diagram of Zirili–Logistic Map.

$y_0, b_1, b_2, \omega) = (0.3, 0.6, 5, 1.57, 10))$, LNIC $((x_0, y_0, a, a_1) = (0.9, 0.6, 1, 1))$, CLSS map $((x_0, y_0, c) = (0.3, 0.6, 0.5))$, LCCCM $((x_0, y_0, \mu, p_1) = (0.6, 0.9, 5, 8.78))$. The ZLM's PD demonstrates a uniform distribution throughout the phase diagram. This indicates that the state trajectories of the ZLM do not concentrate in specific regions but are instead evenly dispersed across the entire region. In contrast, the PD of other maps display non-uniform distributions. This observation suggests that the proposed ZLM map offer enhanced resistance to phase space reconstruction attacks.

7.3.3 Lyapunov exponent

The LE of ZLM and other maps, as listed in Table 2.1, are exhibited in Figure 7.3. LE_x and LE_y represent the LEs associated with the x and y variables, respectively. From the Figure 7.3, it is visible that the LE of ZLM map are positive and high as compared to other maps except IGSCM. Thus it can be concluded that the ZLM is extremely sensitive to initial conditions. The larger the LE, the faster this divergence happens. Thus ZLM is hyper-chaotic, complex, unpredictable and hence suitable for integration into IEAs.

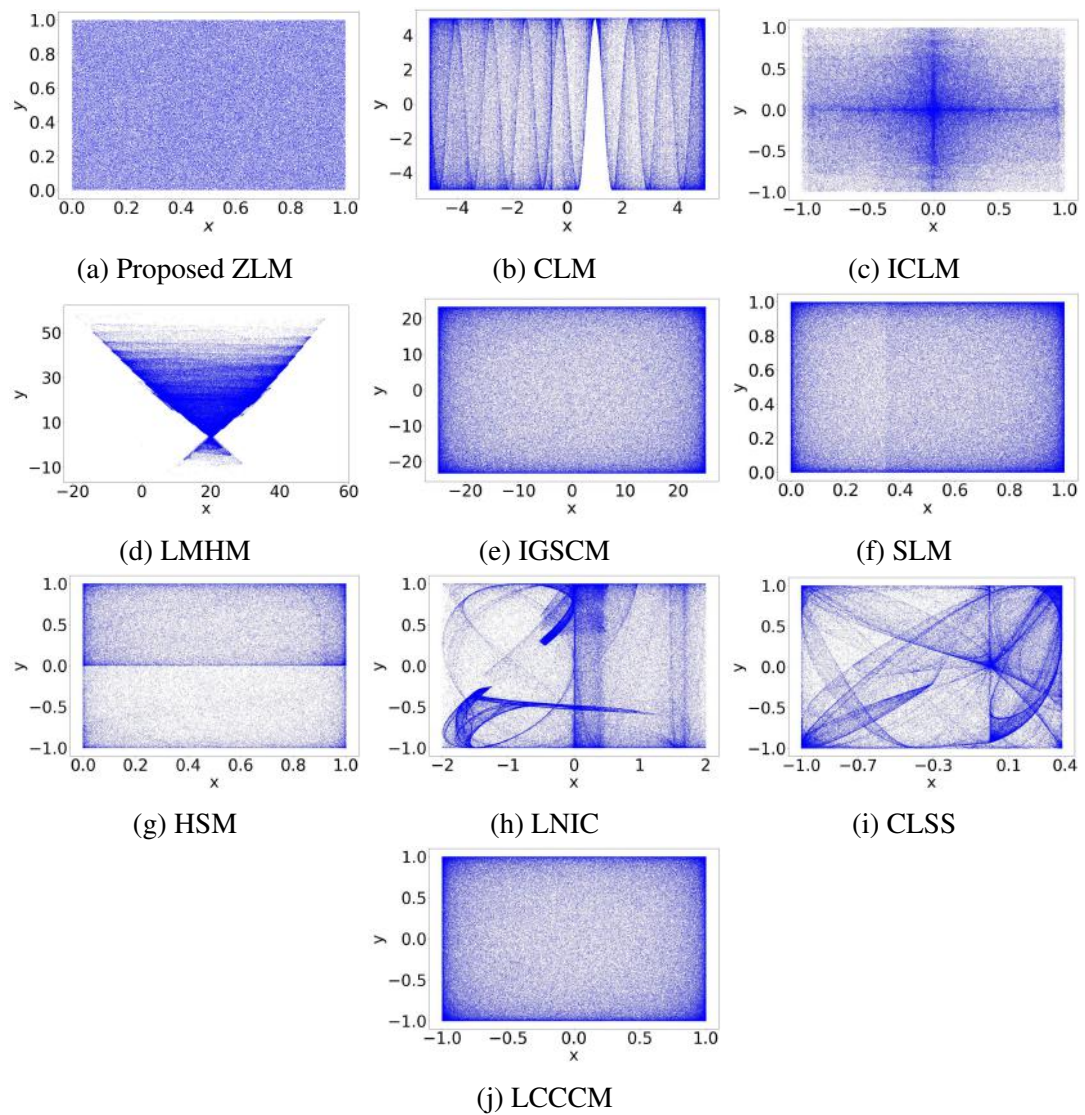


Figure 7.2: Phase diagrams (x and y).

122

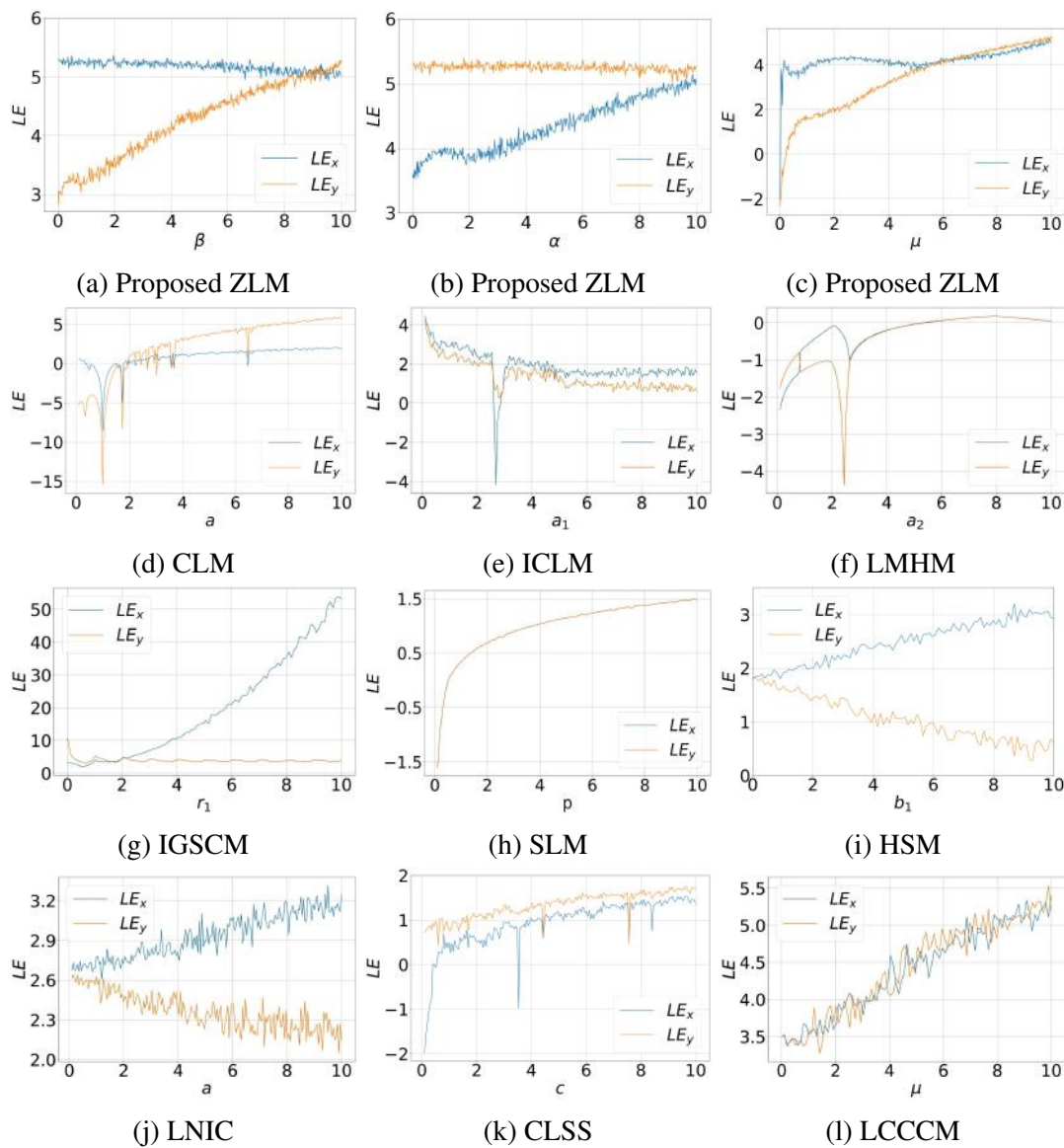


Figure 7.3: Lyapunov exponent diagram of Zirili-Logistic and others maps.

7.3.4 Permutation entropy

Figure 7.4 illustrates the PE of ZLM alongside other chaotic maps listed in Table 2.1. As shown in the Figure 7.4, ZLM consistently exhibits values near 1 across the specified range of control parameters. This suggests that ZLM demonstrates highly complex or chaotic behavior, making it a strong candidate for applications requiring randomness or unpredictability, such as cryptography or secure communications.

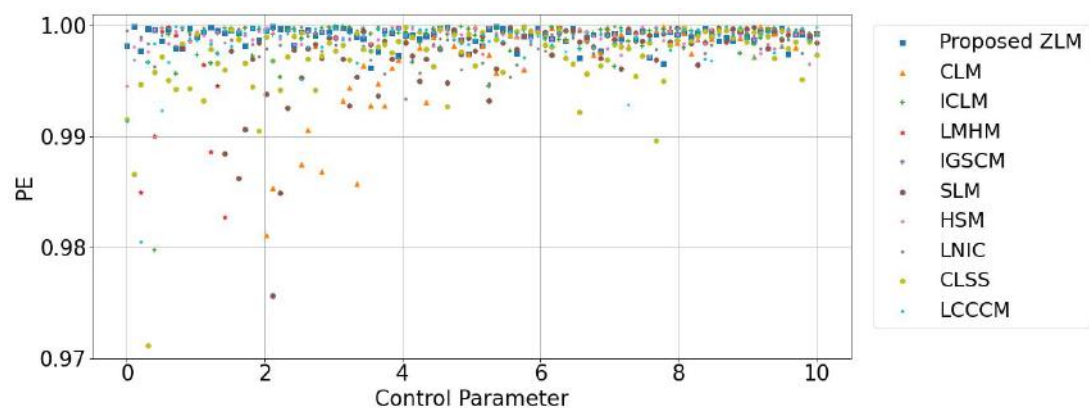


Figure 7.4: Permutation entropy of ZLM.

7.3.5 Sample entropy

Figure 7.5 shows the SE of ZLM compared to other chaotic maps listed in Table 2.1. As shown in Figure 7.5, the ZLM consistently achieves high values of SE around 2 across the evaluated range of control parameters, suggesting that the ZLM exhibits pronounced chaotic behavior. It can be inferred that ZLM is a strong candidate for applications requiring high unpredictability, including cryptography and secure communications.

7.4 Proposed Magic Square Matrix-based Fractal Sorting Matrix

Definition 7.4.1. The matrix A is termed as magic square matrix-based FSM if the initial iteration matrix is a magic square matrix.

124

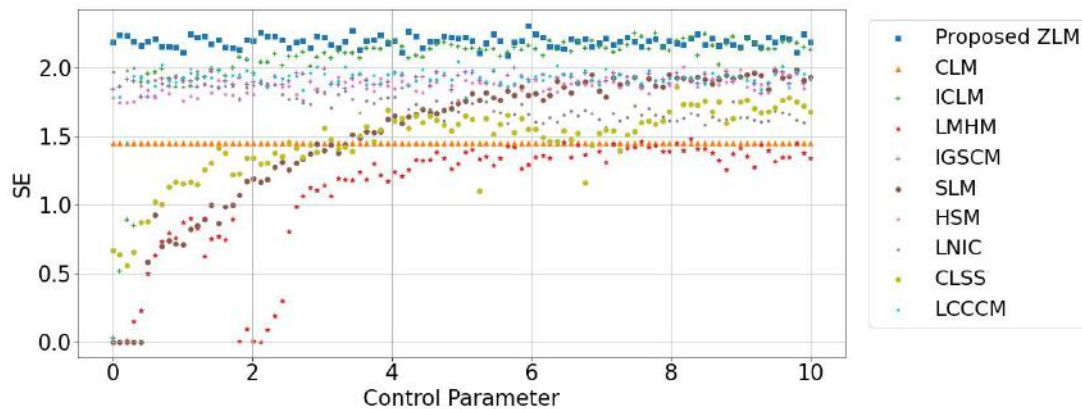


Figure 7.5: Sample entropy of ZLM.

In recent literature [82, 120], FSM (Section 6.1.2) is generated using 2×2 matrix, which severely restricts the available parameter space. Later, the research work [121] introduced a spiral transform-based FSM to extend the FSM construction beyond the 2×2 formulation. While this approach increased dimensionality, it did not introduce a fundamentally new structural design. To overcome these limitations, this work proposes the magic square matrix-based FSM, which integrates the structural properties of magic squares into the FSM. Since, the number of magic squares increases sharply with order, e.g., 8 magic square matrices exist for order 3. The numbers in a magic square are spread out evenly, they don't bunch up in one place. This makes the sorting process look more random and hides obvious patterns. As a result, it becomes harder for someone to notice or guess the structure, which improves security. In contrast to earlier FSM constructions, the magic square matrix-based FSM offers genuine structural novelty together with stronger security guarantees.

According to the definition, we give a class of magic square matrix-based FSM construction method. Consider an initial magic square matrix $\mathbf{A}^{(1)} \in \mathbb{R}^{d \times d}$, we iterate according to the following steps to obtain magic square matrix-based FSM \mathbf{A}^* .

1. Calculate the split sub-blocks of each element in the initial magic square matrix:

$$\begin{cases} \mathbf{A}^{(2)}\{i, j\} = \text{Max}(\mathbf{A}^{(1)}) \times (\mathbf{A}^{(1)}(i, j) - 1) \times J_{d \times d} + \mathbf{A}^{(1)} \\ i, j = 1, 2, \dots, d \end{cases} \quad (7.4.1)$$

where $\mathbf{A}^{(2)}\{i, j\}$ represents the sub-block of each element in the magic square

matrix $\mathbf{A}^{(2)}$. $Max(\bullet)$ represents the maximum element. $\mathbf{A}^{(1)}(i, j)$ denotes the element of the i^{th} row and j^{th} column of matrix. J denotes the matrix of ones.

2. Merge sub-blocks to get matrix $\mathbf{A}^{(2)}$ of order $d^2 \times d^2$:

$$\mathbf{A}^{(2)} = \begin{bmatrix} \mathbf{A}^{(2)}\{1,1\} & \mathbf{A}^{(2)}\{1,2\} & \dots & \mathbf{A}^{(2)}\{1,d\} \\ \mathbf{A}^{(2)}\{2,1\} & \mathbf{A}^{(2)}\{2,2\} & \dots & \mathbf{A}^{(2)}\{2,d\} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}^{(2)}\{d,1\} & \mathbf{A}^{(2)}\{d,2\} & \dots & \mathbf{A}^{(2)}\{d,d\} \end{bmatrix} \quad (7.4.2)$$

here $\mathbf{A}^{(2)} \in \mathbb{R}^{d^2 \times d^2}$ is an magic square matrix-based FSM obtained by iterating $\mathbf{A}^{(1)}$.

3. Repeat steps 1 and 2 to get a higher-order magic square matrix-based FSM. While $\mathbf{A}^{(n)} \in \mathbb{R}^{d^n \times d^n}$ is obtained by iterating over $\mathbf{A}^{(n-1)} \in \mathbb{R}^{d^{n-1} \times d^{n-1}}$ with the following formulas.

$$\mathbf{A}^{(n)} = \begin{bmatrix} \mathbf{A}^{(n)}\{1,1\} & \mathbf{A}^{(n)}\{1,2\} & \dots & \mathbf{A}^{(n)}\{1,d^{n-1}\} \\ \mathbf{A}^{(n)}\{2,1\} & \mathbf{A}^{(n)}\{2,2\} & \dots & \mathbf{A}^{(n)}\{2,d^{n-1}\} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}^{(n)}\{d^{n-1},1\} & \mathbf{A}^{(n)}\{d^{n-1},2\} & \dots & \mathbf{A}^{(n)}\{d^{n-1},d^{n-1}\} \end{bmatrix} \quad (7.4.3)$$

abbreviated as

$$\begin{cases} \mathbf{A}^{(n)}\{i,j\} = Max(\mathbf{A}^{(n-1)}) \times (\mathbf{A}^{(n-1)}(i,j) - 1) \times J_{d^{n-1} \times d^{n-1}} + \mathbf{A}^{(n-1)} \\ i, j = 1, 2, \dots, d^{n-1} \end{cases} \quad (7.4.4)$$

Through the above steps, we can obtain FSM $\mathbf{A}^* = \mathbf{A}^{(n)}$, combined with actual needs and the appropriate number of iterations.

To explain the definition and iterative algorithm of magic square matrix-based FSM, an example is given below.

126

Example 1: Construct the initial matrix as

$$\mathbf{A}^{(1)} = \begin{bmatrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{bmatrix} \quad (7.4.5)$$

1 Applying the iterative steps given above, then performing an iteration and merging to get

$$\mathbf{A}^{(2)} = \begin{bmatrix} 11 & 16 & 15 & 56 & 61 & 60 & 47 & 52 & 51 \\ 18 & 14 & 10 & 63 & 59 & 55 & 54 & 50 & 46 \\ 13 & 12 & 17 & 58 & 57 & 62 & 49 & 48 & 53 \\ 74 & 79 & 78 & 38 & 43 & 42 & 2 & 7 & 6 \\ 81 & 77 & 73 & 45 & 41 & 37 & 9 & 5 & 1 \\ 76 & 75 & 80 & 40 & 39 & 44 & 4 & 3 & 8 \\ 29 & 34 & 33 & 20 & 25 & 24 & 65 & 70 & 69 \\ 36 & 32 & 28 & 27 & 23 & 19 & 72 & 68 & 64 \\ 31 & 30 & 35 & 22 & 21 & 26 & 67 & 66 & 71 \end{bmatrix} \quad (7.4.6)$$

Using (7.4.6), iterate again and get

$$\mathbf{A}^{(3)} = \begin{bmatrix} \mathbf{A}^{(3)}\{1,1\} & \mathbf{A}^{(3)}\{1,2\} & \mathbf{A}^{(3)}\{1,3\} \\ \mathbf{A}^{(3)}\{2,1\} & \mathbf{A}^{(3)}\{2,2\} & \mathbf{A}^{(3)}\{2,3\} \\ \mathbf{A}^{(3)}\{3,1\} & \mathbf{A}^{(3)}\{3,2\} & \mathbf{A}^{(3)}\{3,3\} \end{bmatrix} \quad (7.4.7)$$

$$\mathbf{A}^{(3)}\{j,k\} = 81 \times (\mathbf{A}^{(2)}(j,k) - 1) \times J_{9 \times 9} + \mathbf{A}^{(2)} \quad (7.4.8)$$

2 As shown in Example 1, the elements in magic square matrix-based FSM produced by iteration are irregularly ordered and self-similar.

7.5 Application of magic square matrix-based FSM and map in image encryption algorithm

The chaos-based IEA with the permutation then diffusion method shows good performance and security. We propose a permutation method utilizing ZLM and magic square matrix-based FSM. The size of plaintext image used in this study is $M \times N$, where M is the height of the image and N is the number of width of image. If $M \neq N$, we use the method of zero padding to fill the image with $M \times M$ or $N \times N$ for encryption. The encryption algorithm proposed in this paper consists of following steps:

1. Insert the plain image P having number of rows as M and number of columns as N .
2. Generate a 128-bit hash key H using SHA3-512 from P . Using H , eight decimal numbers $K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8$ are obtained.
3. Obtain initial values and control parameter as given in (7.5.1).

$$\begin{cases} x_0 = \frac{K_1 \oplus K_2}{2^{64}}, y_0 = \frac{K_3 \oplus K_4}{2^{64}}, \\ \alpha = 10 \times \frac{K_5 \oplus K_6}{2^{64}}, \beta = 10 \times \frac{K_6 \oplus K_7}{2^{64}}, \mu = 10 \times \frac{K_7 \oplus K_8}{2^{64}} \end{cases} \quad (7.5.1)$$

4. Iterating (5.2.1), according to Algorithm 7.1, using initial values and parameters to get v .
5. Determine the number of iterations according to the size of plain image and get magic square matrix-based FSM.
6. A sequence of size N is derived from v and sorted in ascending order. The indices are applied to circularly shift the columns of magic square matrix-based FSM. Finally, the shifted matrix is transposed. This adds more randomness to the magic square matrix-based FSM. For every image to be encrypted, there will now be a different shuffling matrix.

128

7. From the v , a sequence of size $M \times N$ is chosen and modified using equation

$$V(i) = \text{mod}(\lfloor v(i) \times 10^5 \rfloor, 256), i = 0, 1, 2, \dots, M \times N - 1. \quad (7.5.2)$$

where $\lfloor \bullet \rfloor$ represents floor operation. $\text{mod}(\bullet, 256)$ represents the remainder when divided by 256. The obtained sequence V is reshaped to the size of image and is stored as CS to diffuse the pixel values.

8. The plain image (P) and magic square matrix-based FSM (A^*) are flattened. The P is scrambled as given in (7.5.3).

$$SI(i) = P(A^*(i)) \quad (7.5.3)$$

where, SI is the scrambled matrix. SI is reshaped to the size of plain image.

9. The diffusion operation is performed using (7.5.4).

$$C(i, j) = \begin{cases} SI(i, j) \oplus CS(i, j), & i = 0, j = 0 \\ SI(i, j) \oplus C(i, j-1) \oplus CS(i, j), & i = 0, j \neq 0 \\ SI(i, j) \oplus C(i-1, j) \oplus CS(i, j), & i \neq 0, j = 0 \\ SI(i, j) \oplus C(i-1, j-1) \oplus C(i-1, j) \oplus C(i, j-1) \oplus CS(i, j), & i \neq 0, j \neq 0. \end{cases} \quad (7.5.4)$$

where C is the encrypted image.

Since the ZLFSM-IEA is symmetric, it uses the same key in the encryption and decryption operations. As encryption and decryption processes are inherently reversible, the decryption process entails executing the inverse operations of the encryption process.

7.6 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed ZLFSM-IEA, we performed a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and

Algorithm 7.1: Obtaining chaotic sequence v .

Input : $x_0, y_0, \alpha, \beta, \mu$
Output: $v = \{x_1, y_1, x_2, y_2, \dots, x_i, y_i, \dots\}$

- 1 $iteration \leftarrow \frac{M \times N}{2}$
- 2 Initialize $v \leftarrow []$
- 3 **for** $i \leftarrow 0$ **to** $iteration - 1$ **do**
- 4 $x_{i+1} \leftarrow \text{mod}(\alpha \sin(\mu x_i(1 - x_i)) + \beta e^{x_i^2 + 0.5(1 - \cos(2x_i)) + y_i^2}, 1)$
 $y_{i+1} \leftarrow \text{mod}(\alpha \sin(x_i^2 + 0.5(1 - \cos(2x_i)) + y_i^2) + \beta e^{\mu y_i(1 - y_i)}, 1)$
- 5 **end**
- 6 $v.append(x_{i+1})$
- 7 $v.append(y_{i+1})$
- 8 **return** v

resilience are compared to various IEAs available in literature in terms of information entropy, NPCR, UACI, correlation coefficient and execution time.

7.6.1 Information entropy analysis

Table 7.1 presents the information entropy values of cipher images generated by the proposed IEA and other existing algorithms. The entropy values for images encrypted using proposed IEA are consistently close to the ideal value, which indicates a high level of randomness. This suggests that the proposed IEA effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it makes it significantly more difficult for an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the proposed IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the plain image content.

7.6.2 Differential attack

Table 7.2 and Table 7.3 present a comparative analysis of NPCR and UACI values for various encrypted images obtained using proposed and other IEAs. The results clearly demonstrate that the proposed ZLFSM-IEA consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related algo-

130

Table 7.1: Comparison of information entropy values of the ZLFSM-IEA with algorithms available in the literature.

Image	ZLFSM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9973	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9968	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9971	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9972	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9974	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9971	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9969	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9974	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9974	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9975	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9974	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9993	7.9992	7.9992	7.9992	7.9991
bridge256	7.9974	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9970	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9973	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9995	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

rithms often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the ZLFSM-IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that ZLFSM-IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

Table 7.2: Comparison of NPCR values of ZLFSM-IEA with algorithms available in the literature.

Image	ZLFSM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.6170	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.6017	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.5987	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6124	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6017	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.5621	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6323	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.5697	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.5956	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.6124	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.6490	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6094	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.5850	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.5804	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.6353	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

7.6.3 Histogram analysis

Figure 7.6 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining the Figure 7.6, it becomes clear that a significant transformation occurs in the statistical distribution of pixel intensities following the IEA. In the case of the plain images, the histograms typically display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 7.6(a-c)). These patterns can often reveal information about the image content, making

Table 7.3: Comparison of UACI values of the ZLFSM-IEA with algorithms available in the literature.

Image	ZLFSM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.6381	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.4882	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.4447	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.3499	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4866	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.3971	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.4897	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.4323	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.7145	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.3546	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.5932	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.3903	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.4829	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.5696	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.6120	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

plain images vulnerable to statistical analysis and attacks.

The histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the IEA has effectively randomized the pixel values across the entire gray-scale range (Figure 7.6(d-f)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the histograms of cipher images confirm that the IEA has successfully obscured the plain image. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

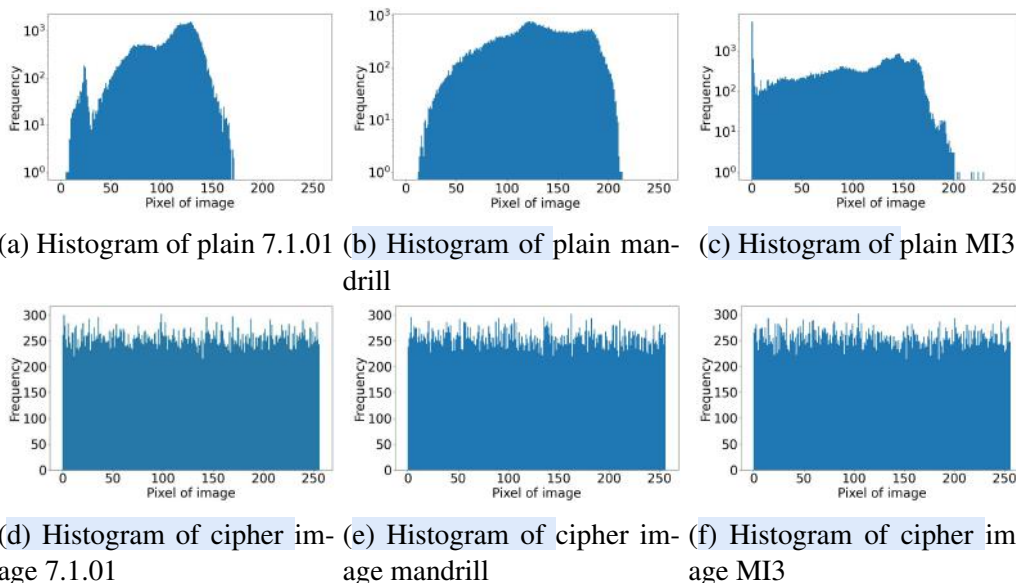


Figure 7.6: Histogram of plain and cipher images

132

7.6.4 Correlation Coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 7.4. As observed from the Table 7.4, the plain images exhibit very high correlation coefficients, with values close to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the ZLFSM-IEA has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of the ZLFSM-IEA in reducing statistical information.

In addition, the pixel intensity distribution is illustrated in Figure 7.7. For the plain images shown in Figure 7.7(a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 7.7(d-f), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

Table 7.4: Comparison of correlation coefficient values of ZLFSM-IEA with algorithms available in the literature.

Image	Plain images	ZLFSM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	HD 0.9630	-0.0011	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD 0.9192	-0.0051	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD 0.8995	-0.0027	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD 0.8625	-0.0042	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD 0.7669	0.0035	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD 0.7202	-0.0048	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD 0.9784	0.0041	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD 0.9795	0.0034	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD 0.9405	0.0024	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085

7.6.5 Resistance to classical attacks

The robustness of proposed ZLFSM-IEA against chosen-plaintext attacks is established through Equation (2.3.8). The operation is visually represented in Figure 7.8. By examining Figure 7.8(a),(b), it is clear that (2.3.8) holds, suggesting that the ZLFSM-IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 7.8(a) and 7.8(b). The resulting NPCR value between these two images is 99.6097%, further re-

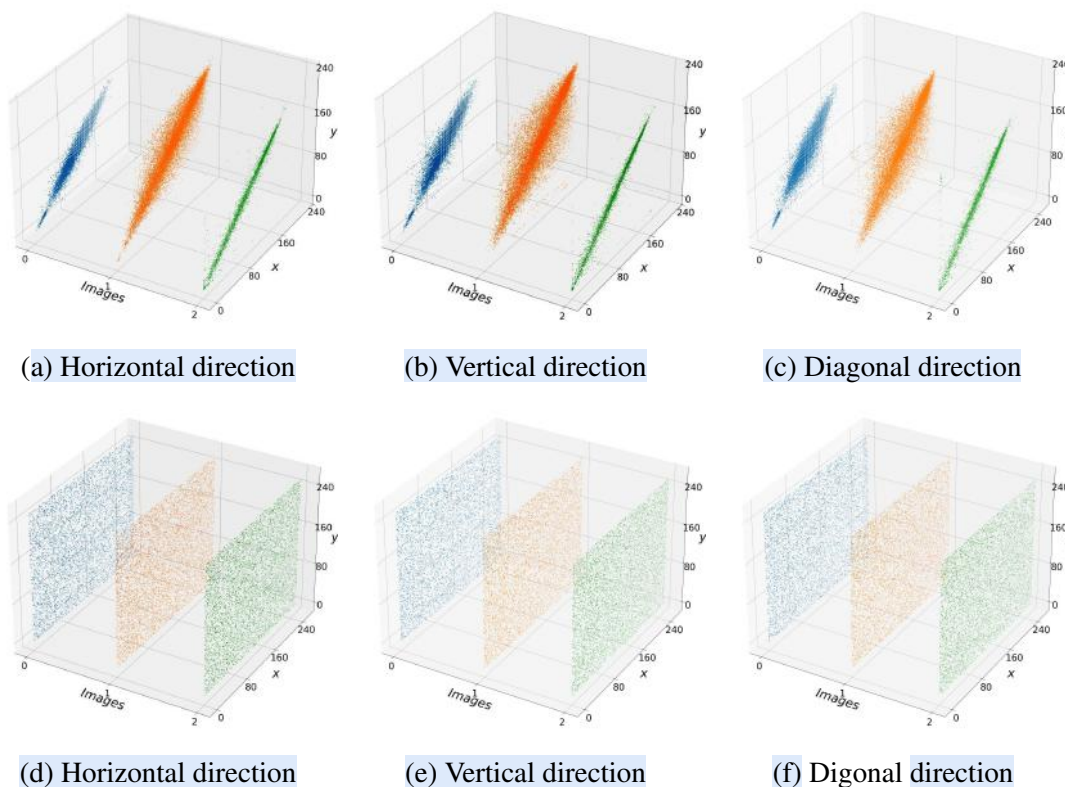


Figure 7.7: Pixel distribution of plain and cipher images obtained using ZLFSM-IEA.

enforcing the ZLFSM-IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed ZLFSM-IEA is resilient against other classical attacks.

7.6.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in Figure 7.9(a). The corresponding decrypted image of the occluded images is shown in the Figure 7.9(b). The decrypted image retains most of the original visual content, indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that the ZLFSM-IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.

134

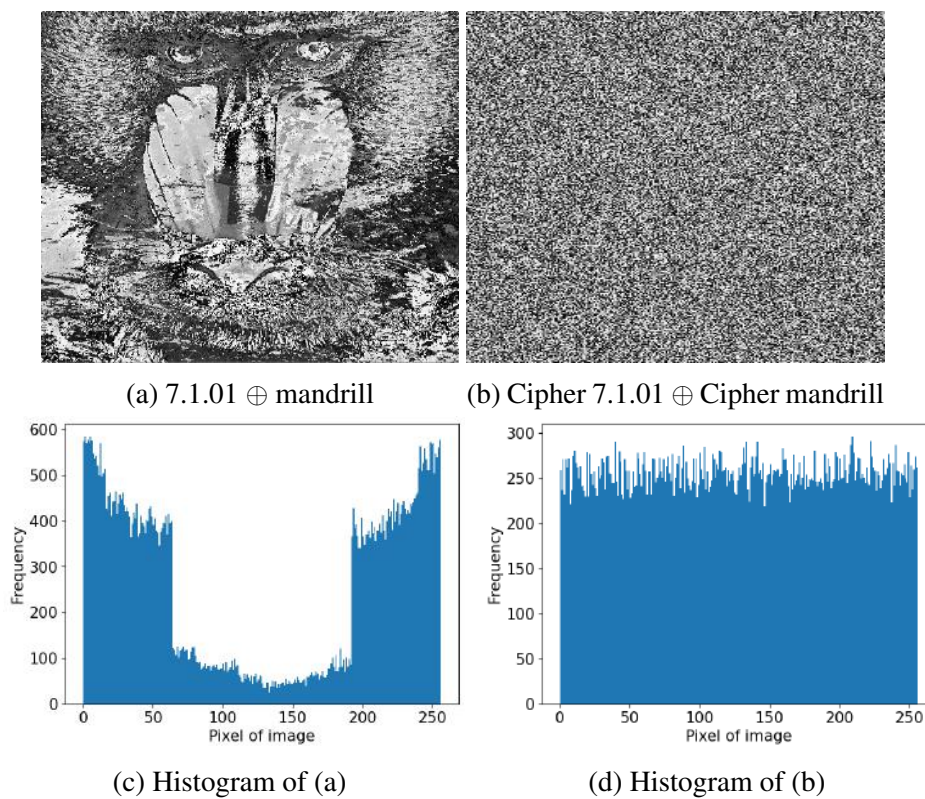


Figure 7.8: Resistance to classical attacks

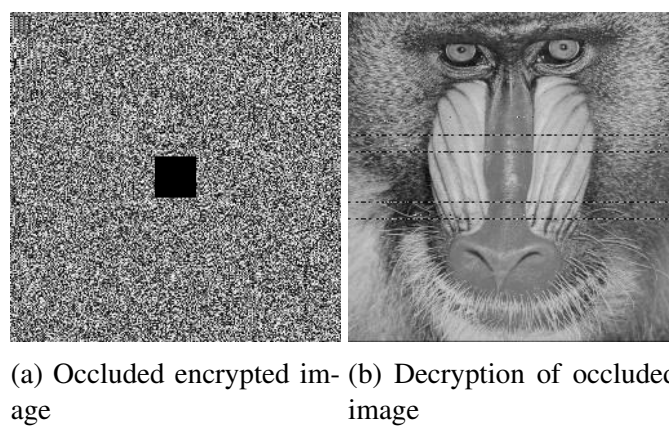


Figure 7.9: Representation of ZLFSM-IEA's resistance to cropping attack

7.6.7 Noise attack

To assess the resilience of the decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 7.10(a), while the corresponding decrypted image is shown in Figure 7.10(b). Despite the presence of noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption scheme can effectively tolerate such distortions. These results confirm that the ZLFSM-IEA is robust against noise attacks and suitable for secure image transmission over noisy communication channels.

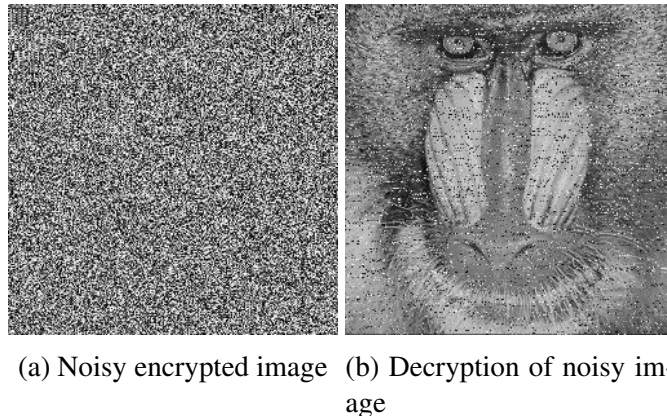


Figure 7.10: Representation of ZLFSM-IEA's resistance to Noise attack

7.6.8 NIST randomness test

Table 7.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the IEA. As shown in the Table 7.5, the cipher image successfully passes all the randomness tests, indicating that the IEA effectively introduces randomness in the encrypted images.

7.6.9 Execution time analysis

The execution time of the proposed IEA is presented in Table 7.6. For a comprehensive performance evaluation, these results are compared with the execution times

Table 7.5: Randomness test results for ZLFSM-IEA.

Test name	p-value	Result
Frequency Test	0.5902	Successful
Run Test	0.8147	Successful
Run Test (Longest Run of Ones)	0.4482	Successful
Block Frequency Test	0.2007	Successful
Universal Statistical Test	0.8650	Successful
Linear Complexity Test	0.1875	Successful
Serial Test	0.4185	Successful
Binary Matrix Rank Test	0.6937	Successful
Non-overlapping Template Matching Test	0.2346	Successful
Overlapping Template Matching Test	0.1245	Successful
Approximate Entropy Test	0.8020	Successful
Random Excursion Test	0.8002	Successful
Random Excursion Variant Test	0.1607	Successful
Cumulative Sums	0.7763	Successful
Discrete Fourier Transform Test	0.4684	Successful

of other encryption algorithms available in the literature. This comparison highlights the efficiency of the proposed IEA in terms of computational speed. As shown in Table 7.6, the ZLFSM-IEA demonstrates strong robustness and high computational efficiency. Although the execution time for ZLFSM-IEA is comparatively higher than that of certain other algorithms available in literature, it offers enhanced robustness and superior security features. This trade-off between time and performance indicates that while ZLFSM-IEA may require more processing time, it compensates with greater resilience against several attacks.

Table 7.6: Comparison of execution time (in seconds) of the ZLFSM-IEA with algorithms available in the literature.

Image	ZLFSM-IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	0.84	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	0.81	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	0.82	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

7.7 Summary

In this chapter, we proposed a novel IEA that incorporates a magic square matrix-based FSM aimed at significantly reducing the inherent pixel correlation present in plain images. This matrix serves to disrupt the statistical relationship between adjacent pixels, thereby enhancing the confusion and diffusion properties essential for secure

image encryption. To further strengthen the encryption algorithm, the algorithm employs ZLM. The chaotic dynamics of the ZLM are analysed using BD, PD, LE, PE and SE. These sequences are utilized to modify pixel intensity values of the plain image, ensuring a high level of randomness in the encrypted image.

The comprehensive analysis of the proposed algorithm demonstrates its robustness against a wide range of cryptographic attacks. Specifically, it shows strong resistance to brute-force attacks due to the vast key space, as well as to statistical and differential attacks owing to the effective decorrelation and high sensitivity to initial conditions. Furthermore, the algorithm is capable of recovering and preserving image content even when portions of the encrypted data are corrupted.

In addition to its security strengths, the algorithm is characterized by a short execution time, which makes it highly suitable for real-time image encryption and decryption applications where speed and reliability are critical. The combination of strong security features and computational efficiency positions the proposed method as a viable solution for secure image transmission in various practical scenarios.

Chapter 8

Image Encryption using multiple chaotic maps

In the pursuit of enhancing the security of digital images, researchers have explored hybrid IEAs that combine the strengths of multiple chaotic maps. This chapter presents an IEA leveraging multiple chaotic maps and linear feedback shift register (LFSR). Section 8.1 discusses the background required for the chapter. Section 8.2 proposes the IEA developed using the multiple chaotic maps like Tinkerbell map, Logistic map along with LFSR. In Section 8.3, we have discussed the analysis of the IEA utilising metrics such as information entropy, differential attack resistance, histogram analysis, correlation coefficients, and randomness tests, demonstrating its robustness in producing secure cipher images. Finally, Section 8.4 summarizes the chapter.

8.1 Background

In this section, we have discussed about the Tinkerbell map and LFSR. The Logistic map is described in the Section 4.1.2.

140

8.1.1 Tinkerbell Map

Tinkerbell map [40] is a 2D discrete chaotic map with four control parameters a , b , c , and d . The Tinkerbell map is defined as given in (8.1.1).

$$\begin{aligned} z_{i+1} &= z_i^2 - w_i^2 + az_i + bw_i \\ w_{i+1} &= 2z_iw_i + cz_i + dw_i \end{aligned} \quad (8.1.1)$$

where z_i and w_i represent the state variables at i^{th} iteration. We have used the values of control parameters as $a = 0.9$, $b = -0.60$, $c = 2.0$, $d = 0.50$ and initial values as $z_0 = -0.72$ and $w_0 = -0.64$. The phase and bifurcation diagram of Tinkerbell map are shown in Figure 8.1 [122].

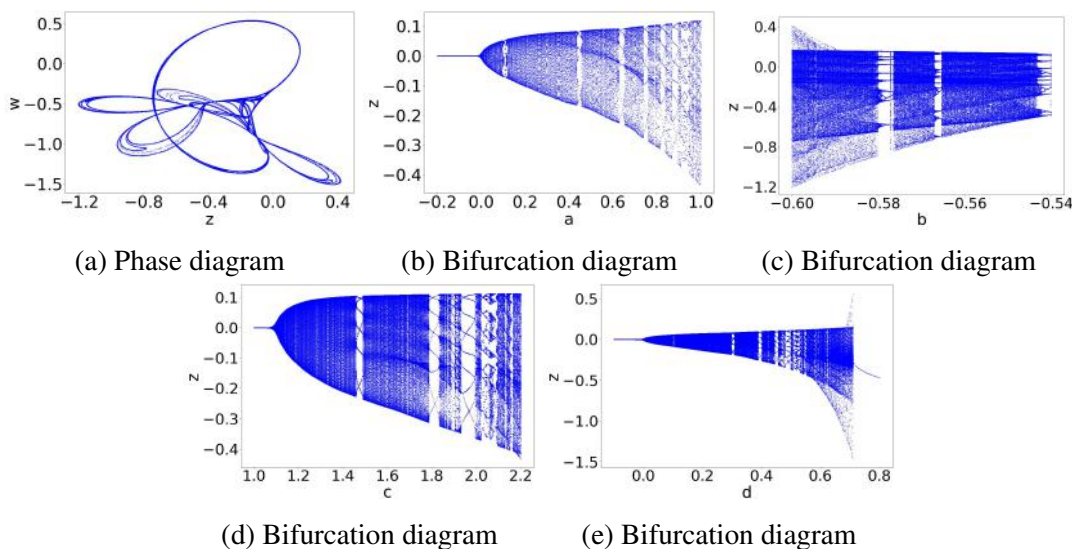


Figure 8.1: Diagrams of Tinkerbell map.

8.1.2 Linear Feedback Shift Register

In computing, an LFSR is a shift register whose input bit is a linear combination of its prior state. If a good feedback function is used, the LFSR generates a random bit stream with a lengthy and complicated cycle. An n -stage LFSR is distinguished by a feedback polynomial of degree n over $GF(2)$. If the input polynomial is primitive, the resulting sequence of states is periodic and has a period $(2^n - 1)$. Here, we have considered an

initial input in the form of polynomial $x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ (11110011) with degree $n = 8$. There are 255 possible initial states. Figure 8.2 exhibits the working of LFSR used in this work. The bits E_0, E_2, E_5, E_7 are the bits to be Xor-ed to get the output bit sequence $E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8$ and feedback to the rightmost bit $E_8 = E_0 \oplus E_2 \oplus E_5 \oplus E_7$.

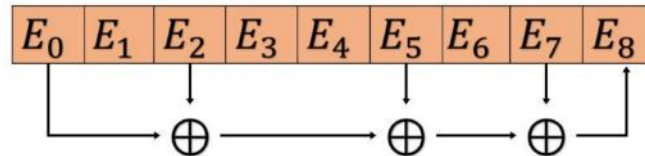


Figure 8.2: Schematic representation of linear feedback shift register

8.2 Proposed image encryption algorithm

The proposed IEA consists of four steps: key generation for Tinkerbell map, sequence generation using Tinkerbell map, two-step permutation, and two-step diffusion process. All of these steps are performed to modify the image, which results in an encrypted image. The Figure 8.3 shows the flow diagram of the IEA that involves a two-step permutation process and a two-step diffusion process. The goal of the confusion process is to hide the relationship between the plaintext and the key. Diffusion asserts that if one bit of the plaintext is altered, half the number of bits in the ciphertext should change, and similarly, if a single bit of the ciphertext is changed, about half of the plaintext bits should change. The goal of the Diffusion process is to conceal the statistical relationship between the ciphertext and the plaintext.

For encrypting an image P of size $M \times N$, the first step is to obtain the two initial seeds for the Tinkerbell map. The initial seed for the Tinkerbell map is generated using (8.2.1).

$$\begin{aligned} x_0 &= \frac{\sum_{i=1}^M \sum_{j=1}^{\frac{N}{2}} P_{i,j}}{M \times \frac{N}{2} \times 256}, \\ y_0 &= \frac{\sum_{i=1}^M \sum_{j=\frac{N}{2}}^N P_{i,j}}{M \times \frac{N}{2} \times 256} \end{aligned} \quad (8.2.1)$$

Using the initial seeds x_0 and y_0 obtained from (8.2.1) and the parameters described in section 8.1.1, the Tinkerbell map is used to generate a 2D sequence of length $4 \times$

142

$\max(M, N)$. Using the first dimension of obtained Tinkerbell map, two sequences X_1 and X_2 of size M are obtained after ignoring the initial few terms so that both sequences X_1 and X_2 are non-overlapping. Similarly, another two sequences Y_1 and Y_2 of size N are extracted using the second dimension of the Tinkerbell map. Further, the sequences X_1, X_2, Y_1 and Y_2 are sorted and their indices are stored in $X_1^{ind}, Y_1^{ind}, X_2^{ind}$ and Y_2^{ind} respectively, for implementing the two-step permutation processes described in (8.2.2) and (8.2.3). Here, the first level permutation of the image pixels is implemented using the index sequence X_1^{ind}, Y_1^{ind} and C_1 is obtained using the plain image P as described in (8.2.2).

$$C_1[X_1^{ind}[i], Y_1^{ind}[j]] = P[i, j] \quad (8.2.2)$$

In continuation, the second step of the permutation process is performed using the other index sequences (X_2^{ind}, Y_2^{ind}) and C_2 is obtained using C_1 as described in (8.2.3).

$$C_2[X_2^{ind}[i], Y_2^{ind}[j]] = C_1[i, j] \quad (8.2.3)$$

The C_2 is the permuted image obtained after a two-step permutation process. Now, the pixels of C_2 are to be diffused. A two-step diffusion task is performed using the sequences of LFSR and Logistic map. In the first step of the diffusion process, LFSR is utilised to obtain sequence of length $250 + M \times N$ using the parameters described in Section 8.1.2 and the sequence K having elements equivalent to the size of C_2 is extracted after ignoring the initial few terms. The element-wise XOR operation is performed between the sequence K and C_2 , and the first-level diffused image C_3 is obtained using (8.2.4).

$$C_3[i, j] = C_2[i, j] \oplus K[i, j] \quad (8.2.4)$$

Further, for the second level of the diffusion process, the Logistic map is utilised. A chaotic sequence of length $250 + M \times N$ is obtained using the parameters described in (4.1.2), and the sequence L having elements equivalent to the size of C_3 is extracted after ignoring the initial few terms. The element-wise XOR operation is performed between the sequence L and C_3 , and the second-level diffused image C is obtained using (8.2.5).

$$C[i, j] = C_3[i, j] \oplus L[i, j] \quad (8.2.5)$$

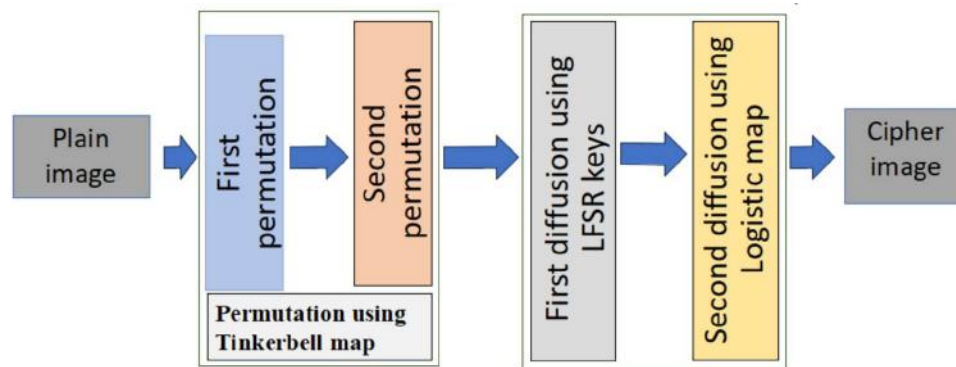


Figure 8.3: Proposed image encryption algorithm.

Since the encryption and decryption processes are symmetric, the decryption process involves the inverse steps of the encryption process. First, inverse diffusion is applied using the sequences of Logistic map. In the second step, LFSR sequences are used to diffuse the pixels. At last, the inverse permutation is applied using the Tinkerbell map.

8.3 Analysis of the image encryption algorithm

To assess the security and efficiency of the proposed IEA, we perform a set of tests on cipher images. Furthermore, the proposed IEA's effectiveness and resilience are compared to various encryption algorithms in terms of information entropy, NPCR, UACI, correlation coefficient and execution time.

8.3.1 Information entropy analysis

Table 8.1 presents the information entropy values of cipher images generated by the proposed IEA and other existing algorithms. The entropy values for images encrypted using proposed IEA are consistently close to the ideal value of 8, which indicates a high level of randomness. This suggests that the proposed IEA effectively distributes pixel values across the cipher image in a uniform manner, minimizing any detectable patterns. Such a distribution is essential for secure encryption, as it makes it significantly more difficult for an attacker to retrieve meaningful information through statistical analysis. Compared to other algorithms, the proposed IEA shows superior performance in terms of entropy, reflecting its enhanced ability to obscure the plain

144

image content.

Table 8.1: Comparison of information entropy values of the proposed IEA with algorithms available in the literature.

Image	Proposed IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	7.9993	7.9993	7.9993	7.9993	7.9793	7.9994	7.9993	7.9992	7.9993	7.9993	7.9992	7.9993	7.9992	7.9993
mandrill	7.9993	7.9993	7.9993	7.9993	7.9793	7.9993	7.9992	7.9992	7.9994	7.9993	7.9993	7.9992	7.9993	7.9993
MI3256	7.9975	7.9975	7.9970	7.9976	7.9766	7.9976	7.9969	7.9973	7.9973	7.9969	7.9971	7.9968	7.9970	7.9974
1.4.01	7.9978	7.9998	7.9998	7.9998	7.9798	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.02	7.9997	7.9998	7.9998	7.9998	7.9795	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.03	7.9995	7.9998	7.9998	7.9998	7.9800	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997
1.4.04	7.9994	7.9998	7.9998	7.9998	7.9796	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998
1.4.05	7.9998	7.9998	7.9987	7.9998	7.9799	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998
barb512	7.9993	7.9992	7.9993	7.9994	7.9792	7.9993	7.9993	7.9993	7.9993	7.9993	7.9992	7.9992	7.9993	7.9994
black	7.9970	7.9973	7.9974	7.9969	7.9765	7.9952	7.9973	7.9964	7.9973	7.8208	7.9969	7.9971	7.9973	7.9972
boat512	7.9943	7.9994	7.9994	7.9993	7.9785	7.9992	7.9993	7.9992	7.9994	7.9993	7.9992	7.9992	7.9992	7.9991
bridge256	7.9973	7.9972	7.9967	7.9971	7.9759	7.9972	7.9972	7.9972	7.9968	7.9972	7.9970	7.9970	7.9973	7.9978
peppers512	7.9914	7.9993	7.9992	7.9992	7.9801	7.9993	7.9992	7.9993	7.9993	7.9993	7.9993	7.9993	7.9993	7.9973
squares	7.9975	7.9973	7.9976	7.9972	7.9777	7.9964	7.9972	7.9967	7.9970	7.9887	7.9973	7.9971	7.9967	7.9748
zelda512	7.9993	7.9993	7.9993	7.9993	7.9798	7.9994	7.9992	7.9993	7.9992	7.9993	7.9994	7.9993	7.9993	7.9798

8.3.2 Differential attack

Table 8.2 and Table 8.3 present a comparative analysis of NPCR and UACI values for various encrypted images using different encryption algorithms. The results clearly demonstrate that the proposed IEA consistently achieves NPCR and UACI values close to the ideal across all tested images. In contrast, other related algorithms often show inconsistencies or fail to meet the ideal thresholds. This consistent performance of the proposed IEA confirms its robustness and high sensitivity to minor changes in the input image. Therefore, it can be concluded that proposed IEA is highly effective in resisting differential attacks, offering superior security in image encryption applications.

Table 8.2: Comparison of NPCR values of proposed IEA with algorithms available in the literature.

Image	Proposed IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	99.6101	99.6147	99.6155	99.5972	99.5922	99.6040	99.5941	99.6098	99.6021	99.3977	99.6075	99.6185	99.6227	99.6300
mandrill	99.5922	99.5995	99.6223	99.6098	99.6227	99.5907	99.6017	99.6071	99.6181	99.3660	99.6162	99.6117	99.6143	99.6056
MI3256	99.6109	99.6368	99.6338	99.6307	99.6201	99.6307	99.5697	99.5804	99.6170	99.5010	99.5758	99.6445	99.6170	99.6506
1.4.01	99.6019	99.6017	99.6119	99.6047	99.6095	99.6055	99.6004	99.6016	99.6094	99.2376	99.6137	99.6105	99.6087	99.6186
1.4.02	99.6048	99.6178	99.2304	99.6016	99.5851	99.6078	99.6171	99.6158	99.6206	99.3032	99.6078	99.6198	99.6039	99.6016
1.4.03	99.6231	99.6131	99.6104	99.6117	99.5970	99.6053	99.5976	99.5954	99.6041	99.3378	99.6108	99.6051	99.6018	99.6116
1.4.04	99.6019	99.6063	99.6156	99.6027	99.5928	99.6126	99.6191	99.6081	99.6041	99.2588	99.6128	99.6103	99.6115	99.6816
1.4.05	99.6065	99.6119	99.6124	99.6099	99.6026	99.6067	99.6046	99.6120	99.6107	99.3029	99.6118	99.6052	99.6138	99.6056
barb512	99.6017	99.6212	99.6120	99.6090	99.5857	99.6128	99.6120	99.6235	99.5987	99.2863	99.6033	99.5983	99.6037	99.6068
black	99.6041	0.1099	99.5804	99.5712	99.6140	99.6170	99.5956	99.6201	99.6429	99.1058	99.6033	99.6307	99.6033	99.5816
boat512	99.6028	99.6048	99.5777	99.6006	99.5861	99.6071	99.6078	99.6094	99.5998	99.2355	99.6315	99.6002	99.6113	99.5916
bridge256	99.6201	99.6368	99.5834	99.6140	99.6277	99.6201	99.5895	99.5941	99.5941	99.3973	99.6475	99.5911	99.5804	99.6126
peppers512	99.6155	99.6181	99.2203	99.5914	99.6006	99.6208	99.6105	99.6296	99.5872	99.3664	99.6166	99.6014	99.5987	99.6316
squares	99.6216	94.4611	99.6475	99.6277	99.6323	99.5667	99.6078	99.5621	99.5850	99.4827	99.6216	99.5651	99.5880	99.6326
zelda512	99.6048	99.6094	99.6140	99.5838	99.6067	99.6075	99.6338	99.6117	99.6006	99.3492	99.6140	99.6147	99.5869	99.6015

Table 8.3: Comparison of UACI values of the proposed IEA with algorithms available in the literature.

Image	Proposed IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	33.4649	33.4596	33.5119	33.4700	32.9488	33.4450	33.5427	33.5215	33.4590	33.3533	33.4218	33.5017	33.4631	33.5303
mandrill	33.4641	33.4832	33.4239	33.4253	33.0260	33.5148	33.4519	33.4471	33.4134	33.4041	33.5828	33.4677	33.5044	33.5228
MI3256	33.4285	33.3253	33.4193	33.4883	32.9003	33.4463	33.3935	33.5144	33.3942	33.5231	33.4326	33.2599	33.4790	33.5028
1.4.01	33.4278	33.3913	33.4613	33.4565	32.9516	33.4375	33.5184	33.4723	33.4479	33.3781	33.4802	33.4677	33.4773	33.4623
1.4.02	33.4215	33.4699	33.4710	33.4742	32.9929	33.4595	33.4946	33.4569	33.4687	33.3739	33.4457	33.4705	33.4728	33.4723
1.4.03	33.4727	33.4715	33.4395	33.4577	33.0346	33.4021	33.4991	33.4078	33.4670	33.3811	33.5185	33.4597	33.4215	33.4613
1.4.04	33.4904	33.4039	33.4475	33.4472	33.0237	33.4591	33.4167	33.4458	33.4396	33.3817	33.4967	33.4753	33.4386	33.4821
1.4.05	33.5091	33.4528	33.4414	33.4823	33.0187	33.4546	33.4811	33.4362	33.4326	33.3856	33.4754	33.4869	33.4366	33.4753
barb512	33.5017	33.4903	33.4525	33.4480	33.0039	33.5036	33.4419	33.5271	33.4796	33.3738	33.4139	33.4472	33.4584	33.4427
black	33.3870	0.0020	33.3606	33.4630	33.0262	33.1236	33.4295	33.4112	33.5089	32.1387	33.5901	33.4486	33.3485	33.4629
boat512	33.4745	33.4335	33.4126	33.4923	33.0314	33.4694	33.4611	33.4229	33.4362	33.3233	33.4689	33.4232	33.3889	33.4657
bridge256	33.4565	33.5100	33.5284	33.3681	32.9774	33.5488	33.4616	33.4363	33.4427	33.4126	33.4118	33.4083	33.4107	33.4123
peppers512	33.5046	33.4297	33.3951	33.5148	33.1133	33.4624	33.4268	33.4878	33.4425	33.4498	33.5125	33.5270	33.4002	33.4520
squares	33.4102	32.9945	33.3971	33.4567	33.1512	33.2762	33.2801	33.4679	33.3559	33.6037	33.4768	33.3543	33.4032	33.4721
zelda512	33.4529	33.4063	33.4575	33.4738	33.0454	33.4410	33.3448	33.4264	33.4418	33.3973	33.4772	33.5236	33.4646	33.4603

8.3.3 Histogram analysis

Figure 8.4 exhibits a comparative analysis of the histograms of both the plain and cipher images. By examining the Figure 8.4, it becomes clear that a significant transformation occurs in the statistical distribution of pixel intensities following the IEA. In the case of the plain images, the histograms typically display noticeable patterns and peaks, reflecting the inherent structure and redundancy within natural images (Figure 8.4(a-c)). These patterns can often reveal information about the image content, making plain images vulnerable to statistical analysis and attacks.

The histograms corresponding to the cipher images appear to be uniformly distributed, indicating that the IEA has effectively randomized the pixel values across the entire gray-scale range (Figure 8.4(d-f)). This uniformity suggests a high level of entropy and demonstrates that the encrypted images do not retain any visible statistical correlation with the plain images. The absence of identifiable peaks or patterns in the histograms of cipher images confirm that the IEA has successfully obscured the plain image information. As a result, such uniform histograms are a strong indication of a robust IEA, as they significantly hinder any attempts by unauthorized parties to extract meaningful information through statistical or visual analysis.

146

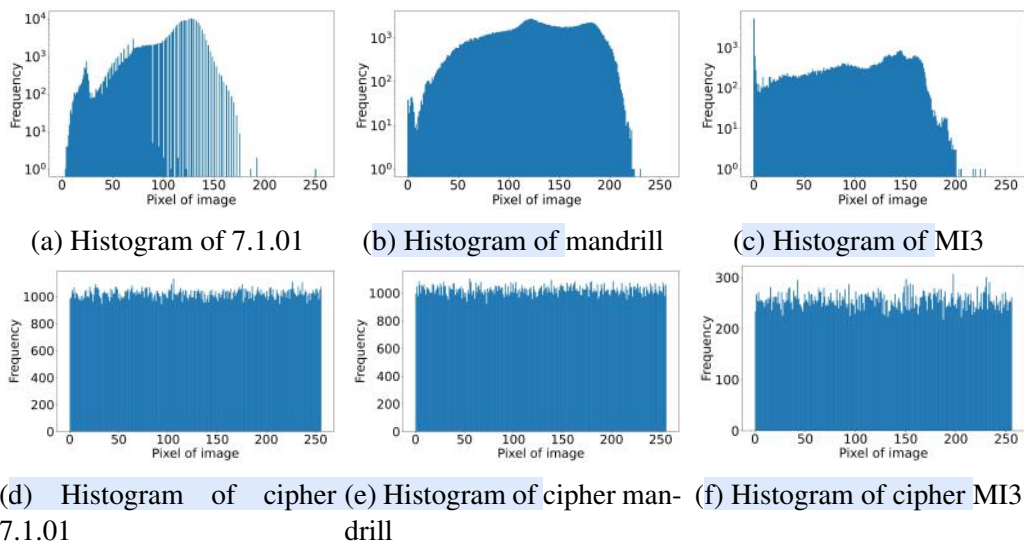


Figure 8.4: Histogram of plain and cipher images

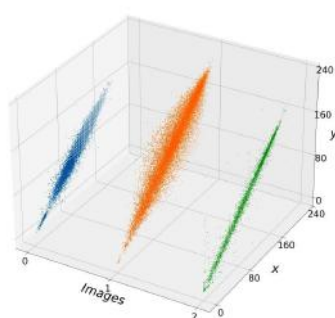
8.3.4 Correlation Coefficient analysis

The correlation coefficients between adjacent pixels in both the plain and cipher images have been computed and are presented in Table 8.4. As observed from the Table 8.4, the plain images exhibit very high correlation coefficients, with values close to 1. This indicates a strong relationship between adjacent pixels, which is common in plain images. In contrast, the cipher images demonstrate significantly lower correlation coefficients, suggesting that the encryption process has effectively disrupted the pixel relationships, resulting in minimal to no correlation between adjacent pixels. That shows the efficiency of the IEA in reducing statistical information.

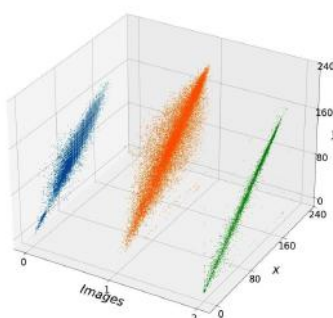
In addition, the pixel intensity distribution is illustrated in Figure 8.5. For the plain images shown in Figure 8.5 (a-c), the pixel values are highly concentrated and follow a linear pattern, reflecting their structured nature. However, for the cipher images exhibited in Figure 8.5 (d-f), the pixel values are distributed uniformly across the region. This uniform distribution is a strong indication of efficient encryption, as it implies a complete loss of the plain image information and an absence of any detectable patterns.

Table 8.4: Comparison of correlation coefficient values of proposed IEA with algorithms available in the literature.

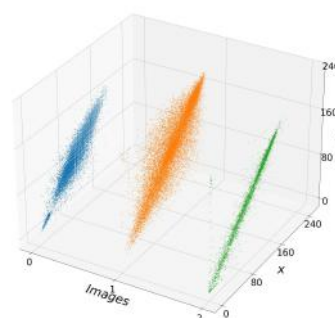
Image	Plain images	Proposed IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	HD 0.9630	-0.0031	-0.0041	0.0009	-0.0028	-0.0046	0.0049	0.0008	0.0091	0.0037	-0.0032	-0.0012	0.0012	-0.0027	0.0002
	VD 0.9192	-0.0027	0.0023	0.0008	-0.0009	-0.0017	0.0025	0.0012	-0.0106	0.0002	0.0029	0.0075	-0.0080	0.0059	-0.0105
	DD 0.8995	-0.0017	0.0148	-0.0038	0.0045	-0.0046	-0.0137	0.0038	0.0151	0.0001	-0.0036	0.0007	0.0058	0.0057	0.0069
mandrill	HD 0.8625	-0.0012	-0.0029	-0.0016	0.0069	0.0047	-0.0101	0.0082	0.0127	0.0087	0.0097	-0.0032	-0.0019	0.0060	0.0028
	VD 0.7669	0.0051	-0.0035	-0.0076	-0.0074	0.0031	0.0046	-0.0105	0.0064	-0.0020	-0.0024	-0.0076	-0.0072	0.0087	-0.0067
	DD 0.7202	-0.0044	-0.0099	0.0052	0.0102	0.0035	-0.0040	0.0090	-0.0043	0.0055	-0.0047	0.0075	-0.0033	0.0091	-0.0040
MI3256	HD 0.9784	0.0019	-0.0172	-0.0054	0.0043	0.0187	-0.0158	0.0152	-0.0273	0.0086	-0.0039	0.0080	-0.0247	0.0130	-0.0091
	VD 0.9795	0.0054	-0.0049	-0.0162	0.0194	-0.0012	-0.0072	-0.0083	0.0156	-0.0011	-0.0020	0.0026	0.0141	0.0152	0.0014
	DD 0.9405	0.0074	0.0052	0.0041	-0.0056	0.0160	0.0035	0.0089	0.0208	-0.0093	0.0226	0.0107	-0.0062	-0.0049	0.0085



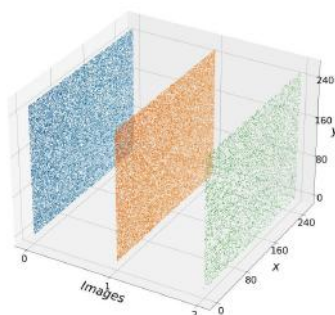
(a) Horizontal direction



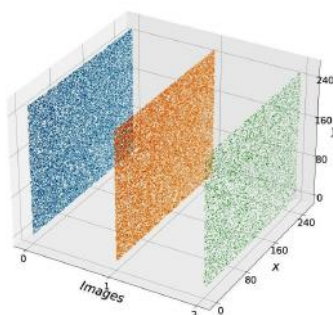
(b) Vertical direction



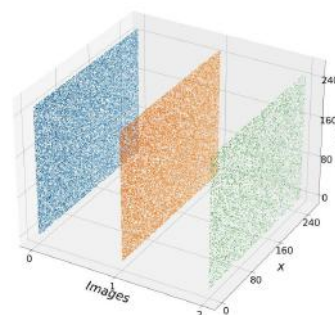
(c) Diagonal direction



(d) Horizontal direction



(e) Vertical direction



(f) Diagonal direction

Figure 8.5: Pixel distribution of plain and cipher images obtained using proposed IEA.

148

8.3.5 Resistance to classical attacks

The robustness of proposed IEA against chosen-plaintext attacks is established through Equation (2.3.8). The operation is visually represented in Figure 8.6. By examining Figure 8.6(a),(b), it is clear that (2.3.8) holds, suggesting that the IEA resists chosen-plaintext attacks. Additionally, a quantitative evaluation is carried out by calculating the value of NPCR for the images displayed in Figure 8.6(a) and Figure 8.6(b). The resulting NPCR value between these two images is 99.6297%, further reinforcing the IEA's effectiveness against chosen-plaintext attacks. Therefore, the proposed IEA is also expected to be resilient against other classical attacks.

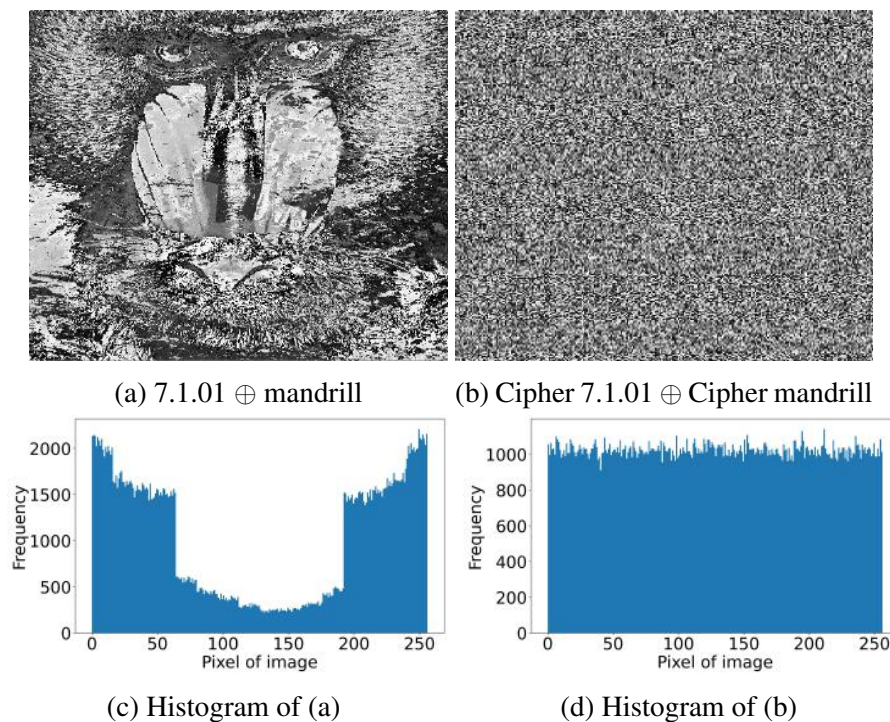
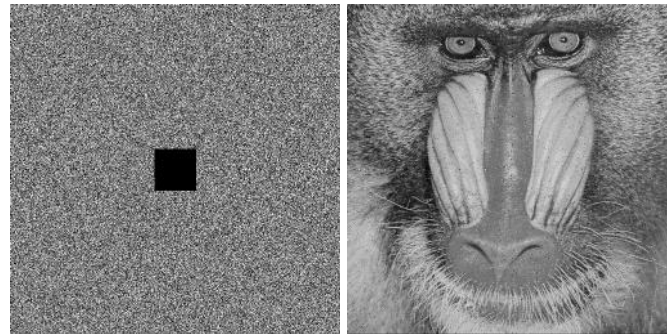


Figure 8.6: Resistance to classical attacks

8.3.6 Occlusion attack

To analyse the strength of the decryption algorithm against the occlusion attack, a small portion of the encrypted image was corrupted. The corrupted image is shown in Figure 8.7(a). The corresponding decrypted image of the occluded images is shown in the Figure 8.7(b). The decrypted image retains most of the original visual content,

indicating that the proposed encryption and decryption process is effective even under partial data loss. This demonstrates that the IEA exhibits strong resistance to occlusion attacks, making it a reliable solution for secure image transmission in lossy or error-prone environments.



(a) Cropped encrypted image (b) Decryption of cropped image

Figure 8.7: Representation of proposed IEA's resistance to cropping attack

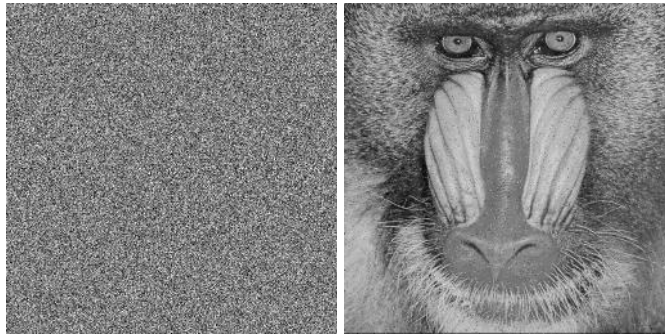
8.3.7 Noise attack

To assess the resilience of the decryption algorithm against noise attacks, salt-and-pepper noise was introduced randomly into the encrypted image prior to decryption. The noise-corrupted encrypted image is depicted in Figure 8.8(a), while the corresponding decrypted image is shown in Figure 8.8(b). Despite the presence of noise, the decrypted image preserves the overall structure and visual features of the original, indicating that the proposed encryption and decryption scheme can effectively tolerate such distortions. These results confirm that the IEA is robust against noise attacks and suitable for secure image transmission over noisy communication channels.

8.3.8 NIST randomness test

Table 8.5 presents the p -values computed at a significance level of $\beta = 0.01$ for all fifteen statistical tests applied to the cipher image generated using the proposed IEA. As shown in the Table 8.5, the cipher image successfully passes all the randomness tests, indicating that the proposed IEA effectively introduces randomness in the encrypted images.

150



(a) Noisy encrypted image (b) Decryption of noisy image

Figure 8.8: Representation of proposed IEA's resistance to Noise attack

Table 8.5: Randomness test results for proposed IEA.

Test name	p-value	Result
Frequency Test	0.8087	Successful
Run Test	0.9649	Successful
Run Test (Longest Run of Ones)	0.2257	Successful
Block Frequency Test	0.9909	Successful
Universal Statistical Test	0.1367	Successful
Linear Complexity Test	0.4793	Successful
Serial Test	0.8064	Successful
Binary Matrix Rank Test	0.8871	Successful
Non-overlapping Template Matching Test	0.7068	Successful
Overlapping Template Matching Test	0.2439	Successful
Approximate Entropy Test	0.9106	Successful
Random Excursion Test	0.1624	Successful
Random Excursion Variant Test	0.5542	Successful
Cumulative Sums	0.6421	Successful
Discrete Fourier Transform Test	0.9342	Successful

8.3.9 Execution time analysis

The execution time of the proposed IEA is presented in Table 8.6. As shown in Table 8.6, the execution time for proposed IEA is comparatively higher than that of certain other algorithms available in literature, it offers enhanced robustness and superior security features [59, 82, 33]. This trade-off between time and performance indicates that while proposed IEA may require more processing time, it compensates with greater resilience against several attacks.

Table 8.6: Comparison of execution time (in seconds) of the proposed IEA with algorithms available in the literature.

Image	Proposed IEA	[60]	[46]	[59]	[76]	[82]	[33]	[85]	[86]	[87]	[88]	[89]	[78]	[91]
7.1.01	1.86	3.29	10.20	1.41	19.46	0.60	1.27	20.61	3.85	4.40	1.93	17.78	537.61	908.52
mandrill	1.72	3.15	8.80	1.66	21.26	0.57	1.30	18.51	5.27	4.03	2.27	15.01	524.53	759.84
MI3256	0.44	0.80	2.20	0.38	5.96	0.13	0.33	4.77	1.13	0.99	0.70	4.29	153.90	265.17

8.4 Summary

In this chapter, we have proposed an IEA leveraging the Tinkerbell map, Logistic map and LFSR. The sequences obtained by the Tinkerbell map are used to shuffle the pixels of the plain image. While, the sequences generated by Logistic map and LFSR are used to modify the pixel values. The performance of the proposed proposed IEA is rigorously evaluated using a diverse set of gray-scale images to ensure its applicability across different visual content. Comprehensive experimental analyses are conducted to assess the algorithm's robustness against multiple types of attacks, including statistical, differential, and brute-force attacks. The results confirm that the IEA effectively disrupts the inherent correlations in image data, ensuring high security. Furthermore, the corresponding decryption algorithm reconstructs the plain image content, demonstrating the algorithm's reliability and lossless recovery capability.

Chapter 9

Conclusion, Future Scope and Social Impact

This chapter serves as the concluding part of the thesis, structured into three distinct sections. Section 9.1 summarizes the research work, recapping proposed chaotic maps, their cryptographic strengths, and the performance of image encryption algorithms. Section 9.2 outlines potential research directions to build upon this work, including hardware implementation, advanced cryptanalysis, and applications to other data types. Finally, Section 9.3 discusses the broader implications of the research, linking the encryption algorithms to societal benefits and United Nations Sustainable Development Goals.

9.1 Conclusion

In this thesis, we have proposed several novel chaotic maps designed to overcome the limitations inherent in traditional chaotic maps. We have evaluated and compared the performance of proposed maps with existing maps in terms of bifurcation diagram, phase diagram, Lyapunov exponent, sample entropy and permutation entropy. The proposed chaotic maps exhibit strong dynamical behavior, including uniform distribution without pattern clustering, high positive Lyapunov exponents, and a wide range of

control parameters.

These chaotic maps have been employed as pseudo-random number generators (PRNGs) for image security applications. The encryption algorithms leveraging the proposed chaotic maps are demonstrated to be both robust and efficient, exhibiting strong resistance to multiple types of cryptographic attacks. Moreover, the decryption process reliably recovers the original image data without any loss, ensuring lossless recovery.

In Chapter 3, we studied the Zirili test optimization function, which is characterized by multiple local minima, despite having a global minimum at zero. The proposed Zirili chaotic map exhibits uniform output distribution, high Lyapunov exponents, complex bifurcation diagram along with high entropy values. These properties confirm its suitability for cryptographic applications like encryption. Its integration into an image encryption algorithm has shown significant efficiency and robustness. Furthermore, the introduction of novel cascading confusion transformation and modified cyclic diffusion with pixel mixing operations has considerably enhanced the algorithm's overall security.

In Chapter 4, we analyzed classical chaotic maps such as the Kaplan-Yorke map and the Logistic map, identifying their limited chaotic range and relatively low or negative Lyapunov exponents. To address these limitations, we introduced coupled Kaplan-Yorke-Logistic map. The map achieves improved chaotic characteristics, including a large control parameter range, high positive Lyapunov exponents, complex bifurcation diagram, and high entropy values. Its application to image encryption proves to be both effective and secure, further strengthened by the implementation of a simultaneous confusion-diffusion strategy.

In Chapter 5, we proposed the SHIELD map, utilizing established functions such as the exponential, sine, and logistic functions. The map demonstrates evenly distributed trajectories, high Lyapunov exponents, large control parameter range along with high entropy values. The SHIELD-based image encryption algorithm is both robust and efficient. Additionally, the introduction of a two-step confusion process and a dynamic diffusion mechanism significantly elevates the security of image encryption algorithm.

In Chapter 6, we proposed two novel extensions of existing $e\pi$ -map termed as a two-dimensional Sine- $e\pi$ map and a three-dimensional Non-linear Sine hyper-chaotic map.

The map demonstrates evenly distributed trajectories, high Lyapunov exponents, large control parameter range along with high entropy values. These maps were successfully utilized in the development of an image encryption algorithm, which demonstrated high robustness and efficiency in securing image data.

In Chapter 7, we introduced the Zirili-Logistic map developed by combining the functions namely Zirili function, sine, exponential, and Logistic map. The proposed map generates a rich spectrum of chaotic dynamics in terms of large range of chaotic parameters, high Lyapunov exponents, ergodic behavior in phase diagram, and a complex bifurcation diagram. In addition, we proposed a magic square matrix-based FSM to scramble the locations of the pixels within an image. These components form the core of a proposed image encryption algorithm, that is validated to be both highly efficient and resistant to cryptographic attacks.

In chapter 8 we studied the Tinkerbell map, the Logistic map, and linear feedback shift registers. Combining the maps, we designed an image encryption algorithm utilising two-step confusion and two-step diffusion operation. The resulting algorithm is shown to be secure and computationally efficient.

The proposed image encryption algorithms have been rigorously evaluated using a diverse set of test images to assess their performance and security characteristics. The results comprehensively demonstrate that the cipher images produced by these algorithms possess strong statistical properties and cryptographic robustness. This includes high entropy, uniform histograms, low correlation coefficients, high NPCR and UACI values, and pronounced sensitivity to initial conditions and encryption keys. The randomness of the encrypted images was further validated through the NIST SP 800-22 statistical test suite confirming that the encrypted images are indistinguishable from true random sequences, effectively resisting any statistical-attacks. Furthermore, the algorithms were proven to be highly resistant to chosen-plaintext attacks, as even minimal alterations in the input image or encryption key produce completely unrelated cipher images, preventing an adversary from deducing the key through analysis of chosen plaintext-ciphertext pairs. All proposed algorithms exhibit significant computational efficiency. They effectively resist brute-force, statistical, and differential attacks. The proposed algorithms are suitable for real-world image security applications due to

156

their speed, reliability, and proven strong cryptographic features.

9.2 Future Scope

While the proposed encryption algorithms demonstrate robust theoretical performance, several research avenues merit further investigation to enhance their practical applicability and security assurance. Future work can be structured into four key directions:

1. **Hardware Implementation:** Transitioning from software simulation to physical realization represents the most immediate priority. This entails implementing the algorithms on FPGA platforms to quantify real-world performance metrics (throughput, latency, power consumption, and resource utilization), followed by potential ASIC design for optimal efficiency in embedded systems.
2. **Advanced Security Cryptanalysis:** To ensure long-term viability, security evaluation must extend beyond standard statistical tests. Future analysis should include resistance to sophisticated adversarial models, such as side-channel attacks (power analysis, timing attacks) and fault injection attacks. Furthermore, an assessment of quantum resistance is crucial to evaluate vulnerability to attacks and to explore potential post-quantum enhancements.
3. **Multi-Media and Complex Data Applications:** The framework's applicability to other data types remains unexplored. Promising directions include adapting the algorithm for real-time video encryption by leveraging inter-frame correlations, and extending it to one-dimensional signals like audio. Validation on complex data structures, such as 3D medical images (CT, MRI) and hyper-spectral imagery, would demonstrate significant versatility.
4. **Standardization and Practical Integration:** For widespread adoption, rigorous benchmarking against established standards (e.g., AES-GCM) and state-of-the-art chaos-based techniques using unified datasets is essential. Subsequently, developing end-to-end encryption protocols for specific use-cases, such as secure messaging or authenticated cloud storage, would bridge the gap between

algorithmic innovation and real-world deployment.

9.3 Social Impact

The proposed image encryption algorithms transcend theoretical contribution, offering tangible benefits that address pressing societal challenges and align with key United Nations Sustainable Development Goals (SDGs). By safeguarding visual data, this framework helps build a foundational layer of digital trust essential for a secure and equitable digital future.

SDG 9: Industry, Innovation, and Infrastructure: The research embodies the technological upgrading. It fosters resilient digital infrastructure by protecting critical visual data in sectors like energy, transportation, and manufacturing from cyber threats, which is essential for economic stability and growth (SDG Target 9.5).

SDG 11: Sustainable Cities and Communities: In the context of smart cities, encrypting data streams from vast surveillance networks helps protect citizen privacy and prevent misuse. This ensures that smart city technologies enhance public safety without leading to surveillance overreach, contributing to safer and more inclusive urban environments (SDG Target 11.7).

SDG 16: Peace, Justice, and Strong Institutions: The technology strengthens institutions by enabling secure digital identity systems. Encrypting biometric data (e.g., fingerprints, facial images) in national ID programs helps prevent identity theft and fraud, promoting just and accountable institutions. It also empowers civil society by allowing the secure sharing of visual evidence (SDG Target 16.6).

SDG 17: Partnerships for the Goals: The universal need for data privacy creates a platform for international collaboration. The underlying principles of this framework can be shared globally, fostering partnerships between researchers, industries, and governments to develop interoperable security standards (SDG Target 17.6).

From securing personal communications on messaging apps and social media to enabling confidential e-commerce and banking, the proposed encryption algorithms

158

ensure practical security benefits in everyday life. By aligning with these SDGs, the work is positioned not merely as an algorithmic advancement but as a crucial enabler for sustainable digital development.

Bibliography

- [1] Majid Khan, Fahad Aljuaydi, Lal Said, and Muhammad Amin. A secure chaotic cryptosystem for thermal Imaging: Logistic map-based encryption with substitution-diffusion and spatial decorrelation. *Journal of Radiation Research and Applied Sciences*, 18(2):101546, 2025. ISSN 1687-8507. doi: <https://doi.org/10.1016/j.jrras.2025.101546>.
- [2] Ibrahim Yasser, Abeer T. Khalil, Mohamed A. Mohamed, Ahmed S. Samra, and Fahmi Khalifa. A Robust Chaos-Based Technique for Medical Image Encryption. *IEEE Access*, 10:244–257, 2022. doi: 10.1109/ACCESS.2021.3138718.
- [3] Alireza A. Arab, Mohammad Javad B. Rostami, and Behnam Ghavami. An image encryption algorithm using the combination of chaotic maps. *Optik*, 261:169122, 2022. ISSN 0030-4026. doi: <https://doi.org/10.1016/j.ijleo.2022.169122>.
- [4] Babak Rezaei, Mahvash Mobasseri, and Rasul Enayatifar. A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications. *Journal of Real-Time Image Processing*, 20(2):30, 2023.
- [5] A Sridevi, R Sivaraman, Varun Balasubramaniam, Sreenithi, Janakiraman Siva, V Thanikaiselvan, and Amirtharajan Rengarajan. On Chaos based duo confusion duo diffusion for colour images. *Multimedia Tools and Applications*, 81(12):16987–17014, 2022.
- [6] Ramesh Premkumar, Miroslav Mahdal, and Muniyandy Elangovan. An Efficient Chaos-Based Image Encryption Technique Using Bitplane Decay and Genetic Operators. *Sensors*, 22(20), 2022. ISSN 1424-8220. doi: 10.3390/s22208044.

160

- [7] Rijmen Vincent and Daemen Joan. Advanced encryption standard. In *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pages 19–22, 2001.
- [8] M.E. Smid and D.K. Branstad. Data Encryption Standard: past and future. *Proceedings of the IEEE*, 76(5):550–559, 1988. doi: 10.1109/5.4441.
- [9] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [10] Kedar Nath Singh, Om Prakash Singh, Naman Baranwal, and Amit Kumar Singh. An efficient chaos-based image encryption algorithm using real-time object detection for smart city applications. *Sustainable Energy Technologies and Assessments*, 53:102566, 2022.
- [11] Xingbin Liu, Shuyi Zheng, and Jing Yang. Image encryption scheme based on 2D-ICCM and bit-planes cross permutation-diffusion using parallel computing. *Computers and Electrical Engineering*, 127:110569, 2025. ISSN 0045-7906. doi: <https://doi.org/10.1016/j.compeleceng.2025.110569>.
- [12] Dilbag Singh, Sharanpreet Kaur, Mandeep Kaur, Surender Singh, Manjit Kaur, and Heung-No Lee. A systematic literature review on chaotic maps-based image security techniques. *Computer Science Review*, 54:100659, 2024. ISSN 1574-0137. doi: <https://doi.org/10.1016/j.cosrev.2024.100659>.
- [13] Kurunandan Jain, Aravind Aji, and Prabhakar Krishnan. Medical Image Encryption Scheme Using Multiple Chaotic Maps. *Pattern Recognition Letters*, 152:356–364, 2021. ISSN 0167-8655. doi: <https://doi.org/10.1016/j.patrec.2021.10.033>.
- [14] Pengfei Ding, Penghui Geng, and Weiwei Hu. A new controllable multi-wing chaotic system: applications in high-security color image encryption. *The Journal of Supercomputing*, 81(1):108, 2025.

- [15] Shashikant C Phatak and S Suresh Rao. Logistic map: A possible random-number generator. *Physical review E*, 51(4):3670, 1995.
- [16] Xiaoling Huang, Youxia Dong, Guodong Ye, and Yang Shi. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Frontiers of Computer Science*, 17(3):173804, 2023. doi: 10.1007/s11704-022-1419-8.
- [17] Huishan Wu, Guodong Ye, Wun-She Yap, and Bok-Min Goi. Reversible blind image hiding algorithm based on compressive sensing and fusion mechanism. *Optics & Laser Technology*, 167:109755, 2023.
- [18] Shufeng Huang, Linqing Huang, Shuting Cai, Xiaoming Xiong, and Yuan Liu. Novel and secure plaintext-related image encryption algorithm based on compressive sensing and tent-sine system. *IET Image Processing*, 2022. doi: 10.1049/ipr2.12429.
- [19] Huipeng Liu, Lin Teng, Yijia Zhang, Ruiying Si, and Pengbo Liu. Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. *Expert Systems with Applications*, 235:121090, 2024. doi: 10.1016/j.eswa.2023.121090.
- [20] Qiang Lai and Hanqiang Hua. Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Systems with Applications*, 264:125854, 2025. ISSN 0957-4174. doi: <https://doi.org/10.1016/j.eswa.2024.125854>.
- [21] Jinwen He, Hegui Zhu, and Xv Zhou. Quantum image encryption algorithm via optimized quantum circuit and parity bit-plane permutation. *Journal of Information Security and Applications*, 81:103698, 2024. doi: 10.1016/j.jisa.2024.103698.
- [22] Vivek Verma and Sanjeev Kumar. Quantum image encryption algorithm based on 3D-BNM chaotic map. *Nonlinear Dynamics*, 113(4):3829–3855, 2025.

162

- [23] Wassim Alexan, Yen-Lin Chen, Lip Yee Por, and Mohamed Gabr. Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption. *Symmetry*, 15(5):1081, 2023. doi: 10.3390/sym15051081.
- [24] C Madan Kumar, R Vidhya, and M Brindha. An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function. *Applied Intelligence*, 52(3):2556–2585, 2022. doi: 10.1007/s10489-021-02508-x.
- [25] Meng-meng Wang, Nan-run Zhou, Lu Li, and Man-tao Xu. A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank. *Expert Systems with Applications*, 207:118067, 2022. doi: 10.1016/j.eswa.2022.118067.
- [26] Xiao Jiang, Yiyuan Xie, Bocheng Liu, Junxiong Chai, Yichen Ye, Tingting Song, Manying Feng, and Haodong Yuan. Image encryption based on actual chaotic mapping using optical reservoir computing. *Nonlinear Dynamics*, 111(16):15531–15555, 2023.
- [27] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology—EUROCRYPT’91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10*, pages 127–140. Springer, 1991. doi: 10.1007/3-540-46416-6_11.
- [28] Wenhao Liu, Kehui Sun, and Congxu Zhu. A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84:26–36, 2016. ISSN 0143-8166. doi: <https://doi.org/10.1016/j.optlaseng.2016.03.019>. URL <https://www.sciencedirect.com/science/article/pii/S0143816616300173>.
- [29] Robert Devaney. *An introduction to chaotic dynamical systems*. CRC press, 2018.
- [30] Steven H Strogatz. *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. Chapman and Hall/CRC, 2024.

- [31] Akshat Tiwari, Prachi Diwan, Tarun Dhar Diwan, Mahdal Miroslav, and SP Samal. A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. *Scientific Reports*, 15(1):14151, 2025.
- [32] Xingbin Liu, Shuyi Zheng, and Jing Yang. Color image encryption scheme based on a novel 2D-CLCM chaotic system and RNA encoding. *Mathematics and Computers in Simulation*, 239:340–360, 2026. ISSN 0378-4754. doi: <https://doi.org/10.1016/j.matcom.2025.06.009>.
- [33] Uğur Erkan, Abdurrahim Toktas, Feyza Toktas, and Fayadh Alenezi. 2D $e\pi$ -map for image encryption. *Information Sciences*, 589:770–789, 2022. doi: 10.1016/j.ins.2021.12.126.
- [34] Yi Huang and Lili Zhou. A hyper-chaos-based image encryption scheme with double parity alternate scrambling. *Multimedia Tools and Applications*, pages 1–15, 2023.
- [35] Michael Crampin and Benedict Heal. On the chaotic behaviour of the tent map. *Teaching Mathematics and its Applications: An International Journal of the IMA*, 13(2):83–89, 1994.
- [36] T. Geisel and V. Fairen. Statistical properties of chaos in Chebyshev maps. *Physics Letters A*, 105(6):263–266, 1984. ISSN 0375-9601. doi: [https://doi.org/10.1016/0375-9601\(84\)90993-9](https://doi.org/10.1016/0375-9601(84)90993-9).
- [37] Jory Griffin.
- [38] Michael Benedicks and Lennart Carleson. The dynamics of the h  non map. *Annals of Mathematics*, 133(1):73–169, 1991.
- [39] J. Fridrich. Image encryption based on chaotic maps. In *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, volume 2, pages 1105–1110 vol.2, 1997. doi: 10.1109/ICSMC.1997.638097.

164

- [40] Alexandre Goldsztejn, Wayne Hayes, and Pieter Collins. Tinkerbell is chaotic. *SIAM Journal on Applied Dynamical Systems*, 10(4):1480–1501, 2011.
- [41] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of atmospheric sciences*, 20(2):130–141, 1963. doi: 10.1175/1520-0469(1963)020%3C0130:DNF%3E2.0.CO;2.
- [42] Piotr Zgliczynski. Computer assisted proof of chaos in the Rössler equations and in the Hénon map. *Nonlinearity*, 10(1):243, 1997.
- [43] Alenrex Maity and Bibhas Chandra Dhara. An Audio Encryption Scheme Based on Empirical Mode Decomposition and 2D Cosine Logistic Map. *IEEE Latin America Transactions*, 22(4):267–275, 2024. doi: 10.1109/TLA.2024.10472959.
- [44] Rui Wu, Suo Gao, Herbert Ho-Ching Iu, Shuang Zhou, Uğur Erkan, Abdurrahim Toktas, and Xianglong Tang. Securing Dual-Channel Audio Communication With a 2-D Infinite Collapse and Logistic Map. *IEEE Internet of Things Journal*, 11(6):10214–10223, 2024. doi: 10.1109/JIOT.2023.3325223.
- [45] Shi-xian Nan, Xiu-fang Feng, Yong-fei Wu, and Hao Zhang. Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM. *Nonlinear Dynamics*, 108(3):2705–2729, 2022. doi: 10.1007/s11071-022-07335-4.
- [46] Yuxiao Zheng, Qingye Huang, Shuting Cai, Xiaoming Xiong, and Linqing Huang. Image encryption based on novel Hill Cipher variant and 2D-IGSCM hyper-chaotic map. *Nonlinear Dynamics*, pages 1–19, 2024. doi: 10.1007/s11071-024-10324-4.
- [47] Zhongyun Hua, Fan Jin, Binxuan Xu, and Hejiao Huang. 2D Logistic-Sine-coupling map for image encryption. *Signal Processing*, 149:148–161, 2018. ISSN 0165-1684. doi: <https://doi.org/10.1016/j.sigpro.2018.03.010>.
- [48] Ning Mao, Xiaojun Tong, Miao Zhang, and Zhu Wang. Real-time image encryp-

tion algorithm based on combined chaotic map and optimized lifting wavelet transform. *Journal of Real-Time Image Processing*, 20(2):35, 2023.

- [49] Liu Shu-Bo, Sun Jing, Xu Zheng-Quan, and Liu Jin-Shuo. Digital chaotic sequence generator based on coupled chaotic systems. *Chinese Physics B*, 18(12): 5219, dec 2009. doi: 10.1088/1674-1056/18/12/019.
- [50] Zhongyun Hua, Yicong Zhou, Chi-Man Pun, and C.L. Philip Chen. 2D Sine Logistic modulation map for image encryption. *Information Sciences*, 297:80–94, 2015. ISSN 0020-0255. doi: <https://doi.org/10.1016/j.ins.2014.11.018>.
- [51] Zhongyun Hua and Yicong Zhou. Image encryption using 2D Logistic-adjusted-Sine map. *Information Sciences*, 339:237–253, 2016. ISSN 0020-0255. doi: <https://doi.org/10.1016/j.ins.2016.01.017>.
- [52] Hongjun Liu, Abdurahman Kadir, and Chengbo Xu. Color image encryption with cipher feedback and coupling chaotic map. *International Journal of bifurcation and chaos*, 30(12):2050173, 2020.
- [53] Xingyuan Wang and Pengbo Liu. A New Full Chaos Coupled Mapping Lattice and Its Application in Privacy Image Encryption. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(3):1291–1301, 2022. doi: 10.1109/TCSI.2021.3133318.
- [54] Lingfeng Liu, ZhiXiang Wei, and Hongyue Xiang. A novel image encryption algorithm based on compound-coupled logistic chaotic map. *Multimedia Tools and Applications*, 81(14):19999–20019, 2022.
- [55] Miaoting Hu, Jinqing Li, and Xiaoqiang Di. Quantum image encryption scheme based on 2D Sine 2-Logistic chaotic map. *Nonlinear Dynamics*, 111(3):2815–2839, 2023. doi: 10.1007/s11071-022-07942-1.
- [56] Madhu Sharma, Ranjeet Kumar Ranjan, and Vishal Bharti. An image encryption algorithm based on a novel hyperchaotic Hénon sine map. *Multimedia Tools and Applications*, 82(8):11949–11972, 2023. doi: 10.1007/s11042-022-13733-y.

166

- [57] Zezong Zhang, Jianeng Tang, Feng Zhang, Hui Ni, Jinyuan Chen, and Zhongming Huang. Color Image Encryption Using 2D Sine-Cosine Coupling Map. *IEEE Access*, 10:67669–67685, 2022. doi: 10.1109/ACCESS.2022.3185229.
- [58] Rui Wu, Suo Gao, Xingyuan Wang, Songbo Liu, Qi Li, Uğur Erkan, and Xianglong Tang. AEA-NCS: An audio encryption algorithm based on a nested chaotic system. *Chaos, Solitons & Fractals*, 165:112770, 2022. ISSN 0960-0779. doi: 10.1016/j.chaos.2022.112770.
- [59] Lin Teng, Xingyuan Wang, and Yongjin Xian. Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. *Information Sciences*, 605:71–85, 2022. doi: 10.1016/j.ins.2022.05.032.
- [60] Qiang Lai, Yuan Liu, and Liang Yang. Remote sensing image encryption algorithm utilizing 2D Logistic memristive hyperchaotic map and SHA-512. *Science China Technological Sciences*, 67(5):1553–1566, 2024. doi: 10.1007/s11431-023-2584-y.
- [61] Uğur Erkan, Abdurrahim Toktas, and Qiang Lai. 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Systems with Applications*, 213:119076, 2023. ISSN 0957-4174. doi: 10.1016/j.eswa.2022.119076.
- [62] Qiang Lai, Genwen Hu, Uğur Erkan, and Abdurrahim Toktas. A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Systems with Applications*, 213:118845, 2023.
- [63] Feyza Toktas, Uğur Erkan, and Zeki Yetgin. Cross-channel color image encryption through 2d hyperchaotic hybrid map of optimization test functions. *Expert Systems with Applications*, 249:123583, 2024. ISSN 0957-4174. doi: <https://doi.org/10.1016/j.eswa.2024.123583>.
- [64] Uğur Erkan, Abdurrahim Toktas, Samet Memiş, Qiang Lai, and Genwen Hu. An image encryption method based on multi-space confusion using hyperchaotic 2d vincent map derived from optimization benchmark function. *Nonlinear Dynamics*, 111(21):20377–20405, 2023.

- [65] Uğur Erkan, Abdurrahim Toktas, and Qiang Lai. Design of two dimensional hyperchaotic system through optimization benchmark function. *Chaos, Solitons & Fractals*, 167:113032, 2023.
- [66] Abdurrahim Toktas and Uğur Erkan. 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. *Neural Computing and Applications*, pages 1–25, 2022.
- [67] Abdurrahim Toktas, Uğur Erkan, and Deniz Ustun. An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm. *Nonlinear Dynamics*, 105(2):1885–1909, 2021. doi: 10.1007/s11071-021-06675-x.
- [68] Qiang Lai, Liang Yang, and Guanrong Chen. Two-Dimensional Discrete Memristive Oscillatory Hyperchaotic Maps With Diverse Dynamics. *IEEE Transactions on Industrial Electronics*, 72(1):969–979, 2025. doi: 10.1109/TIE.2024.3417974.
- [69] Qiang Lai, Yijin Liu, and Luigi Fortuna. Dynamical Analysis and Fixed-Time Synchronization for Secure Communication of Hidden Multiscroll Memristive Chaotic System. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 71(10):4665–4675, 2024. doi: 10.1109/TCSI.2024.3434551.
- [70] Qiang Lai and Genwen Hu. A Nonuniform Pixel Split Encryption Scheme Integrated With Compressive Sensing and Its Application in IoMT. *IEEE Transactions on Industrial Informatics*, 20(9):11262–11272, 2024. doi: 10.1109/TII.2024.3403266.
- [71] Qiang Lai and Liang Yang. Discrete memristor applied to construct neural networks with homogeneous and heterogeneous coexisting attractors. *Chaos, Solitons & Fractals*, 174:113807, 2023. ISSN 0960-0779. doi: <https://doi.org/10.1016/j.chaos.2023.113807>.
- [72] Robert Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1):29–42, 1989.

- [73] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06):1259–1284, 1998. doi: 10.1142/S021812749800098X.
- [74] Linhua Zhang, Xiaofeng Liao, and Xuebing Wang. An image encryption approach based on chaotic maps. *Chaos, Solitons & Fractals*, 24(3):759–765, 2005. ISSN 0960-0779. doi: <https://doi.org/10.1016/j.chaos.2004.09.035>. URL <https://www.sciencedirect.com/science/article/pii/S0960077904005600>.
- [75] Sahar Mazloom and Amir Masud Eftekhari-Moghadam. Color image encryption based on Coupled Nonlinear Chaotic Map. *Chaos, Solitons & Fractals*, 42(3):1745–1754, 2009. ISSN 0960-0779. doi: <https://doi.org/10.1016/j.chaos.2009.03.084>. URL <https://www.sciencedirect.com/science/article/pii/S0960077909002045>.
- [76] Lanhang Li, Yuling Luo, Senhui Qiu, Xue Ouyang, Lvchen Cao, and Shunbin Tang. Image encryption using chaotic map and cellular automata. *Multimedia Tools and Applications*, pages 1–19, 2022. doi: 10.1007/s11042-022-12621-9.
- [77] Shamsa Kanwal, Saba Inam, Fahima Hajjej, Omar Cheikhrouhou, Zainab Nawaz, Ayesha Waqar, Majid Khan, et al. A New Image Encryption Technique Based on Sine Map, Chaotic Tent map, and Circulant Matrices. *Security and Communication Networks*, 2022, 2022. doi: 10.1155/2022/4152683.
- [78] Xilin Liu, Xiaojun Tong, Zhu Wang, and Miao Zhang. A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation. *Multimedia Tools and Applications*, 81(15):21779–21810, 2022. doi: 10.1007/s11042-022-12472-4.
- [79] Walid El-Shafai, Fatma Khallaf, El-Sayed M El-Rabaie, and Fathi E Abd El-Samie. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, 12(10):9007–9035, 2021. doi: 10.1007/s12652-020-02597-5.

- [80] Jiming Zheng, Zheng Luo, and Qingxia Zeng. An efficient image encryption algorithm based on multi chaotic system and random DAN coding. *Multimedia Tools and Applications*, 79(39):29901–29921, 2020. doi: 10.1007/s11042-020-09454-9.
- [81] Pooja Mishra, Chiranjeev Bhaya, Arup Kumar Pal, and Abhay Kumar Singh. A medical image cryptosystem using bit-level diffusion with DNA coding. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–22, 2021. doi: 10.1007/s12652-021-03410-7.
- [82] Yongjin Xian and Xingyuan Wang. Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547:1154–1169, 2021. doi: 10.1016/j.ins.2020.09.055.
- [83] Wei Zhang, Shuwen Wang, Weijie Han, Hai Yu, and Zhiliang Zhu. An Image Encryption Algorithm Based on Random Hamiltonian Path. *Entropy*, 22(1):73, 2020. doi: 10.3390/e22010073.
- [84] Taiyong Li and Duzhong Zhang. Hyperchaotic image encryption based on multiple bit permutation and diffusion. *Entropy*, 23(5):510, 2021. doi: 10.3390/e23050510.
- [85] Xingyuan Wang, Nana Guan, Hongyu Zhao, Siwei Wang, and Yingqian Zhang. A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Scientific reports*, 10(1):9784, 2020. doi: 10.1038/s41598-020-66486-9.
- [86] Xiaosong Gao and Xingbin Liu. CLSM-IEA: a novel cosine-logistic-sine map and its application in a new image encryption scheme. *Signal, Image and Video Processing*, pages 1–15, 2024. doi: 10.1007/s11760-023-02971-8.
- [87] Zhen Le, Quanjun Li, Huang Chen, Shuting Cai, Xiaoming Xiong, and Linqing Huang. Medical image encryption system based on a simultaneous permutation and diffusion framework utilizing a new chaotic map. *Physica Scripta*, 99(5):055249, apr 2024. doi: 10.1088/1402-4896/ad3bf4.

170

- [88] Xilin Liu, Xiaojun Tong, Zhu Wang, and Miao Zhang. A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption. *Chaos, Solitons & Fractals*, 154:111693, 2022. ISSN 0960-0779. doi: 10.1016/j.chaos.2021.111693.
- [89] Xilin Liu, Xiaojun Tong, Zhu Wang, and Miao Zhang. Construction of controlled multi-scroll conservative chaotic system and its application in color image encryption. *Nonlinear Dynamics*, 110(2):1897–1934, 2022. doi: 10.1007/s11071-022-07702-1.
- [90] Omer Kocak, Uğur Erkan, Abdurrahim Toktas, and Suo Gao. PSO-based image encryption scheme using modular integrated logistic exponential map. *Expert Systems with Applications*, 237:121452, 2024. doi: 10.1016/j.eswa.2023.121452.
- [91] Xilin Liu, Xiaojun Tong, Miao Zhang, and Zhu Wang. A highly secure image encryption algorithm based on conservative hyperchaotic system and dynamic biogenetic gene algorithms. *Chaos, Solitons & Fractals*, 171:113450, 2023. ISSN 0960-0779. doi: 10.1016/j.chaos.2023.113450.
- [92] Kamlesh Kumar Raghuvanshi, Subodh Kumar, Sushil Kumar, and Sunil Kumar. Development of new encryption system using Brownian motion based diffusion. *Multimedia Tools and Applications*, 80(14):21011–21040, 2021. doi: 10.1007/s11042-021-10665-x.
- [93] Mohamed Zakariya Talhaoui and Xingyuan Wang. A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Information Sciences*, 550:13–26, 2021. doi: 10.1016/j.ins.2020.10.048.
- [94] Mingxu Wang, Xingyuan Wang, Tingting Zhao, Chuan Zhang, Zhiqiu Xia, and Nianmin Yao. Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. *Information Sciences*, 544:1–24, 2021. doi: 10.1016/j.ins.2020.07.051.
- [95] Jilei Sun. 2D-SCMCI hyperchaotic map for image encryption algorithm. *IEEE Access*, 9:59313–59327, 2021.

- [96] Christoph Bandt and Bernd Pompe. Permutation entropy: a natural complexity measure for time series. *Physical review letters*, 88(17):174102, 2002. doi: 10.1103/PhysRevLett.88.174102.
- [97] Joshua S Richman and J Randall Moorman. Physiological time-series analysis using approximate entropy and sample entropy. *American Journal of Physiology-Heart and Circulatory Physiology*, 278(6):H2039–H2049, 2000. doi: 10.1152/ajpheart.2000.278.6.H2039.
- [98] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.
- [99] Yicong Zhou, Weijia Cao, and CL Philip Chen. Image encryption using binary bitplane. *Signal processing*, 100:197–207, 2014. doi: 10.1016/j.sigpro.2014.01.020.
- [100] Nestor Tsafack, Jacques Kengne, Bassem Abd-El-Atty, Abdullah M Iliyasu, Kaoru Hirota, and Ahmed A Abd EL-Latif. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Information Sciences*, 515:191–217, 2020. doi: 10.1016/j.ins.2019.10.070.
- [101] Chunlai Li, Yan Zhang, Haodong Li, and Yang Zhou. Visual image encryption scheme based on inter-intra-block scrambling and weighted diffusion. *The Visual Computer*, 40(2):731–746, 2024. doi: 10.1007/s00371-023-02812-2.
- [102] Xinxin Kong, Fei Yu, Wei Yao, Shuo Cai, Jin Zhang, and Hairong Lin. Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order HNN: Image encryption and FPGA implementation. *Neural Networks*, 171:85–103, 2024. doi: 10.1016/j.neunet.2023.12.008.
- [103] Yue Wu, Joseph P Noonan, Sos Agaian, et al. NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2):31–38, 2011.

172

- [104] Behrouz A Forouzan. *Cryptography & network security*. McGraw-Hill, Inc., 2007.
- [105] Sundararaman Rajagopalan, Siva Poori, Mukund Narasimhan, Sivaraman Rethinam, Chandrasekar Vallipalayam Kuppusamy, Ramalingam Balasubramanian, Vijaya Moorthi Paramasivam Annamalai, and Amirtharajan Rengarajan. Chua's diode and strange attractor: a three-layer hardware–software co-design for medical image confidentiality. *IET Image Processing*, 14(7):1354–1365, 2020. doi: 10.1049/iet-ipr.2019.0562.
- [106] Yongjin Xian, Xingyuan Wang, Lin Teng, Xiaopeng Yan, Qi Li, and Xiaoyu Wang. Cryptographic system based on double parameters fractal sorting vector and new spatiotemporal chaotic system. *Information Sciences*, 596:304–320, 2022. ISSN 0020-0255. doi: 10.1016/j.ins.2022.03.025.
- [107] C Lakshmi, Karuppusamy Thenmozhi, John Bosco Balaguru Rayappan, and Rengarajan Amirtharajan. Hopfield attractor-trusted neural network: an attack-resistant image encryption. *Neural Computing and Applications*, 32(15):11477–11489, 2020. doi: 10.1007/s00521-019-04637-4.
- [108] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-allen and hamilton inc mclean va, 2001.
- [109] F Aluffi-Pentini, V Parisi, and F Zirilli. Global optimization and stochastic differential equations. *Journal of optimization theory and applications*, 47:1–16, 1985. doi: 10.1007/BF00941312.
- [110] Xiuli Chai, Jianqiang Bi, Zhihua Gan, Xianxing Liu, Yushu Zhang, and Yiran Chen. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Processing*, 176:107684, 2020. doi: 10.1016/j.sigpro.2020.107684.
- [111] Hegui Zhu, Yiran Zhao, and Yujia Song. 2D Logistic-Modulated-Sine-

- Coupling-Logistic Chaotic Map for Image Encryption. *IEEE Access*, 7:14081–14098, 2019. doi: 10.1109/ACCESS.2019.2893538.
- [112] James L. Kaplan and James A. Yorke. Chaotic behavior of multidimensional difference equations. In Heinz-Otto Peitgen and Hans-Otto Walther, editors, *Functional Differential Equations and Approximation of Fixed Points*, pages 204–227, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg. ISBN 978-3-540-35129-0. doi: 10.1007/BFb0064319.
- [113] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, 16(08):2129–2151, 2006. doi: 10.1142/S0218127406015970.
- [114] H. Toutenburg. Fisher, R. A., and F. Yates: Statistical Tables for Biological, Agricultural and Medical Research. 6th Ed. Oliver & Boyd, Edinburgh and London 1963. X, 146 P. Preis 42 s net. *Biometrische Zeitschrift*, 13(4):285–285, 1971. doi: 10.1002/bimj.19710130413.
- [115] M Naim and A Ali Pacha. A new chaotic satellite image encryption algorithm based on a 2D filter and Fisher–Yates shuffling. *The Journal of Supercomputing*, 79(15):17585–17618, 2023. doi: 10.1007/s11227-023-05346-5.
- [116] Akram Belazi, Sofiane Kharbech, Md Nazish Aslam, Muhammad Talha, Wei Xiang, Abdullah M. Iliyasu, and Ahmed A. Abd El-Latif. Improved Sine-Tangent chaotic map with application in medical images encryption. *Journal of Information Security and Applications*, 66:103131, 2022. ISSN 2214-2126. doi: 10.1016/j.jisa.2022.103131.
- [117] William Symes Andrews. *Magic squares and cubes*. Open Court Publishing Company, 1917.
- [118] Narbda Rani and Vinod Mishra. Behavior of powers of odd ordered special circulant magic squares. *International Journal of Mathematical Education in Science and Technology*, 53(4):1044–1062, 2022. doi: 10.1080/0020739X.2021.1890846.

174

- [119] Mahmood Ul Hassan, Asaad Alzayed, Amin A. Al-Awady, Nadeem Iqbal, Muhammad Akram, and Atif Ikram. A Novel RGB Image Obfuscation Technique Using Dynamically Generated All Order-4 Magic Squares. *IEEE Access*, 11:46382–46398, 2023. doi: 10.1109/ACCESS.2023.3275019.
- [120] Yongjin Xian, Xingyuan Wang, and Lin Teng. Double Parameters Fractal Sorting Matrix and Its Application in Image Encryption. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(6):4028–4037, 2022. doi: 10.1109/TCSVT.2021.3108767.
- [121] Yongjin Xian, Xingyuan Wang, Xiaoyu Wang, Qi Li, and Xiaopeng Yan. Spiral-Transform-Based Fractal Sorting Matrix for Chaotic Image Encryption. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(8):3320–3327, 2022. doi: 10.1109/TCSI.2022.3172116.
- [122] SHAOLIANG YUAN, TAO JIANG, and ZHUJUN JING. BIFURCATION AND CHAOS IN THE TINKERBELL MAP. *International Journal of Bifurcation and Chaos*, 21(11):3137–3156, 2011. doi: 10.1142/S0218127411030581.

List of Publications/ Communicated

List of Journal Publications

1. Puneet Kumar Pal, and Dhirendra Kumar, Zirili map-based image encryption method for healthcare, military and personal data security. *Physica Scripta*. 2024 Nov 12; 99(12): 125228. **IF-2.6 (SCIE)**
2. Puneet Kumar Pal, and Dhirendra Kumar, The coupled Kaplan–Yorke-Logistic map for the image encryption applications. *Computers and Electrical Engineering*. 2024 Dec 1; 120: 109850. **IF-4.9 (SCIE)**
3. Puneet Kumar Pal, and Dhirendra Kumar, Varun Agarwal, Efficient image encryption using the Tinkerbell map in conjunction with linear feedback shift registers. *Multimedia Tools and Applications*. 2024 May; 83(15): 44903-32. **IF-3.6 (SCIE)**
4. Puneet Kumar Pal, and Dhirendra Kumar, A Novel Two-dimensional SHIELD map for Audio Data Encryption with Two-step Confusion and Dynamic Diffusion Process. *Physica Scripta*. 2025. **IF-2.6 (SCIE)**
5. Puneet Kumar Pal, and Dhirendra Kumar, Image Encryption Algorithm using Zirili-Logistic Map and Magic Square Matrix-Based Fractal Sorting Matrix. (*Communicated*)

List of Conference Presented

1. Puneet Kumar Pal, and Dhirendra Kumar, A Novel Chaotic Map with High Chaotic Dynamics for Image Encryption Applications. 15th International Con-

176

ference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2024.

2. Puneet Kumar Pal, and Dhirendra Kumar, Image Encryption based on Chaotic Map and Fractal Sorting Matrix. 16th International Conference on Security of Information and Networks (SIN). IEEE, 2023.
3. Puneet Kumar Pal, and Dhirendra Kumar, A novel 3D non-linear sine map and its application in image encryption, International Conference on Graphs, Networks and Combinatorics (ICGNC), Department of Mathematics, Ramanujan College, University of Delhi