A Dissertation

On

Development & Analysis of Cryptographic Schemes for Visual Content

By

SAKSHI DHALL

Roll No. 2K13/Ph.D/CO/04

Under the Joint Supervision of

Prof. Kapil Sharma

Professor,
Department of Information Technology
Delhi Technological University
Delhi, India

Dr. Saibal K. Pal

Senior Research Scientist,
Defence Research & Development Organisation
(DRDO)
Delhi, India

Submitted in fulfillment of the requirements of the degree of
Doctor of Philosophy to the

Delhi Technological University

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road

Delhi-110042

2020

DECLARATION

I, Sakshi Dhall, Ph.D. student (Roll No. 2K13/Ph.D/CO/04), hereby declare that the thesis entitled **"Development & Analysis of Cryptographic Schemes for Visual Content"** which is being submitted for the award of the degree of Doctor of Philosophy in Computer Science & Engineering, is a record of bonafide research work carried out by me in the Department of Computer Science & Engineering, Delhi Technological University. I further declare that this work is based on original research and has not been submitted to any university or institution for any degree or diploma.

Date: _____

Place: New Delhi

Sakshi Dhall
2K13/Ph.D/CO/04
Department of Computer Science & Engineering
Delhi Technological University (DTU)
New Delhi -110042

DELHI TECHNOLOGICAL UNIVERSITY

(Govt. of National Capital Territory of Delhi)

BAWANA ROAD, DELHI – 110042

CERTIFICATE

Date: _____

This is to certify that the work embodied in the thesis entitled **"Development & Analysis of Cryptographic Schemes for Visual Content"** has been completed by **Sakshi Dhall** under our supervision towards fulfillment of the requirements for the degree of Doctor of Philosophy of Delhi Technological University, Delhi. This work is based on original research and has not been submitted in full or in part for any other diploma or degree of any university to the best of my knowledge and belief.

Dr. Kapil Sharma

Professor, Department of IT

Delhi Technological University

Delhi, India

Dr. Saibal K. Pal

Senior Research Scientist

DRDO

Delhi, India

ACKNOWLEDGEMENT

I wish to start by thanking God for choosing me to be worthy for this academic accomplishment and for all the blessings he has bestowed on me always.

I wish to now take the opportunity to express my sincere gratitude to Prof. Kapil Sharma, Professor, Department of Information Technology, Delhi Technological University, Delhi, and Dr. Saibal K. Pal, Senior Research Scientist, DRDO, Delhi for providing valuable guidance and constant encouragement throughout this research work. I wish to humbly thank them for believing in me and my ideas, and always extending their guidance & invaluable support in pursuing my research interests with full academic freedom. Through their vision I could shape and concretize these ideas into something meaningful. I also wish to extend my gratitude towards my supervisors for not only helping with in my academic accomplishments but also for supporting me in my professional as well as personal life and their ups and downs throughout this period.

Their knowledge, expertise and consistent motivation helped me throughout in my endeavor to pursue this research and make this thesis on **"Development & Analysis of Cryptographic Schemes for Visual Content".**

I also wish to very humbly thank the families of Prof. Kapil Sharma and Dr. Saibal K. Pal for being very warm, supportive and motivating whenever I visited their homes for research activities.

I would further like to extend sincere thanks to the faculty and staff of D/o Computer Science & Engineering and D/o Information Technology for their corporation and support in all the proceedings throughout. I wish to extend a special thanks to Dr. Ruchika Malhotra and Prof. Mukhtiar Singh for the encouragement they have always given to me. I also wish to thank Ms. Shruti from the Examination Department, Mr. Gopal and Ms. Sonia from D/o Information Technology, Mr. Ashok from D/o Computer Science and Engineering for always helping me in the procedural matters.

I am also very thankful to Prof. Yogesh Singh, Vice Chancellor, Delhi Technological University, Delhi, who has been a constant source of inspiration and has always motivated young researchers like me to pursue the path of excellence with an aim to achieve higher goals in academics and research. I wish to also thank Mr. D.C. Misra, DDG, NIC, Delhi for strengthening the belief in myself and always fostering me to pursue research.

I also wish to take this opportunity to thank all my teachers who have taught me and shaped me into the person I am, motivated me to be an academician, and have directly indirectly made me capable of succeeding in completing this research work.

I cannot thank enough to Mr. Nitin Jain, who besides sharing a similar research interest as mine, has always been an utmost supporting friend and has always rendered his unconditional help to me in all aspects including research and otherwise. I also want to thank my friend Ms. Shreya Sood who has been an ideal exemplar for me to follow since childhood, and has always been there for me in the need of the hour. My seniors and colleagues at Jamia Millia Islamia (JMI), Delhi, have also guided me throughout and encouraged me in pursuing this research, and I am very thankful to them. This thesis could not have been completed without the support system of my seniors and friends at NIC, Delhi and JMI, Delhi including Ms. Manie Khaneja, Mr. Adhesh Chand Gupta, Ms. P. Laxmi Rama, Mr. Ashwin Ayyappan, Mr. Ashutosh Tiwari, Ms. Ritika Gupta, Dr. Mueenul Hasnain, Dr. Sucheta Nayak, Dr. Anwara Hashmi, Dr. Adila Parveen, Dr. Samina Hussain and Mr. Ibadur Rahman. I feel blessed to have such beautiful souls in my life.

Last but not the least, I wish to thank my parents Mr. Vinod Kumar Dhall and Mrs. Vinodma Dhall for giving their unconditional love and relentless encouragement, always believing in me, keeping me motivated, helping me to overcome the stresses, ensuring that I live up to myself and live my dreams, and being there with me through every thick and thin not only throughout this research but in the journey of my life. I owe everything to you Papa and Mumma, and you both are my biggest blessings and my strengths.

Sakshi Dhall

ABSTRACT

The unprecedented advancement in technology, usage of internet and mobile services along with the upsurge of social networking as an indispensable part of day to day life, has brought forth an unimaginable necessitate for voluminous data transfer over inherently insecure networks. Also, there has been a significant shift in the type of transmitted digital content. The transmissions are no more limited to text-based data; they contain significant amounts of multimedia-based content of which visual content like images form a major part. Further, the emergence of Internet of Things (IoT) as a new reality is leading to significant increase in the multimedia traffic, including visual content, on penetrable networks. Traditional symmetric ciphers like AES, DES, IDEA etc. have been focusing on securing textual data, and are not found suitable for meeting the special resource efficiency requirements and catering the intrinsic properties of redundancy and bulkiness of visual content like images. It has been largely observed that while designing encryption schemes for securing visual content like images, the focus of researchers has been limited largely on one of the two key aspects pivotal to securing visual content i.e. cost efficiency and strength, thereby compromising on the other. Therefore, a need is identified for lightweight solution to secure visual content with complete removal of redundancy for real-time and resource constrained environments.

In the proposed research work, unconventional approaches have been employed to design lightweight encryption schemes many of which have customizable properties to suit the requirements of the specific applications to create balance between desired level of security and efficiency. New chaos-based cryptographic primitives are proposed and are used for customization of standard block ciphers like AES and lightweight block cipher like PRESENT to make them suitable for securing visual content. Also, a conditional encryption based block cipher is customized for its suitability to secure visual content like images. Further, the probabilistic approach has been extended for designing a symmetric image encryption scheme with customizable block size whereby the cipher image generated for the same key and for the same plain image differs each time the plain image is encrypted. Next, use of dynamic encryption has been proposed where by though the encryption scheme is deterministic yet chaos-based dynamism depending on the key and plaintext has been introduced at multiple levels so that cryptanalysis becomes much difficult for an adversary because in absence of

knowledge of key, the adversary will not know the exact structure of the encryption process being used for encrypting a particular plaintext. Security analysis has been performed for proving the strength of all the proposed schemes and their resistance against cryptanalytic attacks. Lastly, weaknesses in existing chaos-based image encryption schemes reducible to solvable mathematical model are studied. Cryptanalysis on one such scheme proposed by Zhou et al. (2014) was performed to unravel the weaknesses in the design of the said scheme and such similar schemes in general. Improvements are also proposed to improve the strength of the said scheme.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

Published in International Journals

[1] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic," *Signal Processing,* vol. 146, pp. 22-32, May 2018. **(SCI, Impact Factor: 4.086)**

[2] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "A chaos-based probabilistic block cipher for image encryption," *Journal of King Saud University-Computer and Information Sciences,* Article in Press. [Online]. Available: https://doi.org/10.1016/j.jksuci.2018.09.015. **(SCOPUS, ESCI)**

Book Chapter

[3] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "A Chaos-based Multi-level Dynamic Framework for Image Encryption," in *Internet of Things (IoT)*, M. Alam, K. Shakil, S. Khan, Eds., Springer, Cham, 2020, pp. 189–217.

Presented & Published in Proceedings of International Conferences

[4] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "A new chaotic-primitive and its application in customizing AES for lightweight multimedia encryption," in *Proc. 3rd International Conference on Computing for Sustainable Global Development 2016* (*10th INDIACom*), Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), Delhi, India, 2016, pp. 607-612. (**Available on IEEE Xplore)**

[5] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "Improvised Block Cipher Customized for Multimedia Security", in *Proc. 6th IEEE Power India International Conference 2014 (PIICON 2014)*, Delhi Technological University, Delhi, India, 2014, pp. 1-5, doi: 10.1109/POWERI.2014.7117735. **(Available on IEEE Xplore)**

[6] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "Cryptographic Primitives for Multimedia Security," in Proc. *1st International Conference on Innovative Advancements in Engineering and Technology (IAET 2014)*, Jaipur National University, Jaipur, Rajasthan,

India, Special issue 2 of *INROADS (An International Journal of jaipur National University)*, vol. 3, no. 1, pp. 335-339, Jan-June 2014.

[7] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "New Lightweight Conditional Encryption Schemes for Multimedia", in *Proc. the 3rd International Conference on Soft Computing for Problem Solving (SocPros 2013)*, Saharanpur Campus of Indian Institute of Technology (IIT) Roorkee, Roorkee, India, Advances in Intelligent Systems and Computing, Springer, vol. 258, pp. 365-377, 2014.

Presented in International Conference

[8] Sakshi Dhall, Saibal K. Pal, Kapil Sharma, "New Primitive for Multimedia Encryption using Chaos, Concepts of Rough Sets and Rule-based Decision Making", *ICM 2014*, Coex, Seoul, Korea, abstract published in the proceedings, 2014.

ABBREVIATIONS

AES	Advanced Encryption Standard
AI	Artificial Intelligence
APNG	Animated Portable Network Graphics
ASCII	American Standard Code of Information Interchange
ATS	Air Traffic Service
BMP	Bitmap
CBC	Cipher Block Chaining
CCTV	Closed Circuit Television
CFB	Cipher Feedback
CHNN	Clipped Hopfield Neural Network
CMYK	Cyan Magenta Yellow Key(Black)
CPU	Central Processing Unit
CTR	Counter
DDCC	Double Differential Cryptanalysis Comparison
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DIB	Device Independent Bitmap
DNA	Deoxyribonucleic Acid
DTH	Direct to Home
DVI	Digital Visual Interface
DWT	Discrete Wavelet Transform
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECB	Electronic Codebook

EPOC	Efficient Probabilistic Public-Key Encryption Scheme
F4V	Flash media container file format
GIF	Graphic Interface Format
GHz	Giga Hetrz
GPS	Global Position System
HCIE	Hierarchical Chaotic Image Encryption
HDMI	High-Definition Multimedia Interface
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission
IND-CCA	Indistinguishability under Chosen Ciphertext Attack
IoT	Internet of Things
IPR	Intellectual Property Rights
ISO	International Standardization Organization
ITU	International Telecommunication Union
JPEG	Joint Photographic Experts Group
LZW Compression	Lempel-Ziv-Welch Compression
MIDI	Musical Instrument Digital Interface
MNG	Multiple-Image Network Graphics
MPEG	Moving Picture Experts Group
MP3	MPEG-1 Audio Layer III or MPEG-2 Audio Layer III (Audio File Format)
MP4	MPEG-4 File Format Version 2
NIST	National Institute of Standards and Technology
NPCR	Number of Pixel Change Rate
OFB	Output Feedback

OHNN	Overstoraged Hopfield Neural Network
PNG	Portable Network Graphics
RAM	Random Access Memory
RGB	Red Green Blue
SDI	Serial Digital Interface
S-Box	Substitution Box
SP-Network	Substitution-Permutation Network
TIFF	Tagged Image File Format
TV	Television
UACI	Unified Average Change Intensity
USC-SIPI	University of South California – Signal and Image Processing Institute
VR	Virtual Reality
WAV	Waveform Audio File Format
WMV	Windows Media Video
XOR	Exclusive OR
YCbCr	Y: Luma Component Cb: Blue-difference Cr: Red-difference
YIQ	Y: Luma Component I: In-phase Q: Quadrature,
YUV	Y: Luma Component UV: Two Chrominance Components
1D	One Dimensional
2D	Two Dimensional
3D	Three Dimensional
5G	Fifth Generation (Cellular Network Technology)

CHAPTER 1
INTRODUCTION

Digitization has emerged as one of the most significant contributors in the area of modern day communications. The ever-evolving digital world is currently witnessing an unexampled growth in the area mobile technology and internet, making digital data transfers a core component of every individual's daily life. Improvement in price-performance ratio of microelectronics technology has given a strong impetus to what we call as digital revolution. Digital information has found its inevitable presence in almost every sphere of life from military to medical science, banking to e-commerce, education to entertainment, tourism to social media to space exploration etc., the list is endless. There is practically no sphere of work or industry which is not utilizing the ease of communication offered because of these advancements.

1.1 Types of Digital Content

As stated earlier, with the offshoot in mobile technology and internet becoming more and more permeant part of our daily routines, the magnitude of available digital data and the need for voluminous information transfers have increased enormously. It is no more limited to the known sensitive sectors of banking, military, space exploration etc. Rather, it has found its significance in sectors like health-care, e-commerce, social networking, live-transmissions, pay-tv, surveillance, usage of smart gadgets/appliances etc. With the kind of these new applications dominating today's data transfers, it is clear that the nature of data transfers has also become diverse leading to emergence of multimedia [1]–[4] forming a significant and in fact predominant part of modern world's communications. Thus, the continuous advancement in technology and increased usage of internet and mobile services has not only increased the necessity of securing sensitive digital data but has also widened the spectrum of types of data, having their own inherent characteristics, requiring security against any kind of breach. Following are the different types of digital data:

1.1.1 Numeric Data

Numeric data refers to the data being stored as numbers to represent measurements, counts, quantifiable characteristic of physical phenomena or physical/logical entities etc. like pollution levels, temperatures/humidity levels in weather forecast, stock exchange statistics, geographical locations (GPS) etc. Much of this data is also streaming data like e-commerce/marketing data to account online clicks for analyzing customers' behaviour, real-time stock market predictions based on computation of value-at-risk etc. Numeric data could include integer data or floating point values and as they are stored in numeric fashion therefore the standard conversion methods from decimal number system to binary number system or floating point representations are used to transmit numeric data and store them in computers.

1.1.2 Textual Data

The textual data comprise of alphanumeric, printable and nonprintable characters (like spaces etc.). The input for such data is normally made through keyboard but other sources include Bar Code Reader, Magnetic Strip Reader, Optical Character Recognition (OCR), voice input converted to text etc. There are three popular coding standards for textual data:

a) ASCII (American Standard Code of Information Interchange) which is an ISO standard, and is an 8-bit code providing encoding for 256 characters.

b) EBCDIC (Extended Binary Coded Decimal Interchange Code) which was developed by IBM and is mainly supported by the IBM mainframe computers. It is also an 8-bit code providing encoding for 256 characters.

c) Unicode is a 16-bit international standard developed to overcome the ASCII & EBCDIC limitations, so as to support multiple language alphabets.

Textual data requires less storage space as compared to other forms of media like images, video etc.

1.1.3 Images

Generically, images are visual perceptions which are sensed by eyes as a collection of color intensities spread over a frame of vision forming a picture, photograph etc. Digital images [3]–[6] are formed of a collection of pixels each representing the color intensity at a particular point in the image, or alternatively, digital images can also store vector information in the form of

mathematical formulation for graphics/geometric figures being represented in the image. The former images are called bitmap images while the latter are called vector-based images. As stated earlier, bitmap images comprise of representation of individual points in the image as pixels. Each pixel denotes the color intensity value in the form of a numeric code as per the encoding scheme used. Colored images normally have 3 color planes i.e. RGB (Red, Green Blue). The resolution of a bitmap image is determined by the number of pixels per inch and the color intensity levels supported by the used encoding scheme. The higher the resolution is, the higher the storage requirement will be. Vector-based images require lesser storage space as compared to bitmap images but they have a very limited scope and they cannot be used for representing general photographs or for capturing real world objects/scenes. In fact, for displaying vector-based images, these images must be converted into bitmap before they are displayed.

For performing image processing, images are sometimes also converted in frequency domains [7] using transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) where the information is represented in terms of respective frequency components instead of pixel values (as represented in spatial domain).

The common file formats [3]–[5] used for images include GIF, TIFF, BMP, PNG, JPEG etc. In the year 2000, the Joint Photographic Expert Group, which is a joint working group of International Standardization Organization (ISO) and the International Electrotechnical Commission (IEC) in collaboration with the International Telecommunication Union (ITU), developed JPEG2000 image compression standard and coding system (ISO/IEC 15444) with an intention to supersede their earlier JPEG standard (ISO/IEC 10918) which was created in 1992.

1.1.4 Audio

Audio data [3], [4] corresponds to storing sounds like voices, human speech, music, background sound effects etc. Sound of any form is basically an analog signal and to be stored on a computer it is required to be digitized in some way. This digitization could be done by sampling and quantizing the analogue signals of the sound and the corresponding digital audio data is called the digitized sound. Audio data can also be represented in binary by storing the digital description of sounds in the form of series of control messages depicting information

like pitch, duration etc. of the sound. Such audio files are called MIDI (Musical Instrument Digital Interface) files. The data in the form of control messages is appropriately converted to produce the desired sound using a MIDI compatible device.

The common file formats used for audio data include MIDI, WAV, MP3 etc. In 2007, the Moving Picture Experts Group (MPEG) which is a working group of ISO/IEC developed a standard MPEG-D (ISO/IEC 23003) for MPEG Surround Audio Coding, Spatial Audio Object Coding and Unified Speech & Audio Coding.

1.1.5 Video

Like an audio signal, a video signal is also an analog signal and hence it is also required to be sampled and quantized in order to be converted to digital form for storage purposes [4]. After digitization, the output video can be represented as a series of moving frames where each frame comprises of pixels representing color intensities. Like images, video signals also comprise of several channels like RGB or YUV or YIQ. Normally, the playback rate is 30 frames per second for human eye to perceive the video. Unlike still bitmap image, the pixel intensities in moving frames of the video keep updating in color and intensities. Since a single frame of video can be sufficiently large, hence, storing a series of such frames require significantly huge amount of storage and therefore normally videos are stored by making use of some video compression techniques. Videos are also stored in transform domain like Fourier or Discrete Cosine Transform (DCT) etc. which help in discarding the data which is not used by the human eye thereby reducing the size of video data. Also, compression techniques are used to compress individual frame's data which is called intra-frame compression. Inter-frame delta compression may also be done by storing the difference between subsequent frames instead of storing entire frame data because usually video sequence involves very little change from one frame to the next.

The commonly used codec/file formats for videos include WMV, Quicktime, Indeo, MPEG-2, MPEG-4 etc. The MPEG standards are internationally accepted ISO standards for video data. Interconnect standards for digital video also include HDMI, DVI (Digital Visual Interface), SDI (Serial Digital Interface), DisplayPort etc.

1.1.6 Multimedia & Virtual Reality

Multimedia refers to combining more than one media of the above mentioned media like text, images, audio etc. together in the data being stored or communicated across the network. Voluminous amounts of digital multimedia content is being generated every day across the globe in the form of content on social media besides its relevance in other sectors like tourism, space exploration, defence, medical science etc. With the concepts like Virtual Reality (VR) [3] the extent and scope of multimedia has surpassed imaginable boundaries. VR refers to technology-aided artificial environment and experiences which are not necessarily reality but appear as reality to human auditory and visual senses by making use of 3D imaging, 360 degree video and photo capture, Photogrammetry, Volumetric 3D capture, Light field capture etc. Though, today VR is visualized to find its place largely in the entertainment and gaming industry but its scope is way beyond. In future, it will be one of the paramount and cost-effective tools for medical trainings, military trainings, engineering designing, architectural designing etc.

The VR content can be accommodated in the traditional video formats like MP4, MOV, F4V, WebM etc. and the codec being currently used is also MPEG4 or H.264. The formal standardization for interoperability purposes about certain aspects of VR are still under consideration by MPEG.

1.2 CODECS FOR DIGITAL IMAGES

Codec refers to a coder-decoder used for encoding and decoding digital data stream. Different codecs include different specifications, algorithms, sampling techniques as per their fields of applications and are generally supported by different operating systems as well. Following are few of the different codecs and/or file formats [3]–[5] used for digital images:

a) ***BMP (Bitmap):*** Bitmap codec provides a raster graphics image file format which represents an image as a rectangular grid of pixels, where each pixel represents a color intensity in a certain number of bits. The number of bits used to represent color intensity of a pixel is called color depth. Bitmap supports both monochrome and colored images with variable color depths and optional alpha channels to support transparency in appearance of the image. The BMP image quality is good but it does not support very

effective compression. As per Microsoft documentation, a particular bitmap representation is defined in a way to aid exchange between different display devices (like graphics cards). This is called device independent bitmap (DIB).

b) ***GIF (Graphic Interface Format):*** This format supports colored images with three constituting color channels, i.e. RGB, where each color constituent per pixel is represented by 8-bit intensity value. Thus, each pixel is represented by 24-bit value. Since each color channel is being represented in 8-bits therefore the color palette for each color channel comprise of only 256 intensities. This restricts GIF images in reproducing true colors of photographs and also GIF cannot appropriately represent color gradients smoothly. GIF is suitable for graphics, logos and other simpler images preferably not involving intricate color gradients. Lempel-Ziv-Welch (LZW) lossless compression technique is used to compress GIF images without any loss of information during decompressing the image back. GIF is one of the most popular formats for exchanging colored images on the web and is being supported nearly by all graphical browsers. GIF also supports animation as a collection of multiple frames in the single file and each frame has its own palette. The different frames are played with time delays giving impact of a video clip.

c) ***PNG (Portable Network Graphics):*** PNG format was developed largely with a view to provide non-patented alternative to GIF in order to overcome the patent issue of LZW compression technique faced while using GIF format and also to overcome the restricted 256 color palette issue associated with GIF images. PNG supports much wider color depths. Also, unlike GIF, PNG is a single-image format and hence does not offer support for animations but its extended formats (though not too popular) like MNG (Multiple-Image Network Graphics) and APNG (Animated Portable Network Graphics) support animations.

d) ***JPEG (Joint Photographic Experts Group):*** JPEG supports lossy compression for digital images with adjustable compression ratio to facilitate striking a balance between storage constraints and image quality. It can achieve significant compression without visually perceptible loss in image quality and hence produce smaller files than PNG with similar image quality. JPEG is one of the most common formats used for storing

photographic images captured by digital cameras and transmitting them over the internet. The file extensions used are .jpg or .jpeg.

JPEG uses Discrete Cosine Transform (DCT) based lossy compression which discards high frequency information relating to sharp intensity transitions that contribute less to the overall image information. JPEG compression algorithm is found most suitable for photographs and paintings having smooth and low color contrast variations. Since significant compression is achieved without much perceptual loss of information hence this format is frequently used for internet transmissions but it is not found suitable for graphics, line drawings etc. where sharp contrast form integral part of the overall image perceptual value and for such images formats like TIFF, PNG, GIF are found better suitable. Also, JPEG format is not very suitable for medical imaging because exact reproduction of original image is not possible here due to lossy compression being used. Further, image editing without loss of image quality is also not possible due to the same reason. Though, lossless editing of JPEG is available now using specific utilities, yet JPEG is not very suitable for images requiring multiple edits in presence of availability of other lossless image formats.

e) ***TIFF (Tagged Image File Format):*** It is a versatile bitmap format. The original TIFF specification was developed to support black and white images generated by desktop scanners with an intent to provide a common image format for such images. TIFF later on extended support for grayscale and then colored images. TIFF offers a flexible, adaptable file format and supports numerous data compression schemes to allow customization of TIFF format as per storage needs. Latest versions of TIFF also support CMYK and YCbCr color spaces, besides the RGB, and also offer support for varied color depths. TIFF is supported by multiple operating systems like Windows, Unix, Macintosh etc. A TIFF file can also act as a container for holding lossy JPEG compressed images or lossless compressed images. TIFF also supports use of lossless LZW compression as well, and hence, TIFF images can be easily edited without loosing image quality. TIFF is frequently used format in scanning, faxing, desktop publishing, optical character recognition, image manipulation etc. related applications and is used as a generic format for interchange between professional image editing applications. TIFF focuses more on support for image manipulating applications rather than other applications as web browsers.

1.3 NEED FOR SECURITY

The digital technology has no doubt proved to be a marvel in its contribution to the kind of communications possible in today's world but it has also paved way for serious possible breaches when sensitive information is stored or shared through susceptible channels.

An effective communication is incomplete without the communicating parties feeling assured that the communication is safe and secure. It is needless to say that a safe and secure communication encompasses a safe channel and secure end points. The role of security in communication has also widened over past few decades. In today's digital world, information is required to be secured against unauthorized access, interception, tampering, disruption etc. Confidentiality, Data Integrity, Availability, Authenticity and Non-repudiation are the major key aspects forming the basis of Information Security [8], [9]. Following gives a brief description of each of these key aspects:

a) **Confidentiality:** Confidentiality also referred as privacy means that no unauthorized entity should be able to access sensitive information over the network while transmission or at the storage points thereby ensuring that the digital content is protected from being disclosed to an adversary.

b) **Data Integrity:** Data Integrity means that the message/data being communicated by the sender should remain intact when received by the receiver i.e. content of the message/data should not have been subjected to any kind of tampering, modification/alteration, addition, deletion and it should not be a replay of an earlier communication.

c) **Availability:** Availability refers to ensuring that the information should be available to authorized parties at relevant time without any kind of interruption.

d) **Authenticity:** Authenticity refers to ensuring all the communicating entities that the peer entity is authentic i.e. who it claims to be. It should be ensured that no adversary is masquerading and pretending to be someone else while taking part in the communication or accessing sensitive information.

e) **Non-repudiation:** Non-repudiation ensures that none of the communicating parties can repudiate the contents of the communication nor can they repudiate having participated in the communication.

Besides the above key aspects, protection of Intellectual Property Rights (IPR) has emerged as a very significant domain attracting attention in recent times. Security mechanisms like encryption, hashing, digital signature etc. are designed to ensure desired security with regard to the mentioned different key aspects of Information Security.

1.4 Securing Digital Content using Encryption

The cryptographic technique – Encryption, forms one of the major countermeasures for achieving a major key aspect of Information Security i.e. confidentiality or privacy. Specific kind of encryption technique called Asymmetric-key Encryption is also used in security mechanisms designed to ensure authenticity and non-repudiation as well.

Encryption refers to the process of converting plaintext to non-perceivable forms (cipher text) thereby facilitating secure transmission of sensitive information from the source to destination. The desired secrecy for converting the plaintext to unintelligible collection of bits is provided by the 'secret key' which forms an integral part of the whole encryption process. Based on the key used for encryption and decryption process the schemes are categorized in the following two categories:

a) **Symmetric:** Symmetric/Private Key Encryption is a form of cryptosystem where the key used for both encryption and decryption is same. The key used is called the Private Key (Secret) [9].
b) **Asymmetric:** Asymmetric/Public Key Encryption is a form of cryptosystem where the key used for encryption is different from the one used for decryption. One is the private key (secret) while the other is the public key [9].

Both these cryptosystems have different applications where the former is used for securing most of the normal data exchanges while the latter being more computationally expensive is used in digital signing, during very sensitive data transfers like key exchanges etc. Further encryption schemes are also classified as:

a) **Stream Cipher:** A stream cipher encrypts the digital data one bit/byte at a time. E.g. Vignere Cipher, Vernam Cipher.

b) **Block Cipher:** A block cipher encrypts a fixed sized block of plaintext as a whole and produces an equal sized cipher text block. e.g. DES, AES etc.

In case of stream ciphers with desired strength for practical applicability the operations performed during encryption are computationally expensive because high strength is to be achieved without making use of multiple rounds of operations whereas in case of block ciphers multiple rounds involving computationally lighter primitives per round are used. Following describes the structure and operations of few standard block ciphers like DES [8], AES [10] and an ultra-lightweight block cipher PRESENT [11].

1.4.1 DES (Data Encryption Standard)

DES [8] is a block cipher with block size of 64 bits and key size of 56 bits. It is based on Feistel cipher structure with 16 rounds of operations. Each of the 16 round keys K_1, K_2, ... K_{16} is 48 bits long and is derived from the original 56-bit key. The overall structure of DES consists of an Initial Permutation, followed by 16 rounds of encryption operations based on Feistel structure, followed by swapping of two halves of the intermediate cipher text and finally a final permutation which is actually inverse of the initial permutation.

The initial permutation and its inverse are defined by tables. The input to the permutation table is a 64-bit block with its bits numbered from 1 to 64. There are 64 entries in the permutation table which contain a fixed permutation of the numbers 1 to 64 indicating the corresponding positions of the input bits in the output 64-bit block.

Each round of DES follows the Feistel structure i.e. the 64-bit input to the round is treated in two 32-bit halves and one of the two halves is substituted while the other is not, and this is followed by swapping of the two halves. To elaborate, the right 32 bit half along with the 48-bit round key are the inputs to the round function which involves both substitution and permutation operations. The 32-bit output of the round function is then XORed with the left 32-bit half and this becomes the substitution value for the left half while the right half remains unchanged. This is followed by swapping of the left and the right halves thereby completing one round of operations.

The decryption algorithm is exactly same as the encryption algorithm except that the round keys are used in the reverse order while performing decryption. The following figure Fig. 1 shows the block diagram for the DES block cipher:

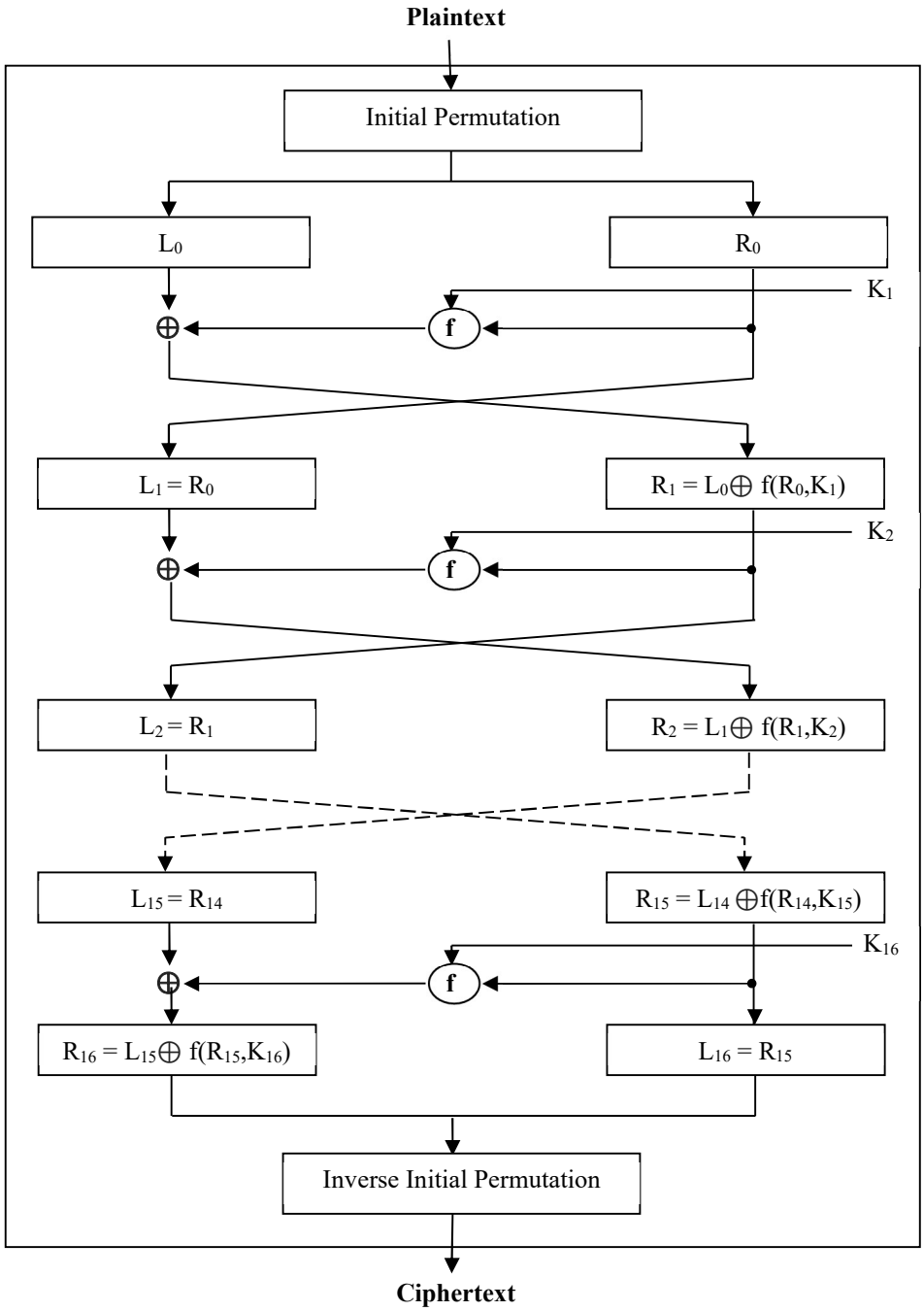


Fig. 1 Block Diagram for DES block cipher

1.4.2 AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) [10] is a block cipher based on symmetric key encryption. It encrypts a plaintext of 128 bits into an equal-sized cipher text taking 128, 192 or 256 bits sized secret key performing 10, 12 or 14 rounds of operation respectively. The 128-bit input block is treated as a 4x4 state matrix of bytes on which several rounds of operations are performed using the 128 bits round keys derived from the original secret key to generate equal sized cipher text block. One round of operation comprises of the following four basic operations:

a) ***Substitute Byte:*** This is a simple look-up based substitution operation, where a 16x16 matrix called S-Box is used for substituting bytes of the state matrix. The first 4 bits of the input data byte act as the row index and its last four bits act as the column index for locating the substituting byte in the S-Box.

b) ***Shift Rows:*** In this operation the bytes of the i^{th} row of the state matrix is circularly left shifted i no. of times.

c) ***Mix Column:*** This operation is used to achieve diffusion by multiplying the state matrix with a fixed matrix. Hence each byte of the output matrix is contributed by all the four bytes present in its column in the input state matrix.

d) ***Add Round key:*** This involves simple bitwise XOR (exclusive-OR) operation between the bytes of the state matrix and the corresponding round key bytes.

Encryption using AES starts with Add Round key operations followed by N_r-1 rounds (where N_r is 10, 12 or 14 for 128, 192, or 256-bit key respectively), each round comprising of Substitute Bytes, Shift Rows, Mix Columns and Add Round Key operations while the last round comprise of Substitute Bytes, Shift Rows and Add Round Key operations. The structure of the decryption procedure is same as that of the encryption in the sense that it also involves Add Round Key operation as the initial step followed by N_r-1 rounds, each round comprising of Inverse Shift Rows, Inverse Substitute Bytes, Add Round Key and Inverse Mix Columns operations. The last round consists of Inverse Shift Rows, Inverse Substitute Bytes, Add Round Key operations. The following figure Fig.2 shows the block diagram for the AES block cipher:

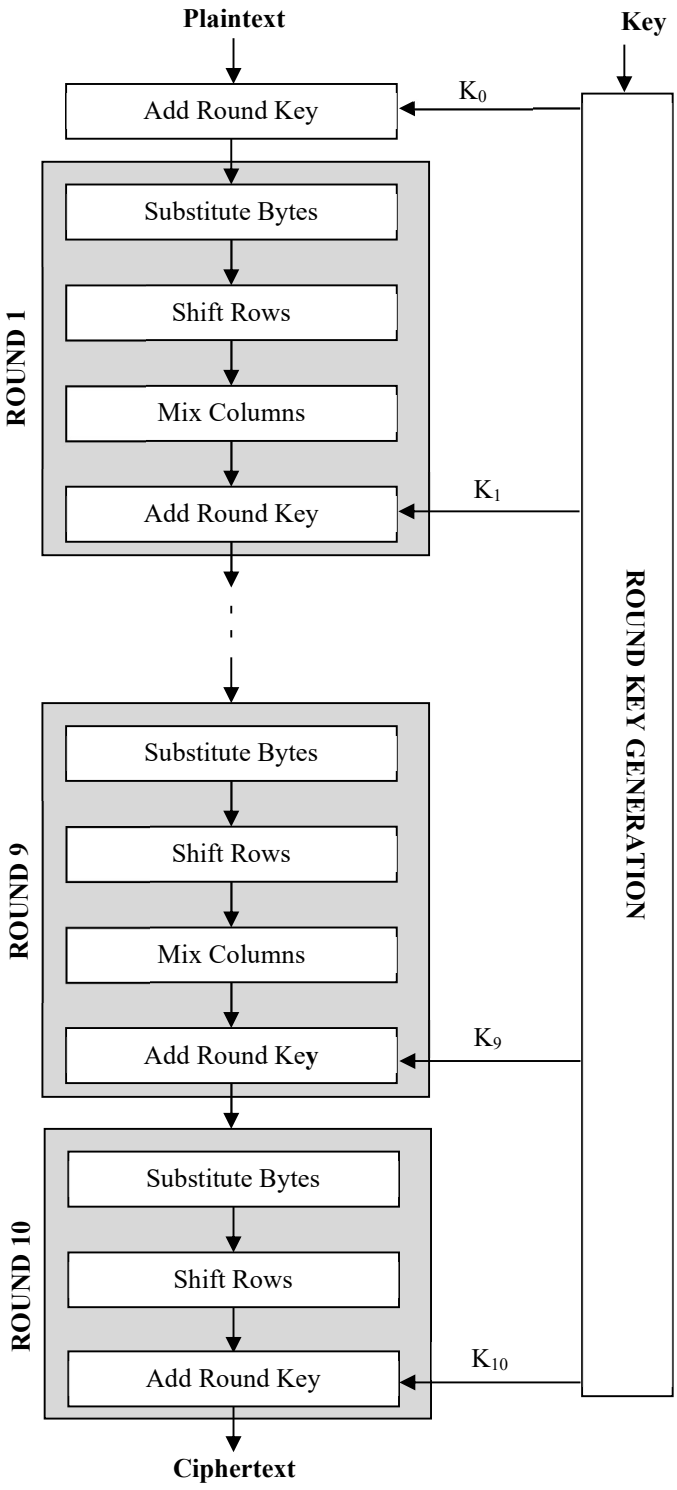


Fig. 2 Block Diagram for AES block cipher with 128-bit key

1.4.3 PRESENT

The PRESENT [11] block cipher uses key size of 80 or 128 bits and encrypts a block of 64 bits. It is an ultra-lightweight block cipher with highly efficient hardware implementation as its prime focus. The 80-bit key variant is proposed to be the one more suitable for applications

in resource-constrained environments having low-security requirements. This block cipher is basically built on the theme of Substitution-Permutation network (SP-network) employing 31 rounds of the basic operations with an extra AddRoundKey operation after completion of all rounds. The original key is used to generate 32 more 64-bit round keys K_1, K_2, ... K_{32} by updating the original key after each round. The per-round operations involved in the block cipher include:

a) ***AddRoundKey:*** This operation is a bitwise XOR (Exclusive OR) of the 64-bit round key with the current input state.

b) ***SBoxLayer:*** The PRESENT block cipher uses a 4-bit to 4-bit SBox for substituting each nibble of current state as per the fixed substitution table as shown below:

x	0	1	2	3	4	5	6	7
S(x)	C	5	6	B	9	0	A	D

x	8	9	A	B	C	D	E	F
S(x)	3	E	F	8	4	7	1	2

c) ***P Layer:*** This operation involves bitwise permutation of the current state bits placed on positions say *i* to the new positions P(*i*) as per the fixed permutation table as shown below:

i	0	1	2	3	4	5	6	7
P(*i*)	0	16	32	48	1	17	33	49

i	8	9	10	11	12	13	14	15
P(*i*)	2	18	34	50	3	19	35	51

i	16	17	18	19	20	21	22	23
P(i)	4	20	36	52	5	21	37	53

i	24	25	26	27	28	29	30	31
P(i)	6	22	38	54	7	23	39	55

i	32	33	34	35	36	37	38	39
P(i)	8	24	40	56	9	25	41	57

i	40	41	42	43	44	45	46	47
P(i)	10	26	42	58	11	27	43	59

i	48	49	50	51	52	53	54	55
P(i)	12	28	44	60	13	29	45	61

i	56	57	58	59	60	61	62	63
P(i)	14	30	46	62	15	31	47	63

The following figure Fig. 3 shows the block diagram for PRESENT scheme:

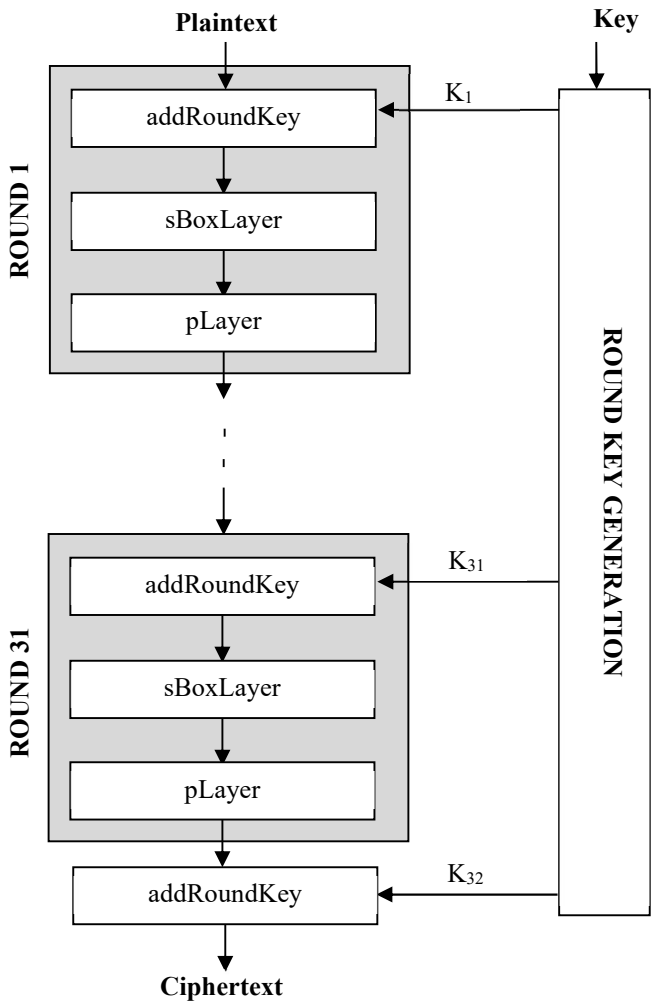


Fig. 3 Block Diagram for PRESENT block cipher

1.5 REQUIRING SECURITY OF VISUAL CONTENT

Following gives a brief on few of the areas and applications requiring security of visual content:

1.5.1 Biometrics for Aadhar & other applications

Biometrics are being widely used for several purposes including authentication. In Indian context, a recent upsurge in requirement of biometric information is for Aadhar. Aadhar is a unique 12-digit number which can be assigned to all Indian residents and in the process of creation of Aadhar essential details along with the biometric data like retina scan, fingerprints are captured for the Indian resident applying for it. Clearly, such sensitive biometric information is vulnerable to be misused, for doing crimes, by an adversary if it gets accessed in an unauthorized way. Therefore, storing and transmitting such bulky and highly sensitive

biometric information is required to be done in secured manner by way of suitable encryption techniques offering high levels of security.

Also, in today's world, fingerprint, retina scans etc. have been used for authentication purposes and recent research have identified scope of human gait as a new biometric which can be used for identification and in future for authentication. Human gait-based systems will require 3D representation of human movement while walking and using it for identification and authentication. Clearly, these biometric-based (including gait-based) identification and authentication systems makes it extremely important to secure such biometric information both at storage and transmission levels to avoid breach of system security relying on such authentication mechanisms.

1.5.2 Digital Pay TV, DTH & Video on Demand

Applications like Digital Pay TV, DTH (Direct to Home) and Video on demand require security of visual content for working of their business and revenue generating model. The visual content is required to be accessed only by the authorized users and that also for limited number of times or for limited time period especially in case of video on demand with electronic rental period. As these applications require real-time transfers which could also be on hand-held devices like mobile phones with constrained resources, hence, the encryption schemes are required to be lightweight while still providing desired levels of security.

1.5.3 Medical Imaging

Medical imaging is another upcoming area requiring security of radiology and other sensitive health-related details of the patients. The advancement in the modern-day medical science and related technology, use of expert systems for diagnosis and use of robots for performing distant surgeries is not unknown. In such situations, it becomes inevitable to protect the sensitive medical imaging information from being misused for malicious intents and for this use of encryption schemes plays a significant role.

1.5.4 Satellite Communication for Space Exploration & Defence Activities

Satellite-based visual content transmission from space to ground stations are done for space exploration and defence activities like target detection, tracking, wide-area surveillance, vehicle navigation etc. Such applications require sensitive data like satellite images/videos

from space, defence maps etc. to be encrypted on-board in satellite and hence such encryption schemes should be efficient because there are limited resources when it comes to functioning in space satellites. Such encryption schemes should also have high radiation-induced fault tolerance because satellites operate in extreme radiation environment.

1.5.5 Aerospace Industry

Though, communication happening between the ground station and aircraft (ATS) is normally audio yet in emergency situations it could involve video transmission as well and this communication is required to be secured. The challenge becomes all the more intense when it comes to fighter aircraft communicating with the ground station at the war time. Clearly, an efficient and attack-free communication channel is required in such situations so that an adversary cannot impact such sensitive real-time communications.

1.5.6 Video Conferencing & Live Transmissions

Video conferencing on significant national and international policy making esp. for defence, with embassies, for policing etc. are common and such transmissions are required to be protected with utmost security because of the nature of sensitive content they hold and the kind of impact they will have if a possible breach happens. Again, these transmissions are real-time and hence require efficient encryption schemes with high strength for suitability.

1.5.7 Social Networking

Exchange of personal information including videos, photographs etc. over social networking sites is the most common thing that almost every individual is doing today. Such mammoth amount of private information is required to be secured on vulnerable networks and storage end points so as to ensure privacy on social-media platforms as such platforms have become the most common means of modern day personal and social communications, specially, in the light of recent revelations that ecommerce industry is targeting personal information of individuals available on social media for business gains.

1.5.8 Smart Homes & Smart Gadgets/appliances

Modern day trends include use of smart gadgets/appliances capable of sensing the environment by collecting real-time data and using artificial intelligence to operate. The concept of Internet of Things (IoT) is becoming a new reality and its applications are penetrating in our homes.

The idea of smart homes is also not unknown. Though, it all appears very fascinating and useful on one hand, yet on the other hand it makes the living in such homes with smart devices more vulnerable to crimes, specially, in case the data collected by the smart devices are accessed in an unauthorized way by an adversary who observes the daily routine activities of people living in the household and then may plan a crime. Therefore, securing such information which may include all kind of data including visual content is inevitable. An example of how smart devices are being practically used today – on 7th September 2018 a real delivery was done by Amazon in Suburban London where the customer was not present at the home when the delivery man arrived for delivery of a parcel. The delivery man talked to the customer through a video door-bell which gave alert to the customer sitting in his office. Using his iphone mobile app, the customer from his office opened the car standing outside the house and the delivery man kept the parcel in the car and the customer again locked the car. The kind of digital communication that happened while this successful delivery of parcel was made, can easily show if any portion of this communication (like the video communication using the video bell, or the signal to open the car from the customer) is unauthorizedly accessed by an adversary then there can be an easy misuse of it for achieving malicious intent, and hence efficiently securing such large-scale daily routine smart communications is a new challenge open today.

CHAPTER 2

BACKGROUND LITERATURE

With the wide range of applications extending to diverse domains both in personal and professional fronts, the need for securing visual content has increased manifolds. Images are a major source of visual content - be it forensics, defence maps, biometrics, personal image sharing on social networking etc. Further, the frequent advancement in the area of Internet of Things (IoT) and device to device communication has widened up the horizon of challenges for securing all forms of data including visual content like images [12]–[15]. The ideas and approaches designed for image security in principle can be extended for videos as they may be treated as moving image frames.

2.1 Visual Content Encryption using Conventional Methods

Confusion and difussion are two characteristics required to be possessed by any secure cryptosystem [16]. Confusion deals with making the relationship between the cipher text and the key bits very intricate and involved, thereby, making the cipher text output completely dependent on the secure key. Diffusion is associated to the dependency of the cipher text bits on the input, i.e. each plaintext bit should contribute to multiple cipher text bits thereby dissipating the redundancy of the plaintext across the whole cipher text. There are two basic types of operations that are performed in every encryption process namely – permutation and substitution. Permutation operation refers to transposition of plaintext bits/symbols to scramble the plaintext and substitution operation involves replacing bits/symbols by other bits/symbols to make the ciphertext unintelligible for the adversary. Several block ciphers and stream ciphers have been designed involving use of permutation and/or substitution operations more particularly to secure textual content with proven strength.

As a naïve approach, the visual content data may be treated as a bit/byte stream and traditional ciphers may be applied to encrypt them. But this is not a suggested and practically secure approach because unlike text-based data, visual content has some special characteristics of its own:

- it is much bulkier,
- there exist strong-correlation among the neighbouring data values and,

- it has dynamic requirements especially for streaming data based on channel bandwidth and the resource constraints posed by the end points which may be small miniature hand held devices like mobile phones etc.

The objective while securing visual media is two-folds i.e. complete removal of redundancy and it should be achieved at low computational cost. Together both these requirements can neither be catered by standard traditional block ciphers with proven strength like AES [10] nor can ultra-lightweight ciphers like PRESENT [11] suffice for such applications. In the native ECB (Electronic Codebook) block cipher mode the redundancy in the plaintext, which usually persists beyond the block size, gets percolated in the ciphertext. Other block cipher modes [8] like CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), CTR (Counter) etc. involve extra computation and require extra information beyond the secret key including Initialization Vector, Counter, Nonce etc. to be communicated to the receiver for decryption to be possible. This makes the encryption process even more computationally expensive when the traditional block ciphers are operated in one of these modes. Further, compression followed by encryption is also not a very good solution due to unnecessary resource consumption involved in compression activity especially when the sender is working in resource constrained environment.

Researchers have, thus, recognized and appreciated the importance for devising separate encryption schemes to handle the special needs and challenges for visual content.

Following are some of the significant approaches followed currently for encrypting visual information.

2.1.1 SCAN-based Encryption

Researchers have proposed several image compression and encryption schemes, mostly stream ciphers, based on SCAN methodology which basically refers to defining a formal language with basic scan patterns, transformations and production rules for generating complex scan paths. Each scan path is such that each individual pixel of the 2D image is accessed exactly once through the scan path. Thus, a scan path provides a sequential order to access the pixels of a 2D image. Clearly, for an image as small as 4×4 in size there will be 16! different scan paths which is a fairly large 14 digit number. So, for an M×N image there are (M*N)! scan paths and the strength of the SCAN language in generating large number of such scan paths

offers security to SCAN based schemes. These schemes make use of formal language to generate one among the many scan paths, which can then act as the key during encryption process for permuting the image pixels [17]–[21]. SCAN language based transposition ciphers in [17]–[18] are claimed to be suitable to be used with other substitution ciphers to generate efficient product ciphers suitable for pictorial data. Also, [22] proposed SCAN based permutation followed by use of XOR operation to change pixel values to enhance security. Further, [23] extended the use of SCAN methodology for compressing, encrypting videos and hiding data in videos. During encryption process the difference between adjacent frames of the video are encrypted for which scan patterns are generated to permute the pixels which act as the encryption keys and substitution rule is also included to add to the confusion and diffusion properties of the scheme. Instead of only using SCAN based permutation, intertwining of permutation and substitution operations has been done to add to the security in this work. The papers [24] and [25] proposed stream ciphers for image security involving permutations based on SCAN language and substitutions based on cellular-automa based which is described in the section 2.1.3.

2.1.2 Chaos-based Encryption

The major advantages of chaos-based encryption are that output of a chaotic map [26] appears as noise to the unauthorized users and it strongly depends on the initial conditions and the control parameters of the generating functions i.e. their slight variations result in significantly different output. Therefore, the initial states and control parameters determine the key in such encryption systems and provide desired strength to the encryption scheme. As stated earlier, a good cryptosystem must possess confusion and diffusion properties and both these properties are sufficed by chaos [26], [27] with its intrinsic characteristics of ergodicity, mixing property, high sensitivity to initial conditions and control parameters. Also, the deterministic nature of chaos, besides being random-like, makes it possible to retrieve the original text back as part of the decryption process.

A general chaos-based cryptosystem follows the structure mathematically represented as:

$$Cipher = D^m(C^n(PlainText, K_C), K_D)$$

where C and D represent the confusion and diffusion functions with keys K_C and K_D respectively and n and m are the corresponding number of rounds performed of each of these

functions. As key is the secret part of any cryptosystem, its strength is majorly dependent on the key-space. For the general cryptosystem defined above, the key-space is $S = (S_C{}^n S_D)^m$ but increasing the number of rounds n and m arbitrarily to increase the key-space leads to increase in the computational cost and therefore a balance needs to be struck between security and speed.

There are two approaches of utilizing chaos for securing data namely -- a) digital chaos b) chaos synchronization [26]–[28], the former is applicable to digital content while latter is applicable directly on analog devices by modulating signals with chaotic signals without requirement to digitize. Digital chaos-based systems are further classified in two types: chaotic stream cryptosystems and chaotic block cryptosystems, where in the former, chaotic functions are used to generate a key stream which is further applied upon as one-time pad on the plaintext with simple operations like XOR, XNOR etc. while in the latter, blocks of plaintext are encrypted using chaotic maps into equally sized cipher text.

Matthews marked the beginning of chaotic cryptography with his paper proposing use of 1-D chaotic map to be used as one-time pad for symmetric stream cipher [27]. Habustu et al. [29] proposed the iterative use of inverse 1D chaotic map (tent map) on initial point representing plaintext. The paper elaborated on the parameter requirements like plaintext & key sizes, times of mappings (iterations), and focused on finite computation size as a means to avoid ciphertext-only attacks to which the system is otherwise vulnerable to as a result of linearity attributed to the tent-map. Further many researchers like Baptista (1998), Alvarez et al. (1999) proposed simple encryption schemes exploiting the ergodicity characteristic of chaotic maps [27].

Besides text, chaos has emerged as an important class of encryption algorithms especially for visual media. Chaotic maps when iteratively applied on two initially close points due to mixing property and high sensitivity to initial conditions, generates results that diverge significantly after a few iterations and loose their correlation. This characteristic of chaotic maps is exploited in visual content like image encryption because adjacent pixels normally have strong correlation and this redundancy in the plaintext gets dissipated in the chaos-based cipher text. Fridrich [30] proposed a 3-step approach to adapt 2D chaotic map to be used in a symmetric cipher for image encryption:

a) Generalizing the chaotic map by introducing parameters which may form part of the secret key.
b) Discretizing the continuous chaotic maps onto finite lattice points representing pixels of the image.
c) Extending to three dimensions in order to introduce substitution of gray values along with permutation of pixels, followed by diffusion of pixels in plaintext across multiple pixels in the ciphertext (besides permutation achieved by the discretized chaotic maps).

Following figure, Fig. 4, is the block diagram of the Fridrich's scheme:

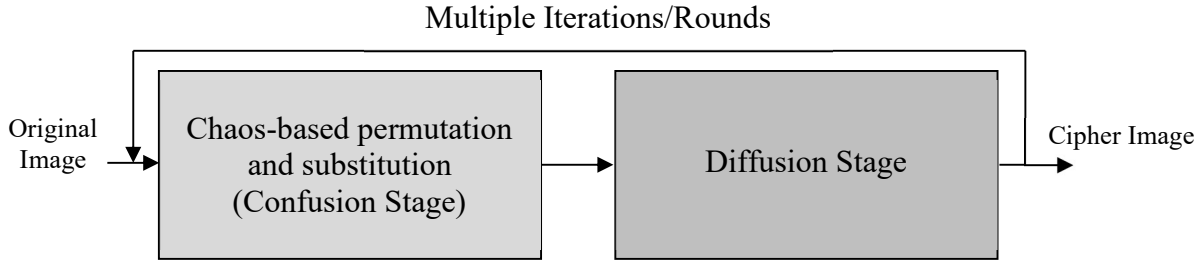


Fig. 4 Block Diagram for Fridrich's Scheme

Lian et al. [31] analyzed the security of Fridrich's algorithm with three different chaotic maps namely Standard Map, Cat Map and Baker Map. He proposed metrics to study key-space, key sensitivity, confusion & diffusion properties and used them to give a comparative study on the use of the three mentioned chaotic maps to avoid known-plaintext, select-plaintext and other statistical attacks. Further he discussed the computational complexity of these chaotic maps & diffusion functions and suggested balance based on the practical application requirements for the trade-off that exist between security and computational complexity. He also proposed security improvements in terms of parameter selection and other scheme design related issues so as to improve the overall strength of the chaos-based schemes.

In another paper Lian et al. [32] incorporated these suggestions and proposed a new block cipher based on improved Standard Map introducing corner pixel confusion with the help of random-scan process. He further proposed some optimizations for reducing computational complexity and elaborated on the proposed system having chaotic confusion, diffusion & key generation (for different iterations) as its integral components. Rigorous security analysis is performed to manifest the strength of the scheme. Results showed that scheme has higher

security for bigger plaintext matrix and thus making it attractive for use in securing large voluminous multimedia exchanges as opposed to traditional ciphers like AES, DES where the block size is fixed.

Fridrich's approach was further extrapolated by Mao et al. [33] from 2D to 3D Baker Map having separate confusion and diffusion stages. Mao et al. proposed to convert the 2D image to a 3D cuboid, and then perform round operations which employ 3D bakers map to perform permutation followed by chaos-based diffusion/substitution. The number of rounds depends on the security requirements. Theoretical & statistical analysis and performance results demonstrate that the proposed scheme possess higher security with higher computational efficiency thereby suiting it for real-time applications. Following figure Fig. 5 is the block diagram for this scheme:

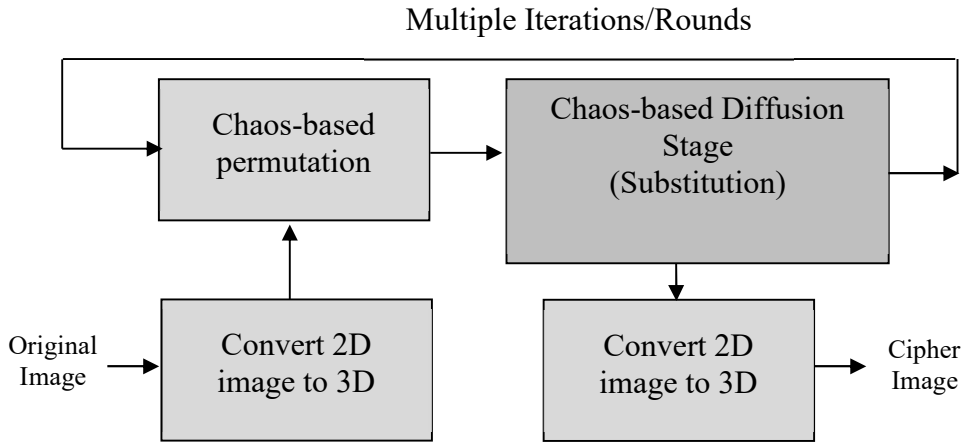


Fig. 5 Block Diagram for Mao et al.'s Scheme

Francois et al. [34] proposed a new approach of using simple chaotic function (logistic map) to perform combined substitution-permutation in an iterative fashion treating the entire image as input stream of 0's and 1's. The author theoretically explained the choice of number of rounds/iterations based on key-space. In-depth security analysis in terms of bit propagation, correlation & randomness analysis, key & plaintext sensitivity is performed along with efficiency comparisons with other chaos-based schemes. Based on the results, a fast and secure scheme is concluded for image encryption treating it as a mere stream of bits, thereby widening the scope of its application on textual data as well. Following figure Fig. 6 is the block diagram for this scheme:

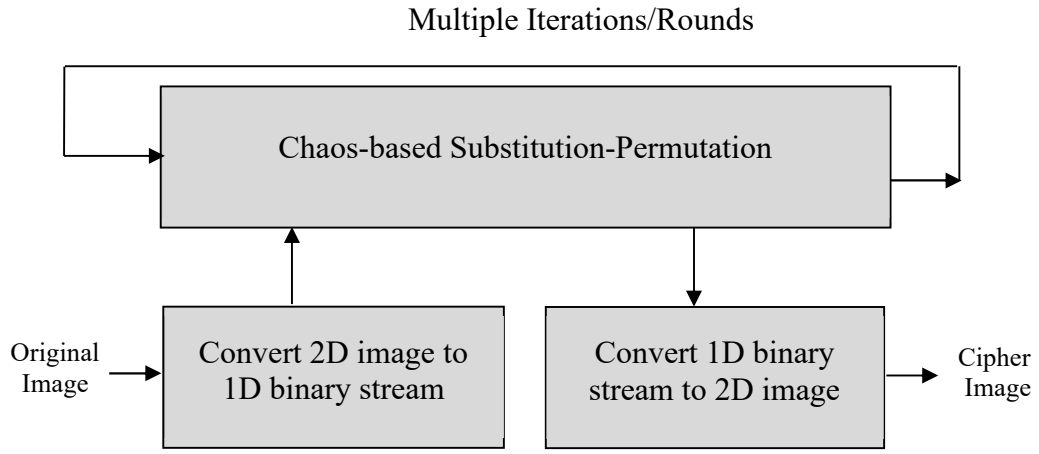


Fig. 6 Block Diagram for Francois et al.'s Scheme

Also, basic guidelines are highlighted and rules are suggested to be followed for designing secure cryptosystem based on chaos in [28]. Security analysis measures, various kind of cryptanalytic attacks on cryptosystems and ways to overcome them enhancing the strength of the overall system are also elaborated in [28].

Giving another dimension to the scope of chaos-based encryption schemes Gschwandtner et al. [35] studied their robustness against transmission errors on noisy channels and lossy compression. The comparative study between traditional ciphers like AES and chaotic-map based permutation only ciphers show that the former can sustain buffer errors to a limited extent while the latter can resist value errors effectively. Also, this tolerance of the latter against value errors in turn explains their potential for supporting lossy compression in the encrypted domain which in no way possible with traditional ciphers. The same is also verified experimentally by the author. But a point to note here is that this tolerance against transmission error and support for lossy compression is achieved on the cost of weaker security as a result of doing away with the diffusion stage.

Chen et al. [36] proposed new format of treating image in the form of 8-independent sub-images transformed using 8-bit planes corresponding to the 256 grayscale levels. To decrease the computational complexity, the upper sub-images with lower information value are applied on with diffusion, while on the remaining, both permutation and substitution are performed.

Kadir et al. [37] made use of skew tent map and hyper chaotic system for generation of confusion and diffusion sequences respectively with application of very basic arithmetic operations for encrypting the RGB components of the color pixels of the image. The strength of the scheme has been proved through thorough security and key-space analysis.

Further, due to vulnerability of chaos-based schemes towards cryptanalytic attacks as discussed later, instead of single chaotic maps several researchers like Gupta and Silakari [38], Alsafaseh and Arfoa [39] in separate works proposed the use of multiple chaotic maps cascaded one after the other or by deriving a new chaotic map from existing chaotic maps keeping the basic operations simple like XOR (exclusive-OR). As per the statistical & sensitivity analysis and time measurements the authors claim that the schemes provide high security while incurring low computational cost. Many more new, improved or hybrid chaotic maps [40]–[52] are being proposed by making improvisations or by combining more than one chaotic map to enhance the chaotic behavior of existing maps. The use of chaos in image encryption is still being explored continuously by researchers including some very recent works [53]–[57].

Despite the significant achievements in the field of chaos-based cryptography, due to the attempt to keep operations simpler for achieving computational efficiency, and due to complete dependency on randomness attributed to chaotic maps as a means of security, many chaos-based schemes have been found vulnerable to cryptanalytic attacks. Especially, the chaotic key-stream based or chaos-based simple permutation and/or substitution ciphers are found susceptible to differential cryptanalysis, known & chosen-plaintext attacks. Papers [58] and [59] discusses cryptanalysis of two such chaos-based schemes. Xu et al. [58] suggests intermediate-cipher feedback to be included as part of the design of the attacked scheme so that the plaintext pixels get diffused across multiple pixels in the final cipher text. It is relevant to mention that Li et. al. [60] has quantitatively estimated that $O(\lceil \log_T (M.N) \rceil)$ known/chosen-plaintexts are required for an efficient plaintext attack on any permutation-only multimedia ciphers with upper bound on the attack complexity to be $O(n.(M.N)^2)$ where M.N represents size of the image, T is the number of possible value levels and n is the number of known/chosen-plaintexts. The cryptanalysis proposed in [61] could be extended to any permutation-only image cipher and this further improved the computational complexity of the plaintext attack for permutation-only cipher to O(n. (M.N)). Li et. al. [62] cryptanalyzed a permutation-only image cipher called Hierarchical Chaotic Image Encryption (HCIE) proposed by Yen et. al. [63]. There are several more chaos-based encryption schemes which

have been cryptanalyzed, some of which very recently [64]–[73]. A survey on cryptanalysis of chaos-based image encryption schemes has been given in Section 2.3.

Besides the criticized low security, another criticized weakness of chaos-based systems is the continuity attributed to most chaotic functions [27]. The criticism is that the use of chaos requires floating-point number processing but this criticism does not stand much, as today's machines are well equipped to process real numbers with ease and efficiency. In fact, this very characteristic of chaos, i.e. playing with real numbers, actually possess great potential and makes it a strong contender to provide security solutions esp. for multimedia in post-quantum computers [74]–[81].

2.1.3 Cellular Automata-based Encryption

The concept of cellular automata is used to encrypt images [82]–[89] by defining a cellular automaton which comprise of a grid of cells corresponding to different states. The cellular automaton also defines the state transition rules which specify the next state of a cell based on the state of the pixels in the neighbourhood including the current state of this cell as well. The cellular automaton is used for pseudorandom generation as well as to perform permutation and substitution operations in image encryption schemes, like, in [88] the cellular automaton is used to generate pseudorandom key-image which is further used to decide operations used to perform substitution on each pixel of the original image to generate the cipher image. The approach of use of cellular automata in image encryption offers unpredictability due to very large number of state transition rules possible based on the radius of neighbourhood. It is also easy to be implemented in hardware and supports parallelism.

2.1.4 DNA encoding-based Encryption

DNA is a biological term which refers to Deoxyribonucleic acid and it carries genetic information of living organisms. There are four types of nucleotides contained in DNA namely cytosine [C], guanine [G], adenine [A] or thymine [T]. Nucleotides A & T are complementary to each other, similarly, nucleotides C & G are complementary to each other. DNA computing was proposed by Adleman in his pioneer work [90] solving an instance of directed Hamiltonian Problem using DNA molecules. The concept of biological DNA has been extended in cryptography, and researchers [91, 92] have proposed use of real biological DNA operations

for message hiding and security but it is not found practically very feasible for real world applications due to high cost and highly equipped lab requirements. Therefore, pseudo DNA cryptography was proposed in [93] which does not involve real DNA and biological operations but simulates principle processes of microbiology for application in cryptography specially to enhance security of other cryptography methods. Extending the work for images, over the last decade several researchers have proposed image encryption schemes based on DNA encoding [94]–[104]. An image is a 2D collection of pixels which are internally represented in binary as 0s and 1s. In this approach, the image is encoded as DNA sequences and DNA operations are defined. Since there are four nucleotides so encoding rule is defined to encode pair of bits as nucleotides. As there are four nucleotides there exists 4! i.e. 24 rules for encoding but since A & T are complementary and C & G are complementary hence following these complementary rules for DNA, 8 rules of encoding are possible which are as follows:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

Any of the encoding rules can be used to generate the DNA sequence and the DNA sequence is then subjected to substitution by defining specific DNA rules/operations. The DNA sequence is converted back to binary again using one of the above rules to generate the cipher text. Mostly, the DNA coding is being used along with chaos. In [94] DNA addition and subtraction operations have been defined. The m×n image is firstly converted to m×(n×4) DNA sequence matrix which is further divided in 4×4 blocks and chaos is used to select the pair of 4×4 blocks DNA blocks on which DNA addition is applied. This is then followed by chaos-based DNA complement operation in order to complete substitution operation on the DNA sequence matrix and finally DNA sequence is decoded back to get pixel values for the cipher image. The paper [95] uses chaos to permute the original image pixel values before converting it to DNA sequence matrix which is created by randomly choosing among the eight encoding rules to generate the DNA sequence. Then chaos-based DNA complementary substitution is performed by randomly selecting one from the six complimentary base pair rules and finally the DNA

sequence is converted back to binary again using randomly selected decoding rule to get the final cipher image. A similar image encryption scheme was proposed in [96] with use of the original plain image's hash (MD5) value for generating initial conditions of the piecewise linear chaotic map (PWLCM) and the Chebyshev maps used during encryption. In the paper [97], chaos is used for choosing the DNA mapping rule for encoding/decoding the image to/from DNA sequence and also for permuting the DNA sequence values. Several more such schemes based on DNA encoding along with use of chaos for image encryption have been proposed by researchers [98]–[104] and some of them have also been cryptanalyzed as well based on weakness in their respective designs [105], [106]. Besides using DNA based encoding, some researchers have proposed use of real DNA sequences as keys for the image encryption process [100], [101]. Also, in [101] the authors proposed image encryption based on their defined Reversible T-DNA cellular automaton, DNA XOR operation, DNA Multiplication operation, DNA Matrix Multiplication operations etc. thereby combining cellular automata along with DNA encoding and chaos together to enhance avalanche effect and ensure high security.

2.1.5 Encryption in Transform Domain

These algorithms use Digital Signal Processing as the basis. The input signal is first converted into frequency domain using transforms like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) etc. The transform coefficients and the motion vectors are then made to undergo operations based on the key followed by reverse transform to get the encrypted image. Some researchers have also used chaos to perform encryption in transform domain [107]–[115]. In the paper [112], discrete fractional wavelet transform has been defined and its application for multiple image encryption has been proposed which encrypts a set of images together and using a sharing rule the encrypted images are shared into each other to get a shared set of encrypted images. In the work [113], use of wavelet is proposed to compress the original image and subsequently chaos-based permutation-substitution encryption is performed on the compressed image. Bao et al. [116] propose SP-Network based encryption followed by hiding the encrypted image in cover image using wavelet transform to ensure that the adversary does not even attempts to attack such an image because the encrypted image does not appear noise-like.

2.1.6 Selective Encryption

Selective encryption is an approach where only parts of the data are encrypted instead of encrypting huge volumes of data. Significant data portions are identified to be encrypted so as to reduce the computational requirements on networks with different client device capabilities. Bhatnagar and Wu [117] proposed to improve efficiency of their encryption scheme by performing the permutation stage using Saw-Tooth space filling curve on the entire original image while chaos-based diffusion stage is being performed only on significant pixels where these significant pixels have been identified using intensity, contrast, location, edginess and texture as parameters in this scheme. Som and Sen [118] treated a grayscale image in terms of 8 bit planes and proposed chaos-based encryption of four significant bit-planes determined by 5% level of significance on contribution of a bit-plane in determination of a pixel value. The approach of selective encryption has been extended to transform domains as well. Taneja et al. [119] used fractional wavelet domain and significant subbands are identified having energy greater than a set threshold energy. These significant subbands are then encrypted using chaos with an intent to achieve a balance between efficiency and security. Similarly, Discrete Wavelet Transform is used in [120] and it uses RC4 to encrypt the lower frequency band besides using shuffling algorithm to shuffle the rest of the image. In fact, [121]–[123] provide reviews on significant contributions in the area of selective encryption for securing multimedia like images.

2.2 UNTRADITIONAL APPROACHES TO ENCRYPTION & THEIR APPLICATIONS FOR SECURING VISUAL CONTENT

2.2.1 Dynamism

The roots of dynamism can be observed from polyalphabetic ciphers proposed as early as 16th century like Vigenere cipher where the idea to use of different transforms based on the secret key first surfaced. In 1984, S. Goldwasser et al. [124] proposed a new approach for encryption called Probabilistic Encryption. The authors highlighted that the traditional ciphers are deterministic trapdoor functions using secret information as trapdoor for security. And there exists a finite possibility that full or partial information about the plaintext may get revealed when attacked by adversary. To address this, the authors propose a probabilistic framework replacing the static one. As per probabilistic encryption, the same plaintext bit 0 or 1 could be

encrypted in several encodings in the cipher text where a possible encoding is chosen through a random mechanism. It is evident that probabilistic encryption framework encourages dynamism in selecting possible encoding for the same message bits in the cipher text to make it tough for the adversary to attack.

A stream-cipher structure is proposed in [125] and use of dynamism is proposed for generating chaos-based pseudo-random key stream used to perform encryption. Pareek et al. [126] proposed dynamism in deciding length of blocks, choosing one chaotic map (for encryption of the block) among four chaotic maps along with their initial conditions and the number of iterations made to the chosen chaotic map. Later, Wei et al. [127] cryptanalyzed this work but did not criticize the dynamic approach, instead, they suggested improvements to strengthen the dynamism by making it plaintext dependent besides being key-dependent. Such dynamism in choosing among multiple chaotic maps has been proposed in [128]–[132] as well.

The papers [133] and [134] proposed use of dynamically changing keys for encrypting different data packets of a communication so as to provide strength against cryptanalytic attacks by adversaries and to ensure that a compromised key do not reveal much information about the communication thereby not causing much harm. Several researchers [135]–[144] have taken the idea of dynamism in keys to another level by making keys dependent on plaintext in the image encryption algorithm or using information extracted from the plaintext (like average intensity value, hash value etc.) and utilizing it in the image encryption operations thereby using this plaintext related information indirectly as the key which definitely needs to be communicated to the receiver along with the key for decryption at the receiver's end. Communication of such plaintext related information in a secure manner to the receiver is required for smooth decryption. It can be done either by hiding such plaintext related information inside the cipher text itself [135] or otherwise securely communicating it with the key, which is not always practically feasible especially in resource constrained environments.

Pareek et. al [145] proposed a block cipher suitable for real-time image encryption. The block cipher involves dynamism by making chaos-based selection of operations to be performed for encryption of each pixel of the image. In another work, Dhall and Pal [146] proposed a 128-bit block cipher based on key-based conditional encryption. The algorithm comprises of two steps i.e. re-adjustment phase and substitution & shifting phase whose operations vary based on the key. Later, Korstanje and Keliher [147] cryptanalyzed the scheme [146] by proposing

distinguishing attacks and plaintext-recovery attacks for keys with certain specific characteristics but did not criticize the conditional nature of choice of operation as such.

Several encryption schemes like Blowfish [148], Twofish [149] use dynamically generated key-dependent S-Boxes in the substitution step of the scheme. Key-based dynamic selection of S-Box for substitution is proposed in [150] and [151]. Further, papers [144], [152] and [153] proposed improvisations on the scheme proposed in [151]. Also, several researchers in their works [154]–[162] have proposed use of key-dependent S-Boxes in the standard algorithms like AES and have demonstrated and proved the strength of introducing key-based dynamism in this form.

Not only for image encryption schemes operating in the spatial domain, the idea of dynamism has also been used in schemes operating in transform domain as well. Key-based dynamic selection of wavelet transform used for image encryption has been used in [163]. The idea of Dynamic Encryption has been discussed most explicitly by Knudsen in [164] where it has been proposed that the while performing encryption and decryption respectively at the sender's and receiver's ends, the receiver is kept unaware about the cryptosystem being used for encryption and only key is known to the receiver. The choice of cryptosystem being used for encryption is being kept to the sender who can change it as often as per message. To ensure smooth decryption at the receiver's end, the sender communicates the executable code for decryption or encrypted decryption algorithm to the receiver along with the cipher text. On receiving the decryption algorithm along with the cipher text, the receiver can decrypt the message using the known shared key. The paper proposes practical advantages for email systems, cloud storage and mobile conversations. This idea has been extended in one of our research works but with a difference as elaborated in Section 4.2. Unlike dynamic encryption proposed by Knudsen [164], in our work the dynamic framework itself takes care of offering key & plaintext dependent dynamically changing encryption operations while the receiver is fully aware of the decryption algorithm i.e. there is no need to communicate or send the decryption algorithm separately to the receiver.

2.2.2 Probabilistic Encryption

The origin of probabilistic encryption is marked by the landmark work by Goldwasser et al. [124, 165] which gave a new dimension to encrypting messages using public-key

cryptography, with proven higher security. In probabilistic encryption, different ciphertexts are produced at different times even when the same encryption scheme is applied with the same key to the same plaintext. The authors highlighted that the traditional deterministic approach is vulnerable to revelation of complete or partial information about the plaintext by rigorous analysis of the cipher text. But with the probabilistic approach, a new concept of semantic security surfaced, i.e., the extraction of any information about the plaintext is hard with polynomially bounded resources. To achieve this, different encodings for same bit 0 or 1 of the plaintext is introduced by employing the concept of probability through random coin flips, and quadratic residuosity problem is used to achieve the desired computational hardness. Later, Fuchsbauer [166] also gave a focused elaboration on the work by Goldwasser et al., and the related number-theoretic concepts for easier understanding.

Rivest and Sherman [167] discussed the role of randomization in generating different cipher text for the same plaintext with the same encryption key at different times. The paper also discussed benefits of randomization and several ways in which randomization can be used in encryption process. ElGamal [168] proposed a public-key cryptosystem based on the difficulty of discrete-logs computation in a large prime modulus. It employs use of a random number, chosen for one-time use for each message being communicated between the communicating parties, making it a probabilistic encryption scheme. Blum and Goldwasser [169] also proposed a probabilistic asymmetric encryption scheme based on intractability of RSA function along with ensuring efficiency as a key trait of the scheme, making it the first of its kind at that time. Okamoto and Uchiyama [170] proposed another provably secure probabilistic public-key encryption scheme based on multiplicative group over ring Z/nZ, where $n = p^2q$ and p, q are primes. The work was later extended to design EPOC (Efficient Probabilistic Public-Key Encryption Scheme) with three versions [171], [172]. Fujisaki and Okamoto [173] proposed a generic model for hybridization of symmetric and probabilistic asymmetric encryption schemes with a purpose to make the resultant scheme highly secure. The authors proved that the resultant asymmetric encryption scheme possesses indistinguishability under chosen ciphertext attack (IND-CCA) irrespective of the strength of the component symmetric and asymmetric schemes used.

Initially, for around two decades, researchers utilized the probabilistic approach in the area of public-key cryptography. Lately, researchers started exploring the scope of probabilistic encryption in symmetric cryptography as well. Papadimitriou et al. [174] proposed a

probabilistic symmetric encryption scheme based on chaotic systems which encrypts a d-bit plaintext to e-bit cipher text such that e > d. The chaotic system is used to create 2^d virtual attractors containing 2^e virtual states. A 1×2^d permutation matrix P is defined representing 2^d virtual attractors with 2^e possible virtual states. Each virtual attractor is associated with some message symbol. The permutation matrix P is then used to map the plaintext symbol to the corresponding cipher text by pseudo-randomly selecting a virtual state (corresponding to the virtual attractor) from matrix P to be the cipher text for the plaintext symbol. Later, Li et al. [175] identified defects in the original proposal, as it largely depends on plaintext and cipher text size for security, and the original proposal is found to be insecure for small sizes used in practical implementation.

Few probabilistic symmetric encryption schemes have been proposed by researchers based on neural networks as well. Leung et al. [176] discussed some defects in an existing probabilistic symmetric encryption scheme based on the chaotic properties of Overstoraged Hopfield Neural Network (OHNN) [177] and suggested another probabilistic symmetric encryption scheme based on clipped Hopfield Neural Network (CHNN) to overcome the shortcomings of the earlier scheme [177].

A symmetric encryption block cipher using the concept of randomization was also proposed by Reddy et al. [178] which encrypts messages in blocks of size 32-bits. The scheme uses six 32-bit random numbers for generating round keys and performing per-round operations. The scheme employs three rounds and random numbers are generated for encrypting set of 250 blocks at a time. Later, Reddy et al. [179] also proposed another probabilistic symmetric block cipher using two 32-bit random numbers in a similar manner in per round-operation as in the earlier scheme. But here same random numbers are used to encrypt the entire plaintext. The scheme works on 64-bit block, has a Fiestel structure, employs six rounds, and involves substitution, rotation and 2's complement as some of the basic operations. In both the schemes, encrypted random numbers are also inserted within the cipher text at key-dependent locations for ensuring smooth decryption by the receiver. But these schemes use random numbers more or less like portion of the hidden secret (i.e. the key, but not literally) which is kept in an encrypted manner inside the cipher text itself. This kind of use of random numbers is not as per the true spirit of probabilistic encryption. It appears to lack one of the basic aspects of

introducing randomization [166] i.e. smoothing out the distribution of 0s and 1s in the plaintext itself and increase the apparent message space size for the attacker.

Ratha et al. [180] proposed another probabilistic symmetric encryption scheme which uses arbitrary n × p matrix for key sequence generation used in the encryption process, where n is the size of the plaintext but the definition of p is unclear. As the scheme description lacks clarity and the authors also didn't explicitly state that how is the arbitrary matrix communicated to the receiver for decryption, hence it does not appear practically implementable in real world as per its original definition. Though, the authors call the scheme optimized yet as per their own observations the algorithm's performance is not fastest among the schemes they chose for comparison. Reddy and Vishnuvardhan [181] proposed use of probabilistic encryption by generating variable length sub key groups using random sequence for simple linear transformations used for converting plaintext to cipher text.

2.3 Survey on Cryptanalysis of Chaos-based Image Encryption Schemes

Though due to efficiency reasons chaos has been widely utilized in proposing new image encryption schemes by researchers yet very often such schemes have been found vulnerable to cryptanalytic attacks. This is due to the simpler and weak designs of the proposed schemes where, normally, reliance of the strength of the scheme has been largely made alone on the random-like unpredictable behaviour of chaotic functions for the adversary in absence of knowledge of the key (comprising of the initial parameters and conditions of the chaotic function used in the scheme) without focusing on the design of the scheme.

Tu et al. [182] cryptanalyzed a chaos-based permutation-substitution cipher [183] for color images and suggested improvements to overcome the identified weaknesses. The original cipher comprised of a permutation step to effectively shuffle bytes across rows and columns of all the three RGB color planes. The intermediate ciphered color image is then reshaped into 3 color planes. Further, the diffusion step is applied by chaotically selecting bytes from the 3 planes to perform add and mod operations with the key stream, previous cipher and original pixel values. Overall, two logistic maps with different initial conditions and parameter values are used to generate required key stream values for the permutation and diffusion steps. Tu et al. identified two weaknesses in the scheme, i.e., use of two fixed parameters $P_0 = C_0 = 0$ during the diffusion step for the first pixel and use of only key-dependent key-stream for permutation.

Exploiting these weaknesses, they demonstrated chosen-plaintext attack on the shuffling rule and diffusion rule to break the cryptosystem by retrieving the respective key-streams for these steps. Further, to overcome these weaknesses they suggested plaintext dependent shuffling (or permutation) and incorporation of values P_0, C_0 used during diffusion as part of the secret key.

Wang et al. [184] showed weaknesses in the use of order of orbit of logistic map in bit-level scrambling of the pixel bits across rows and columns during image encryption proposed in [185]. The authors claimed that the order of the orbit does not provide desired randomness and hence is vulnerable to be attacked for deduction of the initial seed value of the logistic map used during encryption. They gave theoretical analysis and numerical experimental results to establish the identified possible breach in the cryptosystem. The same encryption scheme had been cryptanalyzed using chosen-plaintext attacks earlier in [186], [187] and [61] as well, each cryptanalysis showed subsequent improvement over the previous, in terms of reduced number of plaintexts/cipher texts required to break the cipher. In [61] the authors also highlighted some weaknesses in the original scheme [185] which includes inability to encrypt images with fixed values 0 or 255, insensitivity to change in plaintext and very importantly, weak randomness in the key-streams generated using logistic map. The weak randomness issue was also pointed out in [187] and was exploited by Wang et al. in [184] as elaborated above. In addition, the authors of [187] also suggested some improvements like use of spatiotemporal chaotic map instead of logistic map and introduction of the idea of the self-correlation encryption to ensure that the key-streams used in the encryption process depend on the key as well as the plaintext. In [186] the authors analyzed the encryption scheme [185] from point of view of three possible versions/cases and proposed attacks with least number of required plaintexts (as compared to cryptanalysis proposed in [61] and [187]) and the attacks can be used to crack most other permutation approaches adopted in chaos-based image encryption.

It is relevant to mention that Li et al. [60] has quantitatively estimated that, in general, $O(\lceil \log_T (M.N) \rceil)$ known/chosen plaintexts are required for an efficient plaintext attack on any permutation-only multimedia ciphers. The computational complexity of the attack is proposed to be $O(n.(M.N)^2)$ where M.N represents size of the image, T is the number of possible value levels and n is the number of known/chosen plaintexts. Further, an improvement in the computational complexity of the plaintext attack for any permutation-only cipher to $O(n.(M.N))$ has been proposed in [61].

Li et al. [62] cryptanalyzed a permutation-only image cipher called Hierarchical Chaotic Image Encryption (HCIE) proposed by Yen and Guo [63]. The cipher involves two-level hierarchical permutation procedure using four rotation mappings. The image is considered to be divided into a number of equal sized blocks/sub-images which are permuted among each other at the first level. Further, at the second level, the pixels within each block/sub-image are permuted within the block/sub-image. Contrary to the higher security claims made by Yen and Guo in [63], Li et al. analyzed that the security of the scheme has been overestimated and proved that it is even more easy to perform cryptanalysis on HCIE as compared to any other permutation-only image cipher. Li. et al. demonstrated chosen plaintext attack requiring only $O(\lceil \log_T (M.N/K) \rceil)$ known/chosen plaintexts with computational complexity of $O(M.N.\lceil \log_T (M.N/K) \rceil)$ where M.N represents size of the image, T is the number of possible value levels and K is the number of blocks/sub-images. Clearly, the number of required plaintexts for the attack is lesser than those required for a non-hierarchical permutation-only cipher. This is because, the hierarchical permutation structure facilitates the attacker to perform cryptanalysis and identify permutation matrices for sub-images having size much smaller than size of the original image. This apparently can be done using lesser number of known/chosen plaintext images.

Özkaynaka et al. [188] cryptanalyzed the substitution-only cipher [189] comprising 2 rounds of diffusion operation based on XOR (exclusive-OR) and mod operations among plaintext pixel value, previous encrypted value and the substitution key stream value generated using hyper-chaos. The authors demonstrated a mechanism for complete extraction of the key-dependent hyper-chaotic sequence by taking a small example of a 2×2 image, which in principle is applicable on any sized image. The authors highlighted on the fact that though the actual key parameters used in the hyper-chaotic system may not be revealed directly, yet, the attack revealing the intermediate secret parameters is sufficient to break the cipher.

Norouzi and Mirzakuchaki [190] cryptanalyzed another chaos-based permutation-substitution cipher for encrypting images proposed by Parvin et al. [191]. The structure of the cipher involves row and column permutation followed by a substitution stage similar to the one used in [189]. For the first pixel of the image, a value calculated based on pixels of the entire image, is used in XOR operation, while for others, previous encrypted pixel is used, along with the

plain image and key stream value. The said operations use three pseudo-random sequences generated using two 1D chaotic maps and their combination. Norouzi and Mirzakuchaki [190] exploited the simple design of the scheme and suggested chosen plaintext attack to recover the substitution key stream and subsequently the two permutation key streams hence breaking the encryption algorithm.

Chen and Wang [192] cryptanalyzed multiple-round chaos-based cipher [193] involving bit-level permutation and pixel-level substitution steps. In [193] the authors claimed bit-level permutation to be an effective way of achieving substitution effect during permutation itself thereby adding strength to the cipher. Prior to Chen et al. the same work has been cryptanalyzed for single round of the encryption steps by Zhang et al. [194]. Zhang et al. analyzed that bit-level permutation does not practically add additional strength to the cryptosystem and demonstrated extraction of the substitution key streams and permutation matrix for all bit-planes using chosen-plaintext attack for single-round encryption. The argument given by Zhang et al. for cryptanalyzing only single-round encryption process is that, single round encryption process already involves three iterations of permutations using Arnold's Cat Map, one for each of the three 8 bit-planes of image, and a XOR based substitution step which involves excessive computational load, thus if multiple rounds of this process are employed it may not be suitable for real-time applications. Besides cryptanalyzing single round encryption, they also suggested inclusion of another permutation step i.e. Permutation-Substitution-Permutation architecture as an improvement over the existing Permutation-Substitution structure. But this proposed improvement has been criticized to be insufficient to resist differential attacks by Chen et al., though no theoretical or experimental elaboration has been given by them to directly address this claim. Further, Chen et al. demonstrated differential cryptanalysis on the multiple-round original scheme [193]. In their work, they analyzed that the substitution key stream has no impact on the differential cipher and it depends only on the permutation step. They further elaborated on the mechanism to extract complete permutation key for one, two rounds of encryption with 17 chosen plain images. For three or more rounds of encryption, they proposed double differential cryptanalysis comparison (DDCC) in which two special plain-image sets are chosen and with $16N^2+1$ plain images (where N^2 is the size of plain image) the equivalent permutation key can be extracted.

Özkaynaka and Özer in their work [195] criticized use of only statistical tests and experimental results for performing security analysis of any proposed chaos-based encryption algorithms.

They proposed a general attack scenario to be considered while performing security analysis of chaos-based encryption. Further, they demonstrated an application of the proposed general attack scenario on a chaos-based image encryption proposed by Wang et al. [196]. As part of the general attack scenario, the multiple-round encryption process E is expressed as a simple mathematical model comprising of permutation and substitution functions f and g i.e. E^R (P, K) = (g (f (P, K), K))^R. Further, based on the existing literature related to cryptanalysis of similar schemes, the authors break single round of the cryptosystem and conclude that to assess the security of any proposed chaos-based cryptosystem, its resistance against general attack scenario should be accounted along with statistical and experimental results. There are several more chaos-based encryption schemes which have been cryptanalyzed, some of which very recently [64]–[73].

2.4 TEST IMAGE DATASETS

The test images for analysing the strength of image encryption schemes are normally taken from standard image databases/data sets like:

(i) The USC-SIPI Image Database (University of Southern California) which is available online at http://sipi.usc.edu/database/ .

(ii) Fabien A. P. Petitcolas has made available a photo database specifically for research in information hiding and watermarking in images which is availabale at https://www.petitcolas.net/watermarking/image_database/ .

(iii) The Waterloo Fractal Coding and Analysis Group, University of Waterloo, Canada has made an image repository available for experimentation of image processing algorithms at http://links.uwaterloo.ca/Repository.html .

(iv) Another image database is made available by Pearson-Prentice Hall at http://www.imageprocessingplace.com/root_files_V3/image_databases.htm .

(v) A set of Grayscale images by Computer Vision Group, University of Granada, Spain is available online at http://decsai.ugr.es/cvg/CG/base.htm .

(vi) School of Computer Science, Carnegie Mellon Unversity, Pittsburgh, Pennsylvania, and School of Informatics, University of Edinburgh, Scotland have presented wide collections of image datasets specified at http://www.cs.cmu.edu/~cil/v-images.html and http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm respectively.

Following figures Fig. 7-12 are some of the standard grayscale test images:

Fig. 7 Peppers

Fig. 8 Water Lilies

Fig. 9 Lena

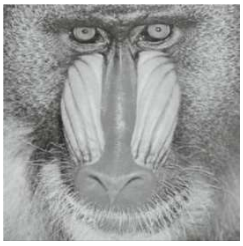


Fig. 10 Baboon

Fig. 11 Cameraman

Fig. 12 Barbara

2.5 METRICS TO MEASURE QUALITY & STRENGTH OF IMAGE ENCRYPTION SCHEMES

The different metrics which are observed to prove the strength of image encryption schemes are as elaborated below:

2.5.1 NPCR, UACI & Correlation Coefficient

NPCR (Number of Pixel Change Rate) [197] is a metric to identify the rate at which number of pixels are changed in the cipher image with one pixel changed in the original image. Likewise, UACI (Unified Average Change Intensity) [197] measures the average change in intensity of the pixels in the cipher image with one pixel change in the original image. Both NPCR and UACI values lie between 0 and 1, and the higher the values are the better is the observation in terms of security with ideal values in terms of percentage being over 99% and 33% respectively [197]. Following formulae represented as equations (1) and (2) are the used to calculate NPCR and UACI respectively for cipher images C and C' representing two ciphers images obtained with only one pixel changed in the original image having dimensions M×N:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad \text{where D(i,j)} = \begin{cases} 0 & if\ C(i,j) = C'(i,j) \\ 1 & if\ C(i,j) \neq C'(i,j) \end{cases} \tag{1}$$

$$\text{UACI} = \frac{\sum_{i,j} |C(i,j) - C'(i,j)|}{M \times N \times 255} \times 100\% \tag{2}$$

While NPCR and UACI are calculated between two cipher images with one-bit changes in the original images, correlation coefficient is evaluated between the original image and the cipher image. It is an indicator of the relationship between the original image and the encrypted counterpart. Its value lies between -1 to 1, where values closer to 1 indicate strong correlation, values closer to -1 indicate strong anti-correlation and values closer to 0 indicate minimal relation between the original and the cipher image. The formula for calculating correlation coefficient for original image P and corresponding cipher image C is represented as equation (3):

$$\text{Correlation Coefficient} = \frac{\sum_{i,j}(P(i,j)-\bar{P})(C(i,j)-\bar{C})}{\sqrt{\sum_{i,j}(P(i,j)-\bar{P})^2 \sum_{i,j}(C(i,j)-\bar{C})^2}} \quad (3)$$

where $\overline{P}$ and $\overline{C}$ represents the average pixel intensities in the plaintext and cipher text respectively.

2.5.2. Histogram Analysis & Entropy

To prevent statistical analysis, the frequency of pixels with different possible intensities in an image should be evenly distributed. This is studied through histogram analysis where a histogram is a plot representing the number of pixels in the image with each color intensity and a uniform histogram depicts that the encrypted image is more resistant against statistical attacks.

The pixel intensity distribution can further be quantified in terms of entropy which basically represents the average number of bits required to represent each pixel value with an ideal value being 8 for a grayscale image. It is calculated using the following formula as shown in equation (4):

$$\text{Entropy} = -\sum_{i=1}^{N} P(S_i) log_2\big(P(S_i)\big) \quad (4)$$

where, S_i represents the bins corresponding to the different color intensities and $P(S_i)$ represents the probability based on frequency of pixels belonging to the i^{th} bin.

2.5.3 Key Sensitivity & Avalanche Properties

Avalanche Effect is a desirable property of cryptographic algorithms. Avalanche Test is used to evaluate Key Sensitivity. The definition of avalanche effect [198] is given as:

"For a given transformation to exhibit the avalanche effect, an average of one half of the output bits should change whenever a single input bit is complemented."

The different observations which are made to test the key sensitivity and avalanche properties are:

i) Number of bits changed in the cipher image with one bit change in the key at all positions.

ii) Number of bits changed in the decrypted cipher image when decrypted using one bit change in the key at all positions.

iii) Number of bits changed in the cipher image with one bit changed per pixel at all positions.

CHAPTER 3

DESIGN OF NEW CHAOTIC PRIMITIVES AND CUSTOMIZATION OF STANDARD BLOCK CIPHERS FOR VISUAL CONTENT SECURITY

As stated earlier, visual content like images have been found to be constituting significant portion of today's transmissions and digitally stored data especially in resource constrained devices like mobile phones. Such visual content has special characteristics of being bulky and strong correlation in neighbourhood. Hence, the need for meeting the special requirements of visual content especially in resource constrained environment is obvious. This has led to surge for finding security solution to prevent sensitive visual content from unauthorized access by focusing and explicitly handling these special characteristics possessed by visual content. As also stated in background literature chapter, due to its special characteristics and requirements, while designing encryption schemes for visual content security [199], [200], the objective becomes two-folds:

- The scheme should be efficient and involve less computation so that when it is applied to bulky visual content with requirements like real-time streaming, the quality is maintained with less cost.
- Since visual content contains significant proportions of redundancy therefore the second primary focus is to ensure that there is complete removal of redundancy in the encrypted output thereby ascertaining high strength of the scheme.

Clearly, the standard encryption schemes proven to be highly secure for textual data are not found practically very suitable for visual content because of the high computational cost involved due to bulkiness of visual content. Also, high redundancy attributed with such data makes standard algorithms unsuitable for them. As an approach to find security solution for visual content like images, the standard algorithms are identified to be customized to make them suitable for visual information. Chaos has been used for achieving the said customization of two standard schemes AES and PRESENT in this work where AES is a scheme with high

proven security but involves significant computational cost while PRESENT is an ultra-lightweight block cipher suitable candidate for applications on bulky visual content.

The proposed improvisation/customizations ensure high strength of the proposed schemes since they are built on proven high strength ciphers with customizations using chaos and other operations to make them suitable to be applicable for data of visual forms.

3.1 CHAOTIC MAPS USED

Following are the details of the chaotic maps used in this work for customizing standard encryption schemes to suit visual content security:

a) Logistics Map which is a standard 1D chaotic map given by:

$$X_{n+1} = \mu X_n(1 - X_n) \tag{5}$$

where, most values of $\mu \in [3.57, 4]$ exhibit chaotic behaviour (baring few islands of stability).

b) Improved Logistic Map which is an improvisation of logistic map proposed by Rui [50] given by:

$$X_{n+1} = A_{LG}(\mu, X_n, k) = L(\mu, X_n) \times G(k) - floor\left(L(\mu, X_n) \times G(k)\right) \tag{6}$$

where, $L(\mu, X_n) = \mu X_n(1 - X_n)$ and $G(k) = 2^k, k \in Z^+, k \geq 8$

c) Logistic-tent Map which is a hybrid Logistic-Tent map proposed by Zhou et. al [40] given by:

$$X_{n+1} = \begin{cases} (rX_n(1 - X_n) + (4 - r)X_n/2) \bmod 1 & X_n < 0.5 \\ (rX_n(1 - X_n) + (4 - r)(1 - X_n)/2) \bmod 1 & X_n \geq 0.5 \end{cases} \tag{7}$$

where, $r \in (0,4]$

3.2 CUSTOMIZATION OF PRESENT BLOCK CIPHER FOR VISUAL CONTENT SECURITY

As PRESENT is a highly efficient block cipher which satisfies the first objective for designing encryption scheme for visual content as it is bulky, hence it was an appropriate candidate to be studied for further improvisation to customize it for application on visual content. Though, in

the original proposal of PRESENT, the algorithm design kept focus on efficient hardware implementation, later, Z. Gong et al. [201] proposed fast and compact software implementation of PRESENT using look-up tables to add efficiency to the permutation layer. But direct application of PRESENT on visual content like images demonstrate that the redundancy in the original image gets propagated to the cipher image as well because of the limited size of the block encrypted i.e. 64 bits. Thus, in the proposed work, chaos is being used for improvisation of this scheme without significantly increasing the computational cost. The key-size of the proposed scheme is increased from 80 bits to 128 bits where 80 bits are used in same manner as in the original PRESENT scheme and remaining 48 bits are used in determining the initial condition for the chaotic map. The increase in the key-space adds to the security of the improvised block cipher.

3.2.1 Proposed chaos-based improvisation of PRESENT with fewer rounds

In the proposed improvisation, to keep the scheme lightweight one of the simplest 1D chaotic maps is used i.e. the logistic map with control parameter $\mu = 4$. And the operation with this chaotic map is also restrained to be the simplest i.e. XOR. To elaborate, a sequence of random-like numbers is generated using the logistic chaotic map with key dependent initial condition or seed (x_0).

Further, these generated values are XORed with the result of XORing of current state and round key as part of each addRoundKey step of the PRESENT algorithm [11]. To ensure that redundancy that exist beyond the block boundaries in the plaintext (input image) gets removed completely the key dependent chaotic values for all blocks are generated together so that due to random-like behaviour of chaotic map the neighbouring blocks will be operated by highly uncorrelated chaotic values. This ensures that even though there exist redundancy in the neighbouring blocks, but XOR operation with chaotic value in each round diffuses this redundancy completely. Further, to reduce the computational expense the number of rounds is decreased from 31 to 18. This is done while carefully balancing the efficiency and security aspects so that security is not compromised while reducing the rounds because Özen et al. [202] proposed related-key rectangle attack on original PRESENT with reduced rounds.

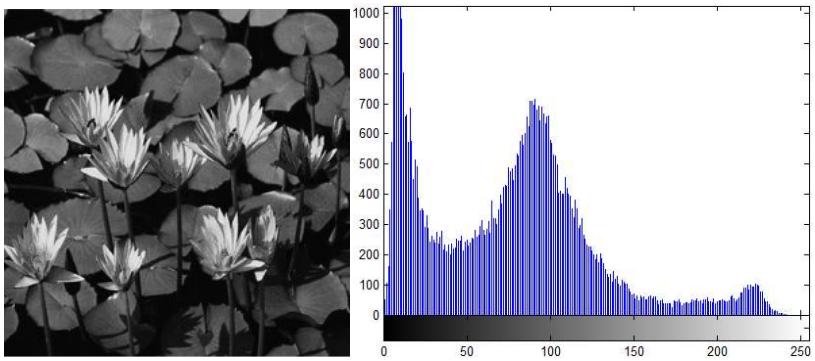
Results show that the above mentioned improvised block cipher has an increased key-space adding to its strength, with complete removal of redundancy in the cipher image and involves

minor increase in computational cost. As mentioned, chaos is added to enhance the security and the number of rounds is reduced to 18 to compensate on minor increase in computations. For still higher security applications the number of rounds may be varied as per the level of desired security. Thus, the proposed improvisation makes the block cipher suitable for multimedia applications, specially, visual content like images.

3.2.2 Observations of improvised PRESENT for Visual Content Security

This section demonstrates some of the experimental observations performed using MATLAB R2011a on machine with Windows 7 32-bit operating system with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM to show the strength and computational time efficiency of the proposed improvised block cipher based on PRESENT modified with use of chaos.

Fig. 13 displays the original 8-bit Grayscale Water Lilies Image (dimensions - 256×256), entropy value along with its histogram. In the Fig. 14, the corresponding image encrypted with original PRESENT block cipher, entropy value and its histogram, are displayed which show significant redundancies in the form of textured regions present in the cipher image. Fig. 15 displays the image encrypted with the improvised block cipher along with its entropy and histogram. It clearly shows higher entropy, no textured zones in the cipher image and a more uniform histogram, thereby demonstrating complete removal of redundancy in the cipher image generated using improvised PRESENT block cipher.



Entropy: 7.2171

Fig. 13 Original Grayscale Water Lilies Image with Histogram

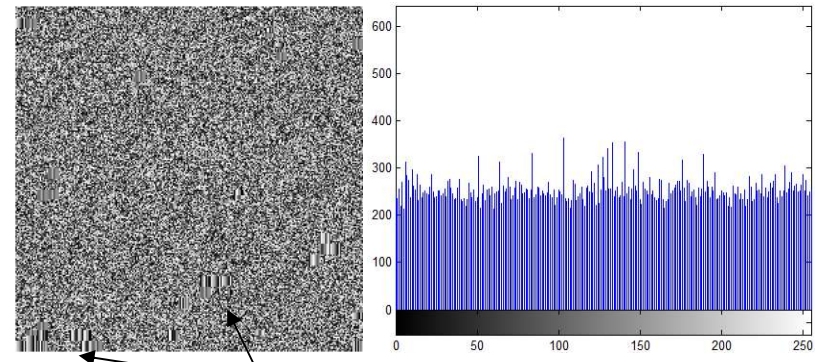


Fig. 14 PRESENT Encrypted Water Lilies Image with Histogram

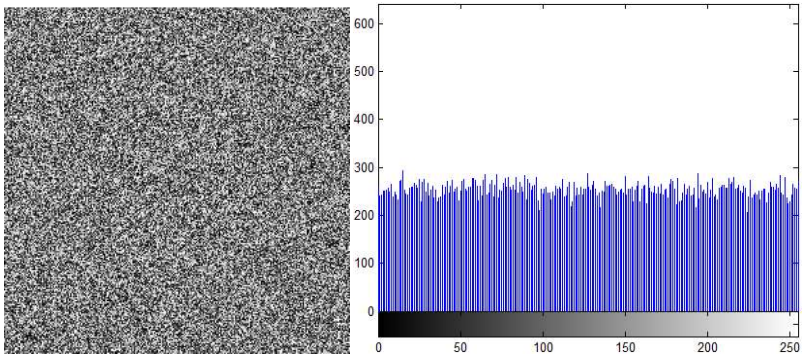


Fig. 15 Proposed Improvised Block Cipher Encrypted Water Lilies Image with Histogram

In another observation, the encrypted images were divided in 64 blocks each of size 32×32, and Fig. 16 demonstrates the uniformity in block-wise entropy achieved with the improvised cipher as compared to the results of the original PRESENT block cipher.

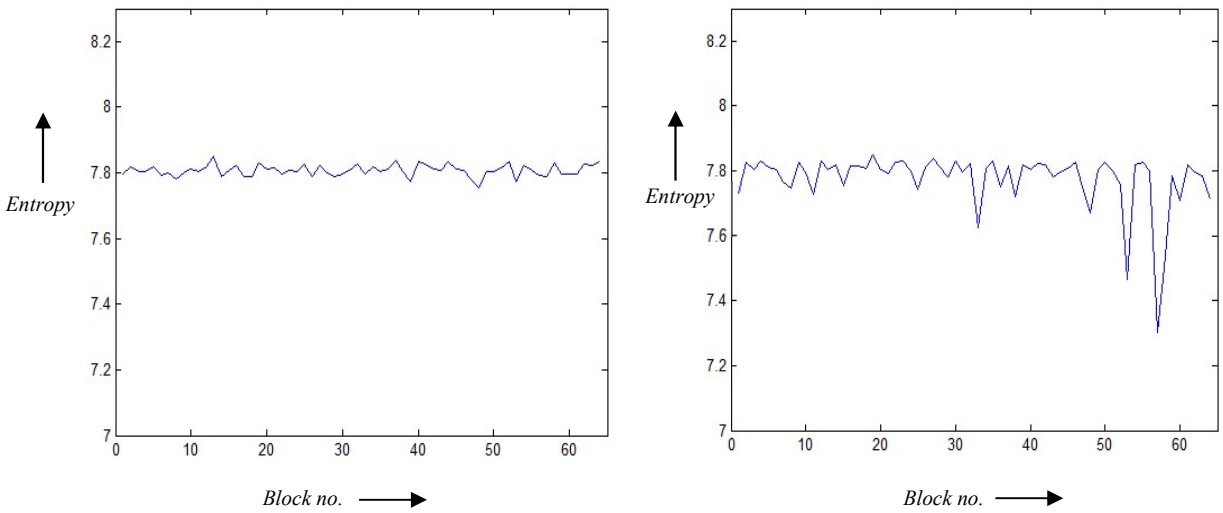


Fig. 16 Block-wise Entopy Plot of Encrypted Image (Water Lilies) with Proposed Improvised Block Cipher vs original PRESENT

Fig. 17 shows that the application of the proposed scheme on plain white image produces a nearly uniform histogram. This demonstrates complete diffusion of redundancy in the cipher image corresponding to plain image with single color value having single peaked histogram.

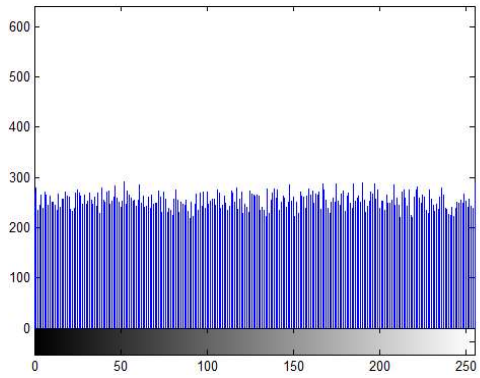


Fig. 17 Histogram of Plain White Image encrypted with Proposed Improvised Block Cipher

The observations to prove strength against differential attack with one bit change in the secret key or one bit change per pixel shows strong avalanche properties as shown in Fig. 18 &19 respectively.

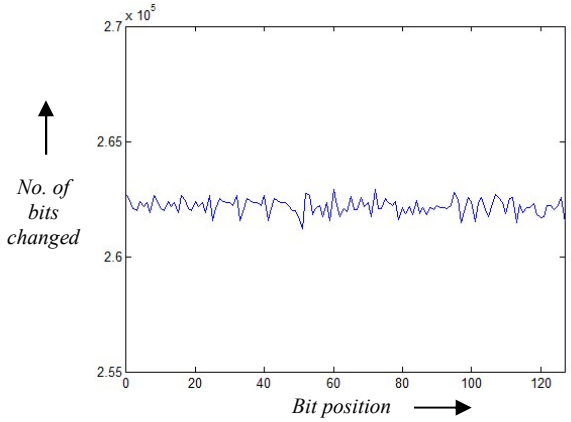


Fig. 18 Avalanche Property – Plot of number of bits changed in the Proposed Improvised Block Cipher Encrypted Image (Water Lilies) with one bit change at each position of the 128-bit key

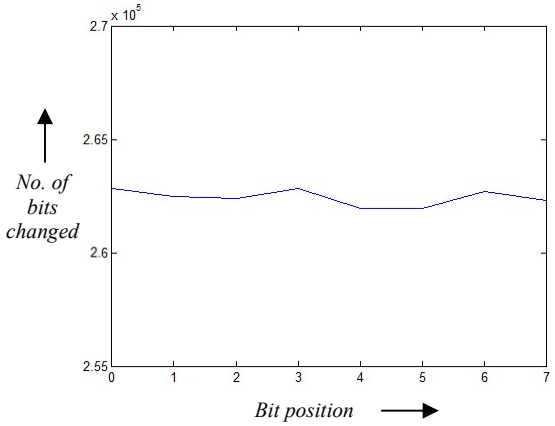


Fig. 19 Avalanche Property – Plot of number of bits changed in the Proposed Improvised Block Cipher Encrypted Image (Water Lilies) with one bit change per pixel at each of the 8 position

Further, to analyze the number of rounds impact on the efficiency and strength of the proposed improvisation, the observations of entropy and time for varying number of rounds are shown in Fig. 20 & 21.

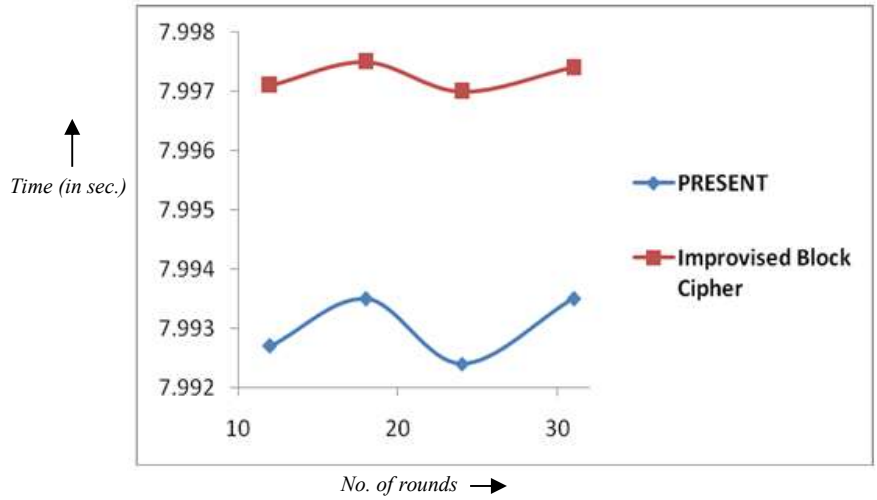


Fig. 20 Plot for comparision of Entropy Variation with change in number of Rounds for PRESENT vs Proposed Improvised Block Cipher

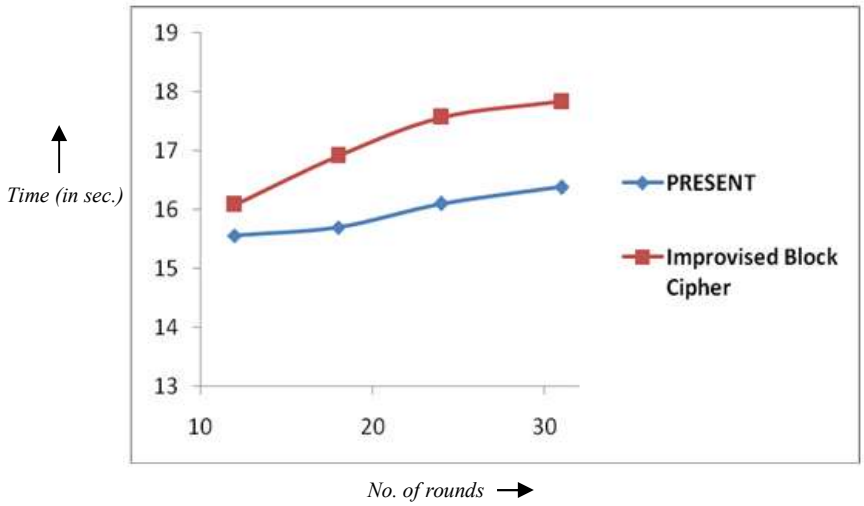


Fig. 21 Plot for comparision of Time Variation (in seconds) with change in number of Rounds for PRESENT vs Proposed Improvised Block Cipher

As evident from the observations, the improvised PRESENT block cipher proposed above, has an increased key-space adding to its strength, with complete removal of redundancy in the obtained cipher image and involves minor increase in computational cost. As mentioned, chaos is added to enhance the security and the number of rounds is reduced to 18 to compensate on minor increase in computations. Entropy stability over round variations apparently demonstrates that reducing the number of rounds does not affect the security. For still higher security applications the number of rounds may be varied as per the level of desired security.

Thus, the proposed improvisation makes the PRESENT block cipher suitable for visual content applications, of which images were chosen for observations in this paper but the idea is extendible to other forms as well.

3.3 Design of New Chaotic Primitives & their applications in customizing AES for Visual Content Security

Chaos basically appears to be noise to unauthorized users and chaotic sequences are highly sensitive to initial conditions and control parameters. Using these inherent properties of chaos, we have designed new chaos-based or chaotic primitives having applicability in designing cryptosystem for visual content security.

The proposed simple chaotic primitives involve cheaper operations and are used to achieve diffusion property in cost-effective way in the cryptosystems for visual information. The strength of the proposed chaotic primitives is observed by its application in traditional encryption scheme like AES [10] and the modified scheme is found to possess high security while encrypting images at lower computational expense.

As stated earlier, the AES scheme in its original form is not directly suitable for visual content like images because the computational cost of the operations involved do not make it practically suitable for such bulkier data, especially when redundancy in plaintext gets percolated in the ciphertext in the native ECB mode. The heaviest per-round operation in AES is identified to be Mix Columns operation. For customizing AES to suit applications for securing visual content this Mix Columns operation is replaced by the chaotic primitive. Two advantages are gained with this approach- firstly, since the introduced chaotic primitives are lighter hence the computational cost is significantly reduced and secondly as the primitive is key-dependent, hence, unlike standard AES now two operations per round are made key-dependent. This enhances the security and that also with lesser computational cost. Following figure Fig. 22 show the comparison between the standard AES and chaotic-primitive based customization.

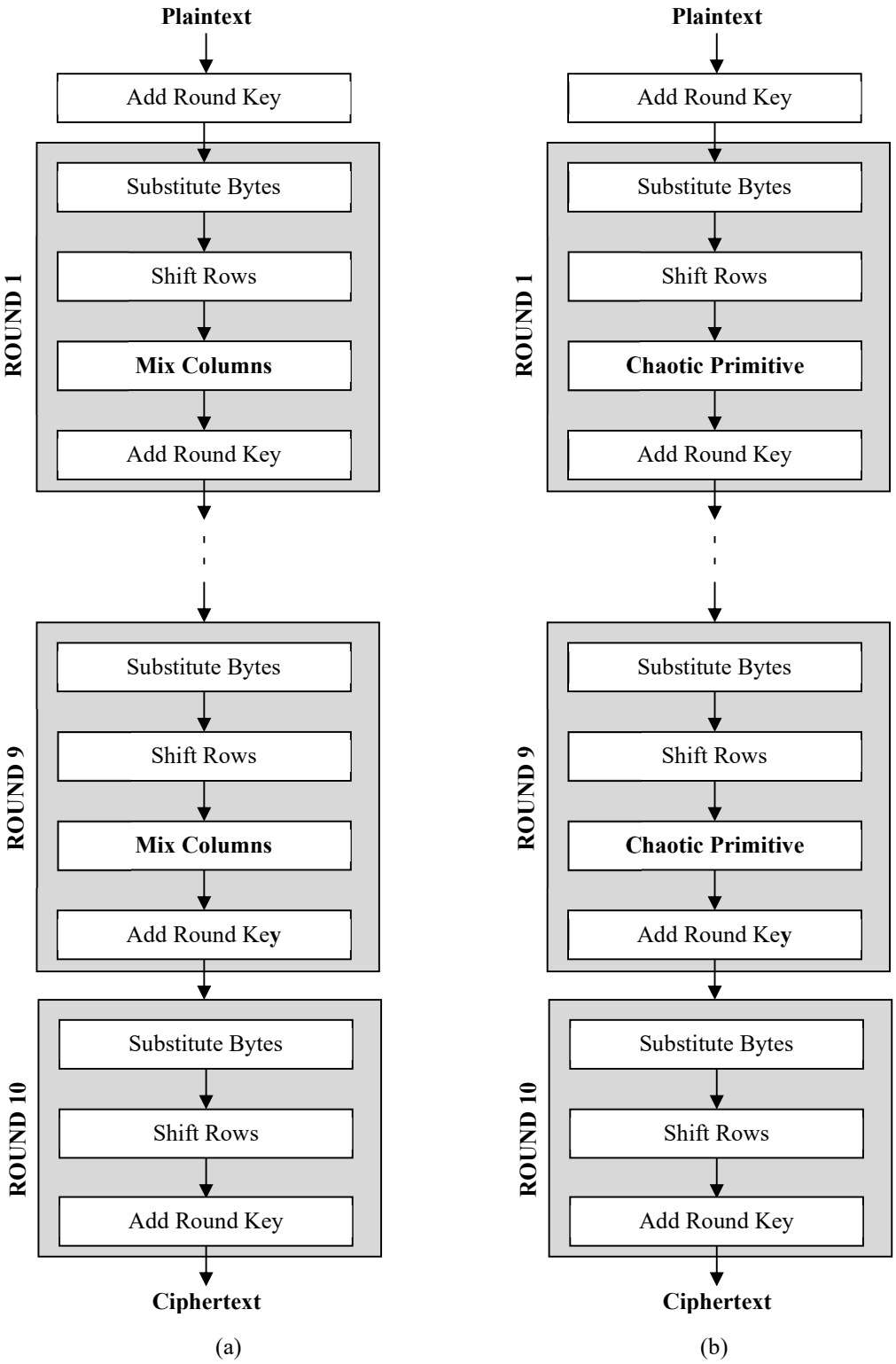


Fig. 22 (a) Standard AES Block Cipher (b) AES customized using chaotic-primitive

3.3.1 Chaotic Primitive 1

Two values at a time from discretized chaotic sequence are used to decide positions of two bytes from the plaintext, say pos1 and pos2. The higher and lower order nibbles of these two bytes are rearranged to create two new bytes say c and d:

$$c_1c_2c_3c_4c_5c_6c_7c_8 = a_5a_6a_7a_8\ b_1b_2b_3b_4$$
$$d_1d_2d_3d_4d_5d_6d_7d_8 = b_5b_6b_7b_8\ a_1a_2a_3a_4$$

c and d are placed at positions pos1 and pos2 respectively in cipher text. Clearly, the operation performed is very light while still providing strong permutation as well as diffusion properties when employed as part of per-round operation.

3.3.2 Chaotic Primitive 2

This primitive involves very simple and highly inexpensive operations and is thus suitable to be used as primitive for substitution and diffusion steps in cryptosystems for visual content security. It takes a chaos based discrete sequence of bytes as input along with the data bytes and generates an equally sized cipher text using the operations as described below:

```
for i = 0 to n-1
   C[i] = P[i] <<< (cs[i] % 8)
C[0] = C[0] ⊕ cs[0]
for i = 1 to n-1
   C[i] = C[i-1] ⊕ C[i] ⊕ (cs[i] % 8)
```

where P[i] : i^{th} byte of plaintext,
cs[i] : i^{th} byte of chaotic sequence,
C[i] : i^{th} byte of cipher,
n : total no. of bytes in plaintext,
<<< : left circular shift operation,
⊕ : XOR (Exclusive OR) operation

The use of above mentioned chaotic primitives for customization of AES proves to be more computationally efficient, provides complete diffusion of redundancies in cipher text and demonstrates strong avalanche properties as shown in the following sections.

3.3.3 Observations of customized AES with Chaotic Primitives

In this section we present the observations to demonstrate that customizing standard encryption schemes like AES using our proposed chaotic primitives makes it suitable for visual content security. To prove the strength of the proposed work, we performed security analysis and few observations taken on 256×256 grayscale images are given as under. The observations are taken using MATLAB R2011a on machine with Windows 7 32-bit operating system with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM. Fig. 23 shows Water Lilies image encrypted using standard AES algorithm with 10 rounds along with the histogram and entropy of the cipher image. As clearly visible, the cipher image contains textured zones which may be vulnerable to statistical or other cryptanalytic attacks.

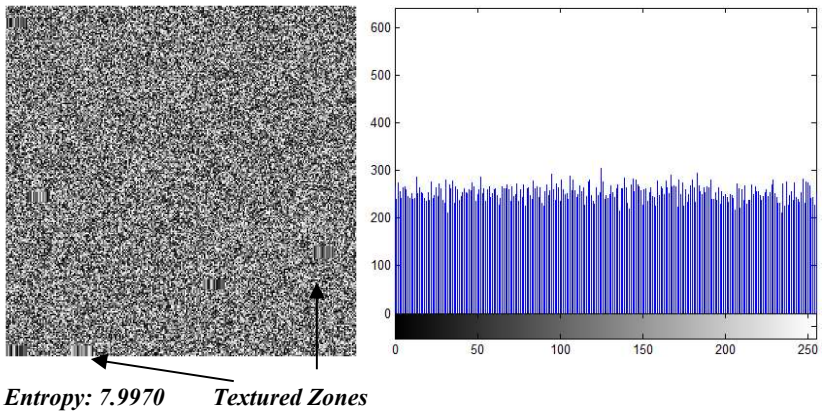
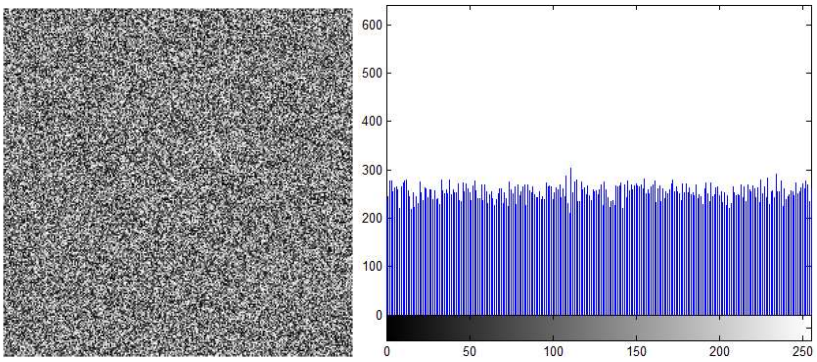


Fig. 23. AES Encrypted Water Lilies Image with Histogram

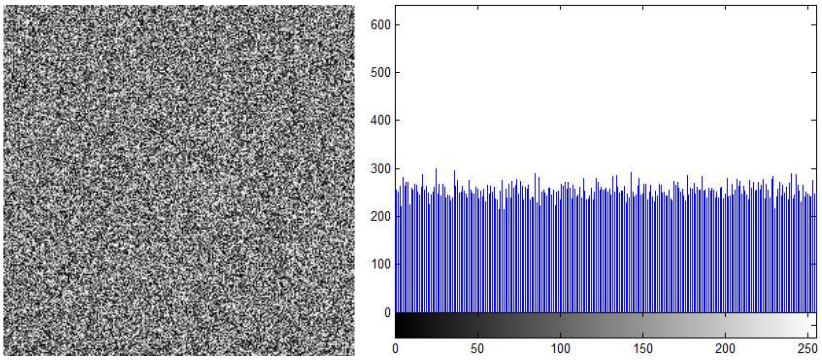
To study the impact of introduction of chaotic primitive 1 to AES scheme, we took observations using three simple and cost effective 1D chaotic maps. These include standard logistic map [26], an improvised logistic map [50] and Logistic-Tent map [50]. The parameter value used for the Logistic-tent map is 3.6 and that for the other two maps is 4. Further, the initial condition is made key-dependent to ensure that the chaotic primitives operation adds confusion to the overall scheme. Fig. 24 shows the encrypted Water Lilies image, histogram and entropy values obtained using customized AES with these three chaotic maps using chaotic primitive 1. As

can be seen, the encrypted images obtained using customized AES do not possess textured zones and hence are visibly not vulnerable.



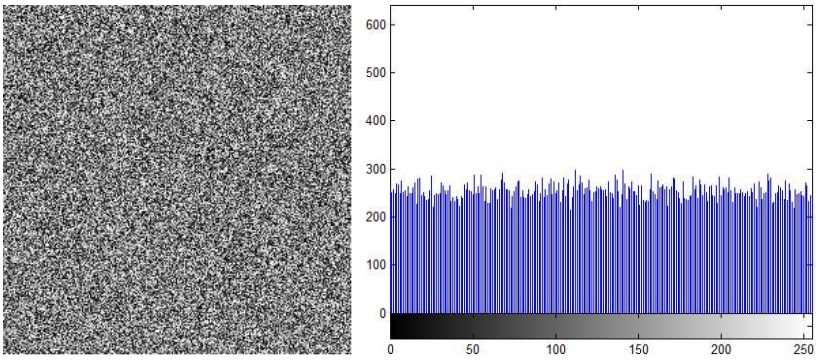
Entropy: 7.9974 No Textured Zones

(a)



Entropy: 7.9975 No Textured Zones

(b)



Entropy: 7.9971 No Textured Zones

(c)

Fig. 24 Proposed Customized AES (with chaotic primitive 1) Encrypted Water Lillies Image with Histogram (a) using logistic map (b) using improved logistic map (c) using logistic-tent map

To establish that all color intensities are randomly distributed across the entire encrypted image and no portion of the cipher image possesses special color distribution distinguishing it from the other, variation of entropy across the image is observed. For this, the image is treated to be

composed of 256 equal sized square blocks and block-wise entropy is plotted as shown in Fig. 25. The plot clearly shows that there is a much smoother or uniform variation of entropy among the different blocks of the cipher obtained using customized AES as compared to standard AES.

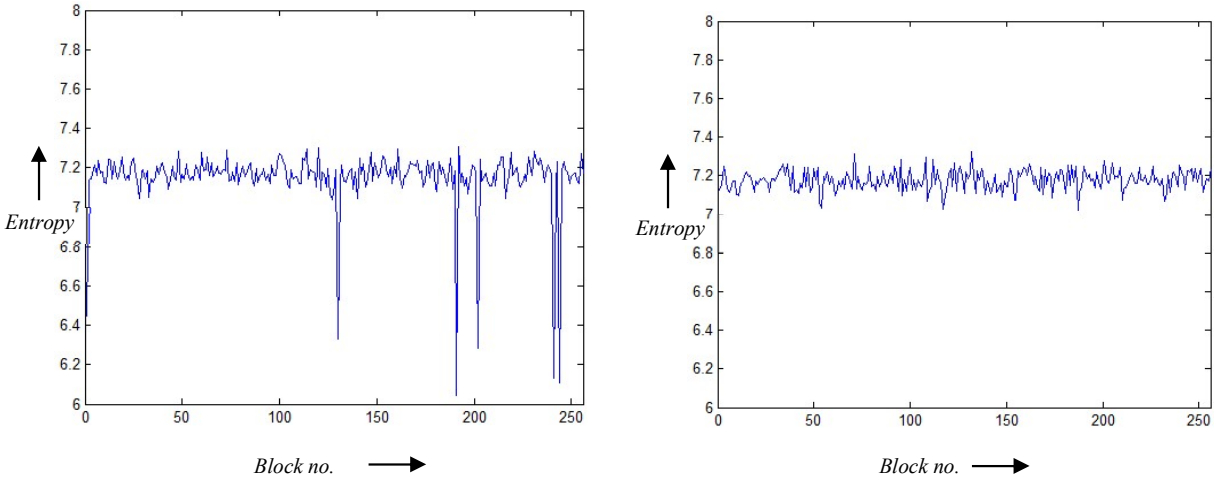


Fig. 25 Block-wise Entopy Plot of Encrypted Water Lilies Image with AES vs Proposed Customized AES (with chaotic primitive 1 using logistic map)

To show that there is complete removal of redundancy in the cipher, observation on plain white image is taken. The cipher image obtained demonstrates uniform distribution of the histogram as shown in Fig. 26 while the plain image contained all identical pixels.

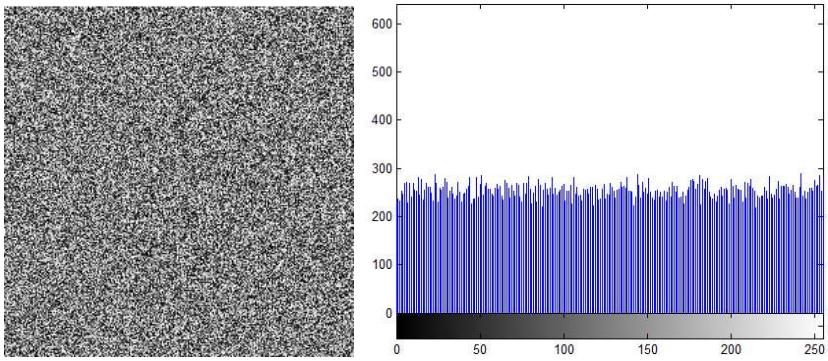


Fig. 26 Encrypted Image and Histogram of Plain White Image encrypted with Proposed Customized AES (with chaotic primitive 1 using logistic map)

Further, to demonstrate the computational efficacy of the customized cipher, time observations are taken which demonstrate that the use of chaotic primitive in place of a bulkier operation in the standard scheme reduces the overall cost to less than 15% of the original cost. The following

table, Table 1 displays the comparison performed on the same machine under identical conditions:

TABLE 1

COMPARISON OF COMPUTATIONAL COST ON ENCRYPTION OF WATER LILIES IMAGE

Encryption Scheme	Time (seconds)
AES	104.019
Customized AES (with chaotic primitive 1 using logistic map)	13.712
Customized AES (with chaotic primitive 1 using improved logistic map)	13.872
Customized AES (with chaotic primitive 1 using logistic-tent map)	13.962

The following observations show strong avalanche properties displayed by the proposed customized scheme. Fig. 27 shows that with a single bit change in the key the cipher image changes by around 50% and this change is persistent for change in any single bit of the key showing that all bits of the key contributes in cipher image generation. Fig. 28 demonstrates that for a single bit change per pixel, the cipher image again changes by approx. 50% irrespective of the bit position in the pixel.

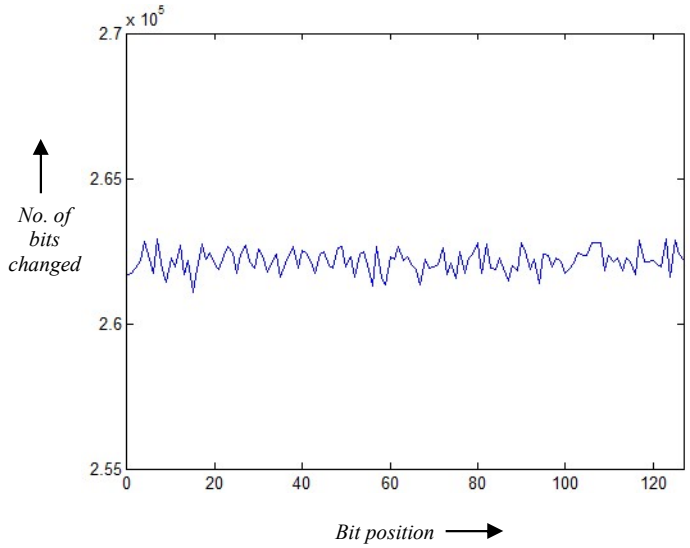


Fig. 27 Avalanche Property – Plot of number of bits changed in the customized AES Encrypted Water Lillies Image (with chaotic primitive 1 using improved logistic map) with one bit change at each position of the 128-bit key

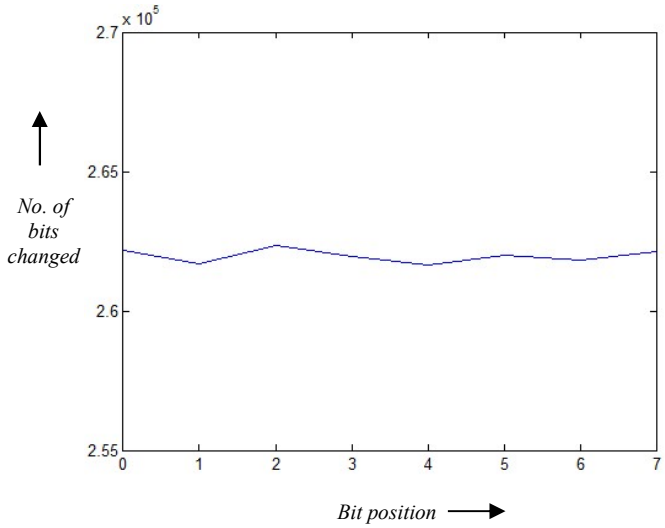
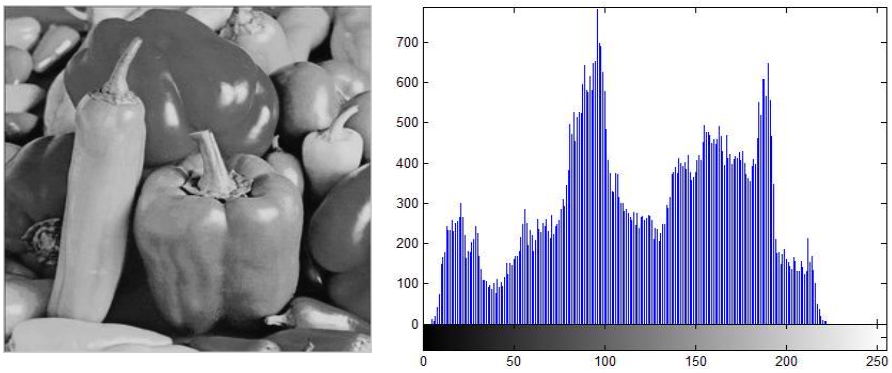


Fig. 28 Avalanche Property – Plot of number of bits changed in the customized AES Encrypted Water Lillies Image (with chaotic primitive 1 using logistic-tent map) with one bit change per pixel at each of the 8 position

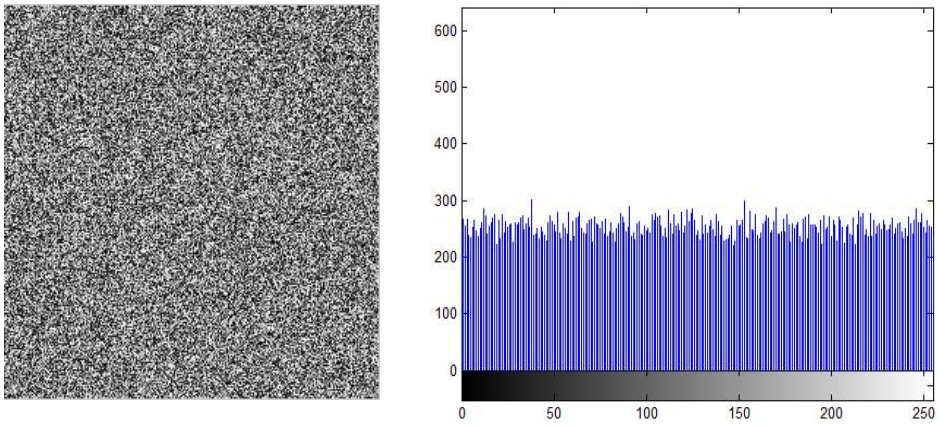
The results of experimental observations show that the proposed chaotic primitive 1 can be incorporated in cryptosystems to provide a cost-effective means for securing images and diffuse redundancies completely in the cipher image. The time observations show a sharp dip in the overall computational cost required to obtain the cipher image and the scheme still demonstrates strong avalanche properties and complete removal of textured zones. In fact, a completely uniform histogram is obtained even for plain white image demonstrating strength of this scheme.

Further, similar experimental observations were made to show the impact on strength and time efficiency of our proposal of chaotic primitive 2 using logistic map (with parameter value set as 4 and initial condition made dependent on the key), and its subsequent application to standard encryption scheme like AES. In the figure Fig. 29, the original grayscale Peppers image with its entropy and corresponding histogram is shown. We observe that our customization with chaotic primitive 2 maintains the strength of the scheme with complete removal of redundancy which is clearly visible from the corresponding encrypted image (with entropy & histogram) and block-wise entropy plot as shown in Fig. 30 & 31 respectively. Similar observations have been taken on several standard images which demonstrated consistent results.



Entropy:7.5543

Fig. 29 Original Grayscale Peppers Image with Histogram



Entropy: 7.9973 No Textured Zones

Fig. 30 Encrypted Peppers Image & Histogram (Customized AES with chaotic primitive 2 using logistic map)

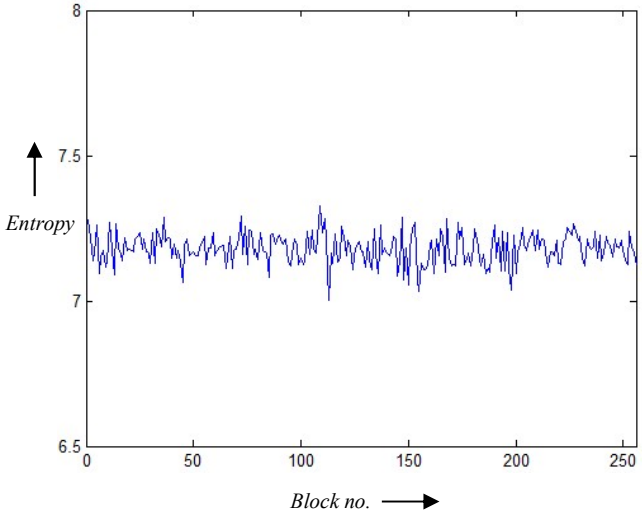


Fig. 31 Block-wise Entropy Variation in Customized AES Encrypted Peppers image (with chaotic primitive 2 using logistic map)

Also, the following table, Table 2 shows that there is a significant improvement in the computational efficiency. With our proposed customization to AES scheme with chaotic primitive 2 the cost has reduced to nearly $1/5^{th}$ of the original cost.

TABLE 2

COMPARISON OF COMPUTATIONAL COST

Image	AES (seconds)	Customized AES (with chaotic primitive 2) (seconds)
Peppers	95.956	19.344
Water Lilies	96.643	18.938
Baboon	95.956	18.985
Lena	96.237	19.063

Like in case of chaotic primitive 1, again the observations for customized AES with chaotic primitive 2 clearly reflect that the computational cost has been significantly reduced and entropy, histogram and block-wise entropy variation display no degradation in the overall strength of the scheme.

3.4 CONCLUDING REMARKS

This chapter proposed an approach for designing cryptosystems for visual content security like images by improvising or customizing standard encryption schemes, like AES and PRESENT in our study, using inexpensive chaotic operations and primitives. New chaos-based primitives suitable for substitution and diffusion have also been proposed and their implementation and experimental observations while customizing existing standard encryption scheme have been shown.

This approach of improvising or customizing standard encryption schemes to suit visual content requirements not only is cost effective but also adds a scope to increase confusion property of the customized scheme by way of introducing more key-dependent operations in the customized scheme. It further also adds a scope of increase in size of the key-space thereby enhancing the security of the overall scheme as is seen in our study of improvising PRESENT block cipher. But when customizing ultra-lightweight ciphers like PRESENT, very clearly, there exist a trade-off between security and efficiency, hence, due diligence will be required to ensure that an inclusion of chaotic-primitive/operation should not increase the computational cost significantly especially for low-security lightweight applications, while on the other hand, significant increase in computation may be acceptable for applications requiring high security.

For low-security lightweight applications, the use of ultra-lightweight schemes like PRESENT as the base algorithm with the additional security provided by the application of chaos, will ensure that while improving & keeping the security high, the overall cost of the chaotically customized scheme will still be lesser than using standard block ciphers like AES etc. to secure visual content.

Though observations have been taken on images but the work can easily be extended to other forms of visual content like videos. Hence, it is concluded that the proposed chaotic primitives can be utilized in encryption schemes for visual content security and also to customize standard ciphers by replacing their bulkier operations with the proposed chaotic primitive. In future, more such cost-efficient chaos-based primitives can be developed to be used as basic operations in encryption schemes for securing visual content.

CHAPTER 4

DESIGN OF DYNAMIC AND UNCONVENTIONAL ENCRYPTION SCHEMES FOR VISUAL CONTENT

In conventional block ciphers like AES, DES, IDEA etc. the algorithm remains fixed and it is the secret key that provides strength to the encryption process. Such block ciphers were largely built for securing textual information. At the first look, it appears that the conventional techniques, designed for securing text, should in principle be directly applicable on any form of data including visual content like images but, this does not hold true in practice. As discussed in the previous chapters, the reason is that visual content data like images, videos etc. have special characteristics, i.e. they are bulky in size and possess strong correlation among neighboring data bytes and these characteristics were missing in textual data. Hence, these characteristics do not get directly addressed in such conventional encryption schemes specially when they are used in native ECB mode. These ciphers are static in their operations and secrecy is provided only by the private key. They largely rely on the mathematical complexity of the applied computations and secrecy of the key. They are computationally expensive and their static behavior makes them susceptible to get broken, if not truly practically at least theoretically, when undergone significant analysis by the attacker [203]–[205]. Attacks are also proposed on AES family of cryptosystems even when used in, the otherwise considered secure, CTR mode [206]. The static operations in these block ciphers are predetermined irrespective of the key being used and such static designs are more susceptible to cryptanalytic attacks and add to vulnerabilities and weakness of the system. Also, now a days many applications require securing visual content like images in resource constrained environments like mobile phones [207]–[209] and in such applications traditional schemes like AES will prove to be computationally more expensive.

Further, Internet of Things (IoT) has given an altogether new dimension to security challenges required to be addressed in the emerging world of smart cities specially with respect to data which is not necessarily text-based and is magnanimous and requires to be processed in environments with adaptive needs. Images form one such type of data which forms significant

proportions of modern-day transmissions including data being generated by devices like mobile phones, IoT devices such as smart bells, surveillance devices, CCTVs etc. specifically when operating in environments requiring adaptability to dynamic changes in security requirements maintaining balance with resource availabilities.

Though, there are several encryption schemes which have been proposed for securing multimedia including images yet there has been no encryption standard till date designed to cater to the special needs of multimedia content. The fact that traditional static standard schemes are not being directly able to address security concerns for visual content like images and absence of any image encryption standard lead to the motivation for exploring dynamic encryption as a paradigm shift for encrypting images and later other forms of multimedia. The approach can definitely be extended later to cater to other forms of multimedia as well. Introducing dynamism as part of the design of the encryption scheme does not take away the deterministic nature that every cryptosystem must possess. Despite offering dynamism in structure of the encryption process based on the key and also on the plaintext, this work very well follows the Kerckhoff's principle according to which every cryptosystem should be secure even if everything else about it is publicly known except the secret key. Also, introduction of chaos-based dynamism can ensure that without using intricate mathematical operations, the dynamic framework could provide high security itself. Statistical and cryptanalytic attacks will intuitively become difficult when the encryption algorithm is dynamically changing with change in key and/or plaintext. This argument can be made stronger by highlighting that cryptanalytic attacks are normally designed by identifying some weak operation or loophole within the design of the static scheme and then the system is tried to be cracked by exploiting the identified loophole to extract partial or complete information about the plaintext or key or both [183], [185], [189], [191]. But identifying such loopholes in a dynamic cryptosystem will surely be much difficult as the adversary will not even be equipped with the complete knowledge of the structure of the cryptosystem itself, which, of course, will be dynamically changing. Thus, chosen/known plaintext attacks will not be possible on such encryption scheme involving dynamism.

Also, Probabilistic Encryption [124], [165] encourages dynamism in selecting possible encoding for the same message bits in the cipher text to make it tough for the adversary to attack. In probabilistic encryption, different cipher texts are produced at different times even when the same encryption scheme is applied with the same key to the same plaintext. As

already elaborated in Section 2.2.2 the conventional non-probabilistic encryption approach is vulnerable to revelation of complete or partial information about the plaintext by rigorous analysis of the cipher text. But with the probabilistic approach different encodings for same bit 0 or 1 of the plaintext is introduced to achieve the desired computational hardness.

In this chapter, the staticness in the design of the encryption algorithm, for securing visual content like images, is targeted to improve the overall security of the cryptosystem by means of including randomness using Probabilistic Encryption or by including key/plaintext-dependent dynamically decided operations etc. Three major untraditional schemes for encrypting visual content like images have been proposed which include:

a. Conditional encryption based three variants suitable for Image Encryption
b. A chaos-based Probabilistic Block Cipher for Image Encryption
c. A chaos-based Dynamic Framework for Image Encryption

4.1 CONDITIONAL ENCRYPTION BASED THREE VARIANTS SUITABLE FOR IMAGE ENCRYPTION

This work is an extension of a previously authored work [146] with the intent of customizing it to suit the requirements of visual content like images, increasing the security without significantly increasing the computational cost and keeping it in line with the basic conditional approach. Three variant schemes were developed keeping the conditional approach proposed in [146] as the base. Key-based S-Box rotation, S-Box generation and use of FAN transform (to permute pixel values) were used in these three variants.

The base block cipher based on conditional encryption [146] involves 8 rounds and uses 128-bit key to generate eight 128-bit round keys (one per round) and encrypts a block of 128 bits. Each round comprises of two phases i.e. key-based Readjustment Phase which conditionally changes partially or fully the plaintext and/or round key followed by Substitution & Shifting Phase. Fig. 32 shows the block diagram of the base block cipher based on conditional encryption.

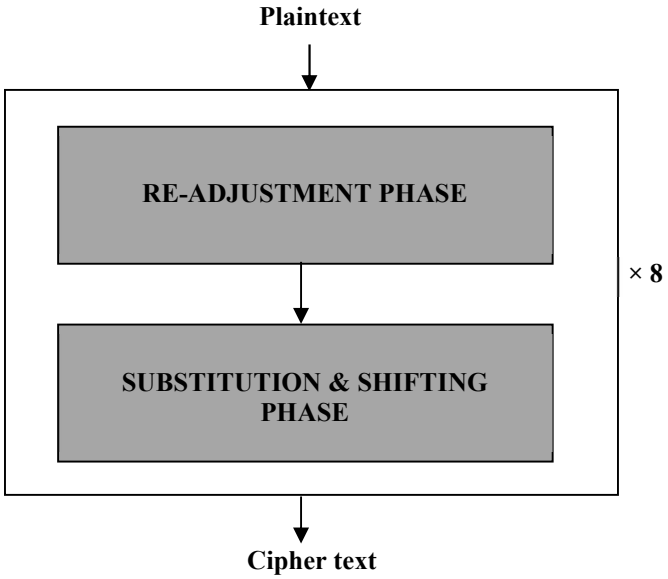


Fig. 32 Block diagram of base block cipher based on Conditional Encryption

Following are the details of the operations performed as part of this base algorithm. In this base scheme, the 128-bit key is used to generate 8 round keys, one for each round. The notations rk[i], P[i], C[i] denote the i^{th} byte of the round key, plaintext and cipher text respectively. The operators ⊕, <<, >>, %, & denote XOR, left-circular shift, right-circular shift and modulo operations respectively. Also 'q' represents the number of non-zero bytes (of round key) with even parity and 'r' represents the parity of 128-bit round key.

a) Re-adjustment Phase: This is the first phase per round in the overall encryption process. It re-arranges and/or negates part or all bits of the plaintext and/or the round key. The intent of this phase is to perform minor operations on the plaintext and round key based on the conditional approach where the decision of the operations performed is based on the parity of the round key and the number of non-zero even parity bytes in the round key.

ALGORITHM 1: Re-adjustment Phase of Base Conditional Encryption Scheme

INPUT: P (128-bit plaintext), rk (128-bit round key), q (the number of non-zero bytes of round key with even parity), r (parity of 128-bit round key)

1: **if** (r is even)
2: **if** (q%2 == 0)
3: swap the two 64-bit halves of rk
4: negate the I^{st} half (first 64-bits) of P
5: **end if**

```
6:   else
7:    if (q%2 == 0)
8:       negate all 128-bits of P
9:       swap the two 64-bit halves of P
10:   else
11:      negate I^st 64 bits of rk
12:      negate last 64 bits of P
13:      swap the two 64-bit halves of P
14:   end if
15:end if
```

b) Encryption: The encryption process involves 8 rounds and each round begins with the readjustment phase as described above, followed by substitution using AES S-Box. This is further followed by conditional bitwise shifting and XOR operations on the readjusted plaintext to generate the cipher text.

ALGORITHM 2: Per-round operations of Base Conditional Encryption Scheme

INPUT:P (128-bit plaintext), rk (128-bit round key), q (the number of non-zero bytes of round key with even parity), r (parity of 128-bit round key)

```
1: I = Re_adjustment_Phase(P, rk, q, r)
2:C = AES_SBox_based_Substitution(I)
3: bytes_XOR = 0
4:  for i = 0 to 15
5:      bytes_XOR = bytes_XOR ⊕ rk[i]
6:  end for
4: if (bytes_XOR % 2 ==0)
5:  for i = 0 to 15
6:    C[i] = C[i] << (rk[i] % 8)
7:    end for
8:  else
9:   for i = 0 to 15
10:  C[i] = C[i] << (rk[15-i] % 8)
11:   end for
12:end if
13:C[0] = C[0] ⊕ rk[0]
```

14: **for** i = 1 to 15
15: C[i] = C[i-1] ⊕ C[i] ⊕ rk[i]
16: **end for**

The base conditional encryption scheme described above is built on computationally less expensive fundamental operations like shifting, XORing, substitution and negation. With block size of 128 bits it showed impressive results for textual data but is not found suitable when applied directly to multimedia due its fixed block size. In this thesis, we propose three variants of the described scheme having customizable block size, maintaining low operational cost, addressing the issue of redundancy in the plaintext, and therefore making them suitable for multimedia applications especially visual content like images. In all the three proposed variants, position of the pixels has been brought out as a parameter so as to overcome the redundancies present in the plain image. The variants maintain the key size of 128-bits and as the block size is customizable so the entire image can be encrypted in one go or in parts as per the application's security requirements. As mentioned, to bring pixel position as one of the parameters determining the cipher image, the intermediate cipher image pixels are XORed with the respective pixel positions in all the variants. We now present the three proposed variants in details where we let 'n' be the customizable block size (in bytes).

4.1.1 First Variant

This variant (Variant 1) introduces conditional left or right rotation of the AES SBox [154] before performing the substitution as per the base algorithm. The round key dependent **sBoxRoundConstant** determines the number of rotations of the SBox. Also, the intermediate cipher image is parameterized as per the pixel positions by introduction of XORing operation with the pixel positions. Following represent the details of the re-adjustment phase of the proposed First Variant based on conditional encryption.

ALGORITHM 3: Re-adjustment Phase of First Variant

INPUT: P (n-bit plaintext), rk (128-bit round key), q (the number of non-zero bytes of round key with even parity), r (parity of 128-bit round key)

1: **if** (r is even)
2: **if** (q%2 == 0)
3: swap the two 64-bit halves of rk
4: negate the Ist (n/2)-bits half of P
5: sBoxRotationDirection = "left"

6: **else**
7: sBoxRotationDirection = “right”
8: **end if**
9: **else**
10: **if** (q%2 == 0)
11: negate all n bits of P
12: swap the two (n/2)-bit halves of P
13: sBoxRotationDirection = “left”
14: **else**
15: negate Ist 64 bits of rk
16: negate last n/2 bits of P
17: swap the two halves of P
18: sBoxRotationDirection = “right”
19: **end if**
20: **end if**

Each round of the encryption process in the First Variant starts with the readjustment phase which besides readjusting the plaintext and/or round key as per the base algorithm, in this variant, also determines the sBoxRotationDirection for subsequent SBox rotation for the substitution operation. The sBoxRotationConstvalue is also determined by performing XOR on the 16 round key bytes. Further, after the readjustment phase the substitution based on the key based rotated SBox is performed. Here, the AES SBox is rotated as per the generated sBoxRotationDirection and sBoxRotationConst. The intermediate cipher bytes are then XORed with their respective positions in the image, and finally the shift and XOR operations are applied to yield the cipher. Following represents the per-round operations of the proposed First Variant based on conditional encryption where besides the other operators, & is used to denote bitwise-AND operation.

ALGORITHM 4: Per-round operations of First Variant

INPUT: P (n-bit plaintext), rk (128-bit round key), q (the number of non-zero bytes of round key with even parity), r (parity of 128-bit round key)

1: (I, sBoxRotationDirection) = Re_adjustment_Phase(P, rk, q, r)
2: sBoxRotationConst = 0
3: **for** i = 0 to 15
4: sBoxRotationConst= sBoxRotationConst $\oplus$ rk[i]
5: **end for**

```
6: C = AES_SBox_based_Substitution(I, sBoxRotationConst, sBoxRotationDirection)
7: bytes_XOR = 0
8:  for i = 0 to 15
9:      bytes_XOR = bytes_XOR ⊕ rk[i]
10:end for
11: for i = 0 to n-1
12:    C[i] = C[i] ⊕ (i & 0xFF)
13: end for
14: if (bytes_XOR% 2 ==0)
15:    for i = 0 to n-1
16:      C[i] = C[i] << (rk[i%16] % 8)
17:    end for
18:  else
19:   for i = 0 to n-1
20:        C[i] = C[i] << (rk[15-(i%16)] % 8)
21:    end for
22: end if
23: C[0] = C[0] ⊕ rk[0]
24: for i = 1 to n-1
25:    C[i] = C[i-1] ⊕ C[i] ⊕ rk[i%16]
26: end for
```

4.1.2 Second Variant

The second variant involves generation of key-based SBox [155] for substitution instead of performing conditional left or right rotation of the AES SBox as done in first variant. Also, unlike first variant, there is no change in the Re-adjustment Phase as compared to the base algorithm.

The strength of this variant (Variant 2) lies in the key-based SBox generation. And to ensure that the pixel position determines the cipher output, as in first variant here again, the intermediate cipher bytes are XORed with the respective pixel positions.

The second variant is an improvement over the first variant in terms of efficiency. The first variant involved key-based conditional left or right rotation of the AES SBox in each round thereby involving higher computation, while this variant generates key-based SBox once for all the rounds thereby making it even lighter.

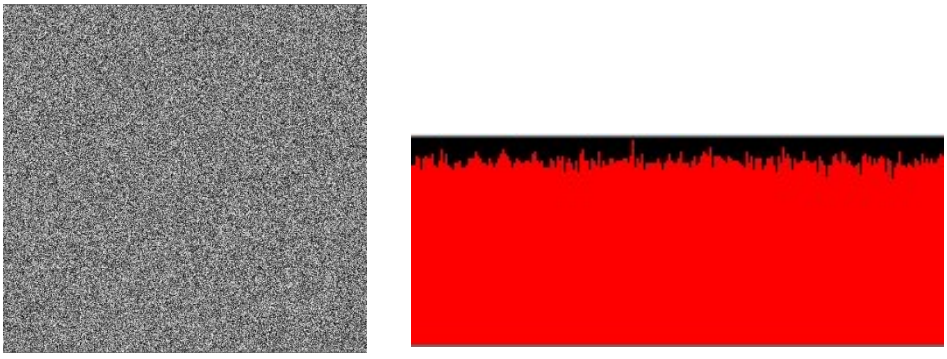
4.1.3 Third Variant

This variant (Variant 3) is an extension of the second variant so as to increase the strength of the encryption process. FAN transform [210], [211] based scrambling of the image is included as the pre-processing step adding another layer of security to this variant thereby enhancing its strength.

FAN transform provides a one to one mapping for carrying out transposition of the image pixels from one location to the other. Application of several iteration of the FAN transform reduces correlation among the neighbouring pixels and converts the image to incomprehensible form. After the application of FAN transform, the scrambled image is made to undergo key-based generated SBox substitution followed by the XOR and shifting operations as done in second variant.

4.1.4 Observations & Security Analysis of Conditional Encryption based three variants suitable for Image encryption

The three variants based on conditional encryption are implemented using Java on machine with Windows 7 32-bit operating system with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM. The strength of the three variants is demonstrated using a number of observations taken on 512×512 sized 8-bit grayscale images, however, the schemes can be extended to other color planes without any modification. Fig. 33 shows encrypted Peppers image (Variant 1), entropy and its histogram. The encrypted image does not contain any textured zones indicating that the redundancies in the original image are not propagated in the encrypted counter-part. The histogram of the cipher image is found to be smoothly distributed and the variation in entropy across the cipher image is also nearly uniform.



Entropy: 7.999

Fig. 33 Encrypted Peppers Image with Histogram

Fig. 34 represents the block-wise entropy of the encrypted peppers image (Variant 1) observed by dividing the image into 64 equal blocks of size 64×64. Observations taken with Variant 2 and Variant 3 also show similar results with complete removal of redundancies after encryption, smooth histograms and uniform block-wise entropy across the cipher image.

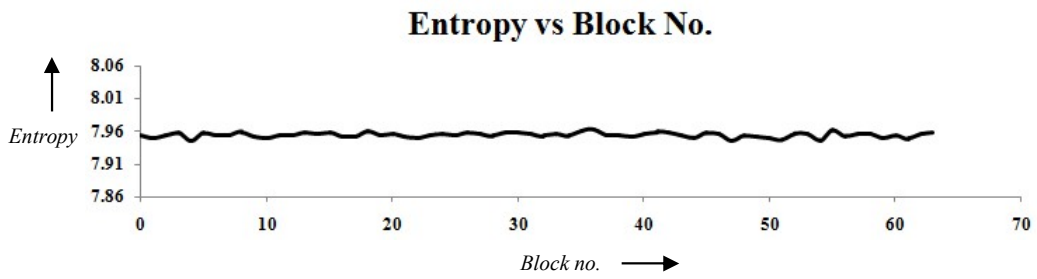


Fig. 34 Blockwise Entropy Plot of Encrypted Peppers Image (Variant 1)

Further, the avalanche properties for the three variants are also studied by observing:

i) Number of bits changed in the cipher with one bit changed per pixel.
ii) Number of bits changed in the cipher with one bit change in the key.
iii) Number of bits changed in the decrypted image when decrypted using a key having one bit changed as compared to the original key used while encryption.

The graphs for all the above set of observations show variation within the acceptable range, and average of around 50% change of bits in all the above scenarios, thereby indicating strong avalanche properties. Fig. 35, 36 & 37 shows some of the avalanche observations for the three variants.

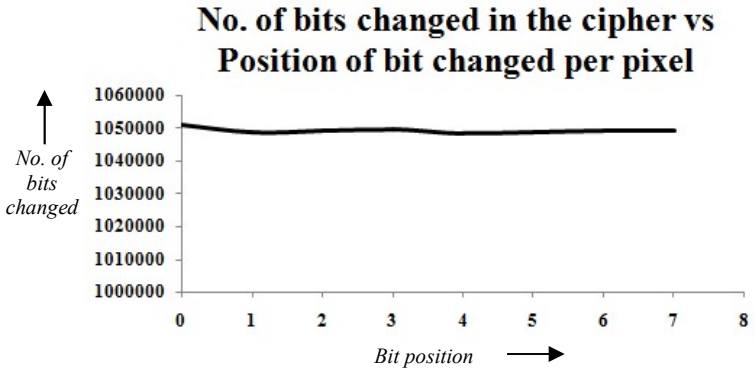


Fig. 35 Number of bits changed in the cipher with one bit changed per pixel (Peppers Image, Variant 1)

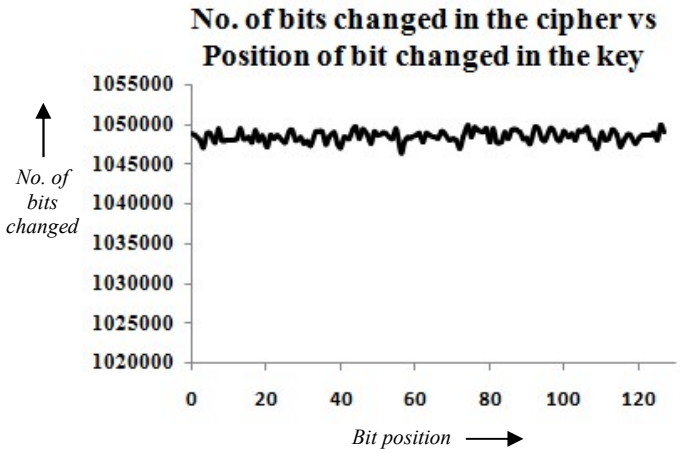


Fig. 36 Number of bits changed in the cipher with one bit change in the key (Peppers Image, Variant 2)

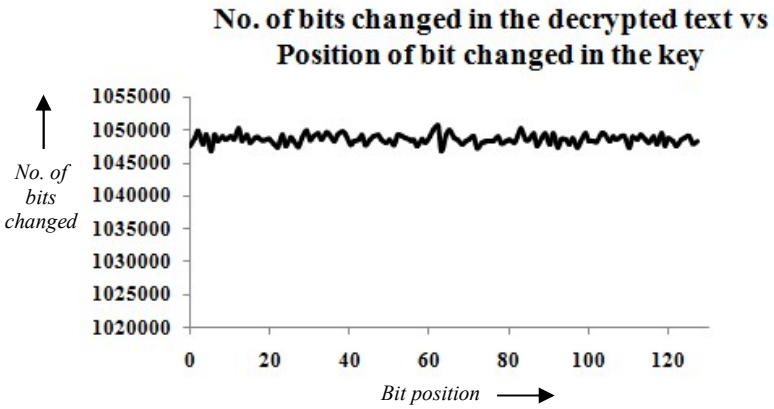
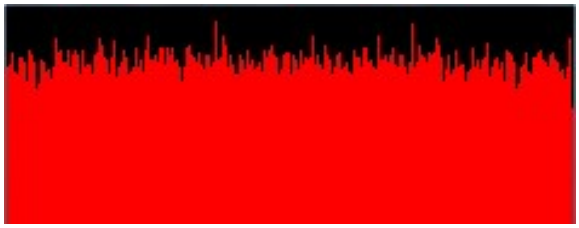


Fig. 37 Number of bits changed in the decrypted cipher with one bit changed while decryption (Peppers Image, Variant 3)

Also, similar set of observations were taken on plain white image and the results were identical. Fig. 38 & 39 shows the histogram and plot of numbers of bits changed in cipher with one bit change in key respectively, obtained with Variant 2 for plain white image. These observations show complete removal of redundancy in cipher and strong avalanche property possessed by the scheme even when the input plain image had 100% redundancy.



Entropy: 7.995

Fig. 38 Histogram & Entropy of Encrypted White Image (Variant 2)

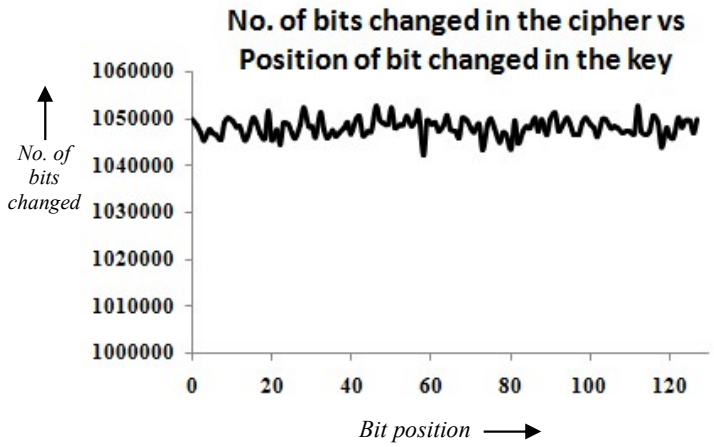


Fig. 39 Number of bits changed in the cipher with one bit change in the key (White Image, Variant 2)

In addition to the above, the NPCR, UACI were taken for the three variants on Peppers and Plain White Image. The NPCR, UACI observations are specified in Table 3 as under:

TABLE 3

NPCR, UACI FOR ENCRYPTED PEPPERS & PLAIN WHITE IMAGE

Variant	Image	NPCR	UACI
1	Peppers	0.99599	0.33522
	White	0.99545	0.33601
2	Peppers	0.99610	0.33500
	White	0.99597	0.33565
3	Peppers	0.99620	0.33451

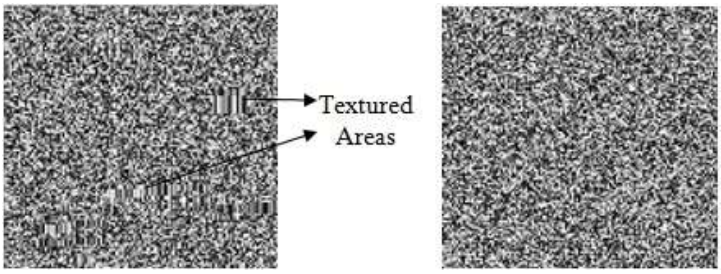
Also, correlation coefficient values are also evaluated between the original Peppers image and the corresponding cipher image obtained using the three variants to indicate the relationship between the original image and the encrypted one as shown in Table 4. Clearly, as the values are very close to zero hence it shows that the original image and the cipher image obtained after applying the three variants are not co-related.

TABLE 4

CORRELATION COEFFICIENT FOR ENCRYPTED PEPPERS

Variant	Correlation Coefficient
1	- 0.001894
2	- 0.000991
3	- 0.000683

As the high-level structure of the proposed schemes is similar to that of AES, involving multiple rounds with each round constituting transposition and non-linear substitution operations with an additional conditional approach, thus a comparative study with the standard AES algorithm is also done. It shows that the cipher generated using AES in ECB mode contains significant redundancies while the same are completely removed in the ciphers generated with the proposed schemes. Fig. 40 shows a magnified section of the ciphers generated using AES (containing textured areas) and proposed scheme (Variant 2) for Peppers image (redundancies completely removed).



Encryption using AES **Encryption using proposed scheme(Variant 2)**

Fig. 40 Comparison of Encryption using AES and proposed scheme

Further AES in CBC mode is not a feasible option as it involves a significant increase in the computation for bulky multimedia content and also recovering and decrypting back the plaintext becomes difficult in case of packet loss on the network.

In addition to the above, time observations show that Variant 1 takes around 40% less time and Variant 2 takes around 50% less time as compared to AES thereby highlighting the computational efficiency of these schemes.

4.2 A CHAOS-BASED DYNAMIC FRAMEWORK FOR IMAGE ENCRYPTION

As stated earlier, with the frequent advancement in the area of Internet of Things (IoT) and machine to machine communication the requirement of securing all forms of data including visual content, like images, has increased manifolds [212]–[215]. With the concept of smart cities becoming reality, intelligent IoT devices are required to securely communicate visual content like images with each other for various applications including surveillance, medical imaging, expert systems etc. Also, when it comes to communications of visual content including those by IoT devices, some applications have high security requirements while for

others efficiency may be a more significant factor and hence, practically such devices are operating in environments with varying/dynamically changing security requirements as per the application and resource constraints at hand. Therefore, there is a need for encryption schemes which are adaptable based on the changes in the operating environment and changing security needs. Also, this idea of adaptability of encryption scheme is well aligned and will be well utilized with the dynamic AI capabilities supported in the upcoming 5G technology for modern day communications.

Therefore, in another work, a multiple-round, adaptive and dynamic framework for image encryption is proposed which is deterministic and mainly uses chaos to achieve random-like key- and plaintext-dependent dynamism thereby making it practically impossible to design chosen/known-plaintext and differential attacks.

New dimensions to dynamism have been proposed in this work, which are not employed in the existing works including that the number of operations performed per round of the encryption scheme be decided dynamically. Also, the sequence of encrypting pixels will also be dynamically decided. This is incorporated along with dynamic decision on the type of operations performed. This kind of multi-level dynamism has not been used in existing literature and it will ensure that structure of each round of operations dynamically changes in an unpredictable way for the adversary. This is done with an objective to increase the level of difficulty manifolds for an adversary to perform cryptanalysis to break the cryptosystem. In absence of knowledge of the key, the attacker will be completely unaware about the number and nature of operations performed in the different rounds thereby averting cryptanalytic attacks.

Also, due to dynamically changing non-sequential access of pixel positions during encryption process the type and number of per-round operations performed on the same pixel position will vary if the same key is applied with a slightly modified image. Hence, proposed work will offer resistance against known/chosen plaintext, differential and impossible differential attacks. Further, chaos has been made integral part of the framework to ensure high level of randomness in dynamism with less computational expense. Thus, the overall dynamism of the framework makes it difficult for the attacker to guess the structure and operations of the encryption process to perform cryptanalysis.

4.2.1 Description of the proposed Chaos-based Dynamic Framework

In this proposed dynamic framework, chaos has been primarily used to introduce random-like dynamism in the overall structure of the proposed framework. Each pixel is visualized to be composed of three parameters i.e. (x, y, color byte) and, as part of the encryption process, a new color byte value is to be generated for each pixel. To ensure complete removal of redundancy existing in the plaintext, besides these three parameters, each pixel is assigned a key-based *'chaotic value',* where $0 < chaotic\_value < 256$. Hence, for encryption, each pixel has an additional parameter which is used in calculating pixel's counterpart in the cipher image. The encryption process uses operation look-up tables from which operations are selected dynamically to encrypt the pixels. The framework has three key features as stated below:

i) The framework offers chaos-based dynamism at multiple levels during the encryption process.

ii) Non-sequential data byte encryption is proposed, to achieve faster diffusion results and to resist known/chosen plaintext, differential and impossible differential attacks.

iii) The framework is also flexible and adaptive. The key sizes, the number and nature of operations in look-up tables, the minimum/maximum number of operations per round and number of rounds can be adjusted as per need so as to strike a balance between resource constraints and the security requirements.

As per the proposed framework, the different levels at which dynamism may be introduced using chaos include:

i) Dynamism in choosing the number of operations performed per round.

ii) Dynamism in choosing look-up table of operations.

iii) Dynamism in selecting the operation from the chosen look-up table.

iv) Dynamism in deciding sequence in which pixels are encrypted.

Clearly, new levels of dynamism have been introduced in this proposal, i.e., dynamic decision of number of operations performed per-pixel in different rounds and dynamic decision of the sequence in which pixels are encrypted. Very importantly, these decisions are made using chaos as it provides an easy means to achieve random-like dynamism with less computation. To elaborate, the additional *chaotic value* adds dynamism to the encryption operations applied

as it can act as one of the deciding factors, along with pixel coordinates, for determining the look-up table and further from within this look-up table, an operation, to be operated on the pixel, is selected dynamically using chaos. Further, the proposal is to encrypt pixels in dynamically chosen non-sequential fashion, where the coordinates of the pixel to be encrypted is determined using chaos and previously encrypted pixel. Chaos is used to determine its x-coordinate while the y coordinate is calculated based on the value of the previous encrypted pixel value. For the first pixel y-coordinate value is initialized to 0. In case the pixel at the generated pixel coordinates (x,y) is already encrypted in the current round of encryption process then the sequentially next pixel is chosen to be encrypted in its place. This way all the pixels get operated on in each round of encryption.

Clearly, the encryption of pixel bytes is not sequential and also the number and kind of operations operated on pixel values during multiple-round encryption process is also not fixed. Further, all this is decided with random-like dynamism using chaos, hence, there exists a large number of possible operation paths through which a plaintext pixel may pass before it gets transformed into corresponding cipher image pixel. As a result, even for the same key with a slightly modified image, the same pixel position gets operated upon by drastically different number and kind of operations. Thus, the proposed dynamic framework will offer high resistance against known/chosen plaintext, differential and impossible differential attacks.

4.2.2 Description of per-round operations in the proposed Chaos-based Dynamic Framework

Unlike conventional algorithms where the operations made per-round are fixed and are same in each round, the proposed work provides a fixed basic framework for each round with flexibility to accommodate different number of different kinds of operations per round i.e. the number, type and sequence of operations performed per round varies across different rounds even for the same pixel. Besides the dynamically decided operations used to achieve confusion, a diffusion step is performed at the end of each round which diffuses the two halves of the intermediate cipher text in one another. This along with non-sequential byte encryption ensures that minutest change in anywhere in the plain image gets diffused throughout the cipher image in subsequent rounds of the algorithm.

Following algorithm represents the per-round encryption rules as per the proposed framework:

ALGORITHM 5: Per-round encryption in proposed Dynamic Frameworks

```
INPUT: I (image), M (height of the image), N (width of the image)
op_count = generate_chaos_based_per_round_op_count( );
for i = 1 to M*N
    (x, chaotic_value) = generate_chaos_based_dynamic_values( );
    y = (x * previous_encrypted_pixel) % N;
    if (is_pixel_encrypted(x,y))
        (x,y) = find_next_unencrypted_pixel_position(x,y);
    end if
    (op_table, op) = choose_op_table_and_op (x,y, chaotic_value);
    j = 1;
    C(x,y) = I(x,y);
    while (j ≤ op_count)
        C(x,y) = C(x,y) op chaotic_value;
    end while
    previous_encrypted_pixel = C(x,y);
end for
C = diffusion_stage(C);
```

where,

*, % refers to the multiplication and modulus operation respectively,

op_table is the dynamically selected look-up table of operations chosen based on the pixel coordinates (x,y) and chaotic_value,

op_count is the number of operations performed (min<=op_count<=max), where min and max offers flexible limits to the number of operations performed per round

op is a dynamically selected operation from the look-up table *op_table.*

The following figure, Fig. 41 shows the per-round block diagram of the proposed dynamic encryption framework.

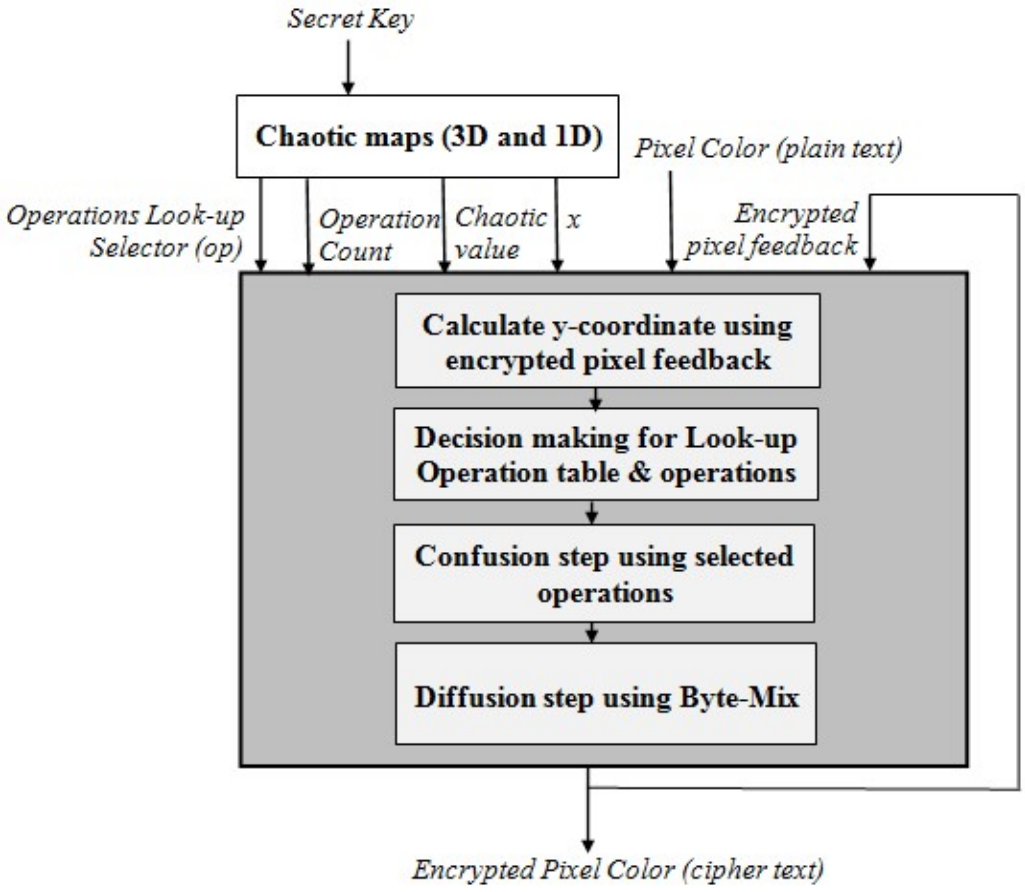


Fig. 41 Per-round block diagram for the Proposed Dynamic Encryption Framework

4.2.3 Definition of Diffusion Stage in the proposed Chaos-based Dynamic Framework

In the diffusion stage the image is treated in two equal-halves (divided horizontally) and the corresponding pixel bytes of the two halves say a and b are then mixed to generate two new pixel bytes a' and b' for substitution in place of a and b respectively. The following represents generation of a' and b':

$$a = a_1a_2a_3a_4\ a_5a_6a_7a_8$$

$$b = b_1b_2b_3b_4b_5b_6b_7b_8$$

$$a' = a_5a_6a_7a_8\ b_1b_2b_3b_4$$

$$b' = b_5b_6b_7b_8\ a_1a_2a_3a_4$$

For observation purpose, in the current implementation of the proposed framework, we choose to incorporate dynamism at three levels i.e.

i) dynamism in the number of operations performed per round, and

ii) dynamism in selection of the operations.

iii) dynamism in deciding order in which pixels are encrypted.

We have restricted use of a single look-up table containing the operations {<<, ⊕, negation, XNOR, >>}, where ⊕, <<, >> represent bitwise XOR, left-circular shift, right-circular shift operation respectively.

The choice of *chaotic_value*, *op_count* and *x*-coordinate value are made key-dependent by using a 3D chaotic map [216]. Operations *op* are selected through random-like numbers generated using 1D chaotic map i.e. Logistic-Tent map [40] making the operation selection key-dependent. Hence, the number and kind of operations involved per-round in cipher image generation are decided dynamically. To maintain a balance between efficiency and security, the maximum value of *op_count* has been restricted in the range 1 to 4. For higher security applications the minimum and maximum limit of operations can be adjusted. Also, note that the choices for operations *op* are reversible operations so that any combination of these operations can be used during encryption and decryption is always possible. Following equations (8) & (9) give the mathematical details of the two chaotic maps used:

a) Logistic-Tent Map

$$X_{n+1} = \begin{cases} (rX_n(1-X_n) + (4-r)X_n/2) \; mod \; 1 & X_n < 0.5 \\ (rX_n(1-X_n) + (4-r)(1-X_n)/2) \; mod \; 1 & X_n \geq 0.5 \end{cases} \quad (8)$$

where $r \in (0,4]$

b) 3D-Chaotic Cat Map

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \; (mod \; 1) \quad (9)$$

where, A is

$$\begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix}$$

and $a_x, a_y, a_z, b_x, b_y, b_z$ are all being positive integers.

4.2.4 Key Description

Two chaotic maps (i.e. a 3D chaotic map and a 1D chaotic map) are used in the proposed work to have increased key space. Currently, only one out of three initial conditions (or seed values) of 3D chaotic map and parameter value for 1D logistic_tent map is made key dependent, while other two seed values of 3D chaotic map, seed value for 1D chaotic map and all six parameters for 3D chaotic map are kept fixed, such that $a_x = a_y = a_z = 1$ and $b_x = b_y = b_z = 2$. So, there is a scope to make other parameter and seed values also key-dependent by increasing the key-size.

In the current implementation, a 128-bit key is used. Parameter value for Logistic-Tent map is calculated by XORing the odd positioned bytes of the key together and the even positioned bytes of the key together to get two bytes and finally these two bytes are treated as a 16 bit integer value which is further converted into a decimal no. (of 4 decimal precision) falling in the range 3.57 to 4. Further, one seed value for 3D chaotic map is generated by treating the 128 bit key as 16 bytes, say key(0) to key(15), and calculating the seed value in the following way:

i) $tmp(i) = key(i) + key(i+8), 0 \leq i < 8$
ii) treat the obtained 8 tmp bytes as 64-bit unsigned integer which is then transformed into decimal number (of 4 decimal precision) between 0 and 1 to be treated as a seed value for 3D chaotic map.

As per the current implementation, all employed operations are very primitive and are directly implementable in hardware. From this perspective, per-round number of operations involved for encrypting M×N image using the implemented framework is on an average 9MN. This is because, 3 operations per pixel are required for calculating y-coordinate of pixel in the non-sequential encryption pattern and verifying that this pixel has not been encrypted so far. Further, on an average for each pixel there will be (1+2+3+4)/4 = 2.5 operations performed per round and before performing each operation firstly an operation is selected from the look-up table, so, doubling the average number of required operations per round. Therefore, on an average 3MN+5MN = 8MN operations are employed in the confusion step and further MN operations in the diffusion step, making it 9MN operations in total. In addition to these operations, some additional computations are required for generating chaotic sequences and for recalculating the position coordinates in case a pixel at position (x,y) is already encrypted.

Clearly, the per-round computational cost of current implementation of the proposed dynamic framework is much lesser than that of the per-round operations required in standard schemes like AES which involves computationally heavier operations including matrix multiplication of 4×4 state matrix (in Mix Columns step of AES per-round operations [10]). Mix Columns alone require much bulkier operations i.e. 4 multiplication modulo irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ and 3 addition (XOR) operations per byte besides other round operations.

4.2.5 Observations & Security Analysis of the proposed Chaos-based Dynamic Framework for Image Encryption

The scheme is implemented using MATLAB R2011a on machine with Windows 7 32-bit operating system with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM. A number of observations including NPCR, UACI, correlation coefficient between original and encrypted image, histogram, entropy, block-wise entropy variation and avalanche properties are taken on 256×256 grayscale images, as in principle, the grayscale logic can always be extended to the three RGB planes of colored images. Few of the observations are as discussed below.

Firstly, NPCR and UACI observations are taken to prove the efficacy of the scheme in generating entirely different cipher image with very minor change in the original image. These observations are significant to prove strength of the proposed framework against differential attacks. Observations of Correlation Coefficient between the original image and the corresponding cipher image are also taken to display the strength of the proposed scheme against statistical attacks.

Table 5 gives the entropy, NPCR, UACI and Correlation Coefficient observations taken for several rounds of the implemented framework on the grayscale water lilies image. The observations of NPCR, UACI and Correlation Coefficient are taken by complementing a single pixel at a time for several randomly chosen positions and averaging the results. The results show NPCR and UACI values approach their respective expected values i.e. more than 99% and 33% respectively for round count 8 and beyond. This suggests that application of 8 or more rounds of the implemented framework leads to generation of cipher image which is highly sensitive to any minor change in the original image. Correlation Coefficient having value very close to 0 indicate that the plaintext image and the cipher image are highly uncorrelated. The results demonstrate that the implemented framework with 8 or more rounds offers high

resistance against statistical and differential attacks by adversary. Further, Table 6 shows these observations taken for several images including plain white image with 8 rounds of encryption, which again are favorable and demonstrate strength of the proposed work.

TABLE 5
ENTROPY, NPCR, UACI & CORRELATION COEFFICIENT FOR ENCRYPTED WATER LILIES IMAGEWITH ROUND VARIATIONS

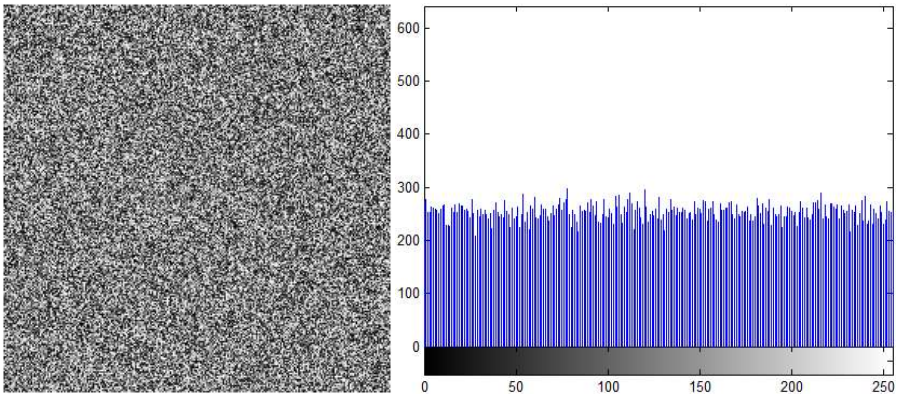
Round Count	Entropy (Cipher Image)	NPCR (%)	UACI (%)	Correlation Coefficient
2	7.9966	61.16	19.27	1.09×10^{-04}
4	7.9965	87.71	29.09	-6.34×10^{-05}
6	7.9974	92.91	30.94	-5.67×10^{-04}
8	7.9974	99.45	33.32	1.70×10^{-04}
10	7.9974	99.55	33.45	-2.52×10^{-04}
12	7.9973	99.58	33.48	-8.26×10^{-04}
14	7.9971	99.59	33.51	6.01×10^{-04}
16	7.9975	99.59	33.46	-12.00×10^{-04}

TABLE 6
ENTROPY, NPCR, UACI & CORRELATION COEFFICIENT FOR CIPHER IMAGES CORRESPONDING TO DIFFERENT PLAINTEXTS

Grayscale Image	Entropy (Cipher Image)	NPCR (%)	UACI (%)	Correlation Coefficient
Water Lilies	7.9974	99.45	33.32	1.70×10^{-04}
Baboon	7.9971	99.49	33.37	-5.39×10^{-05}
Lena	7.9973	99.40	33.32	-6.82×10^{-04}
Plain White	7.9974	99.54	33.45	-7.15×10^{-04}

As the NPCR, UACI and Correlation Coefficient observations show that 8 rounds of the proposed implemented framework approach respective required values indicating that it provides high strength against statistical and differential attacks, therefore, all further observations are taken with 8 rounds of the proposed work.

Fig. 42 displays the encrypted 256×256 Water Lilies image with corresponding histogram and entropy values. As can be seen clearly, the image encrypted with proposed scheme has complete removal of redundancy present in the plain image.



Entropy: 7. 9974

Fig. 42 Encrypted Grayscale Water Lilies Image with Histogram

Block-wise entropy variation in encrypted image is observed to note the uniformity in entropy across the encrypted image when divided in equal sized blocks. Fig. 43 shows the plot for block-wise entropy variation in encrypted Water Lilies image 256×256 divided into 256 blocks each of size 16×16. It is evident from the plot that the entropy variation across blocks is very small which indicates uniform intensity distribution at lower levels of granularity.

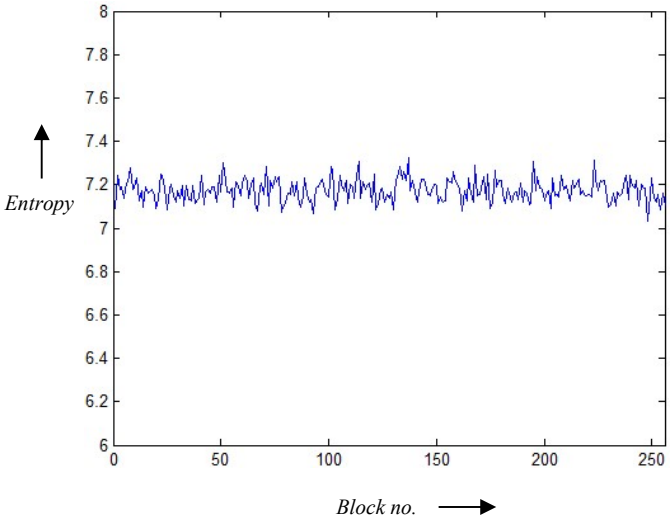


Fig. 43 Block-wise Entropy Plot of Encrypted Grayscale Water c Image

To observe the impact of variation of plaintext size, block-wise entropy variation in the encrypted image with the proposed scheme is also observed for images with sizes 512×512, 256×256, 128×128, 64×64 and 32×32 and it is observed that the block-wise entropy is nearly uniform irrespective of the plaintext size. Fig. 44 and 45 shows the plot of block-wise entropy variation for Lena image with sizes 512×512 and 32×32 respectively. These observations show that though the present work considers image as a single block, however, sub-blocks of the image can be encrypted using specific or changing block cipher modes of operation like CBC, CTR etc.

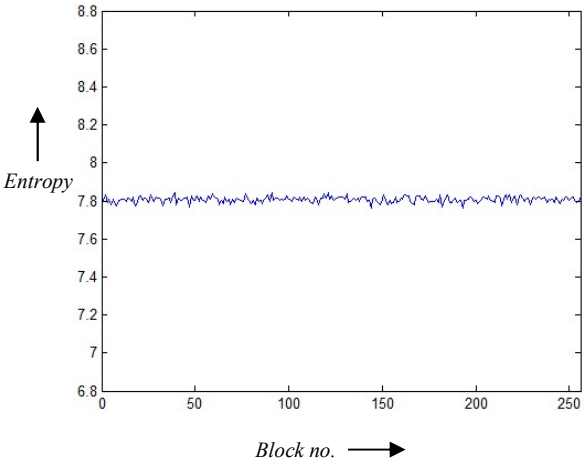


Fig. 44 Block-wise Entropy Plot of Encrypted Image (Lena – 512×512)

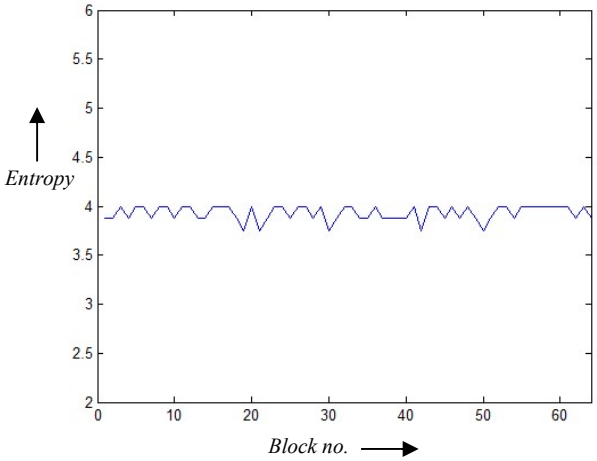


Fig. 45 Block-wise Entropy Plot of Encrypted Image (Lena – 32×32)

Nearly uniform histogram is obtained on encrypting a plain white image using the implementation of the proposed framework as shown in Fig. 46. This observation verifies complete removal of redundancy and uniform distribution of intensities in cipher image for original image having complete redundancy and single peaked histogram.

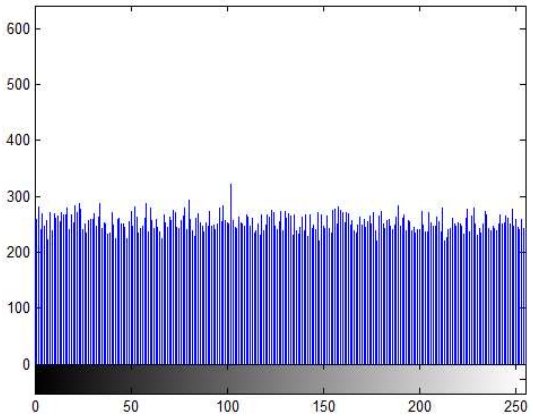


Fig. 46 Histogram for Encrypted White Image

To demonstrate strength against differential cryptanalysis, avalanche properties are also investigated. The plots Fig. 47 & 48 show a nearly 50% change in the number of bits changed in the encrypted 256×256 Water Lilies image with one-bit change in the key, one-bit change per pixel in the original image respectively. Fig. 49 shows that the decrypted image also changes by around 50% when decrypted by one-bit changed key. These plots show that the cipher demonstrates strong avalanche properties and the observations are nearly uniform irrespective of the position of the bit changed. These observations show significant and uniform contribution of each bit of the key to the pixels of the cipher image thereby establishing that implementation of the proposed framework possess strong confusion property.

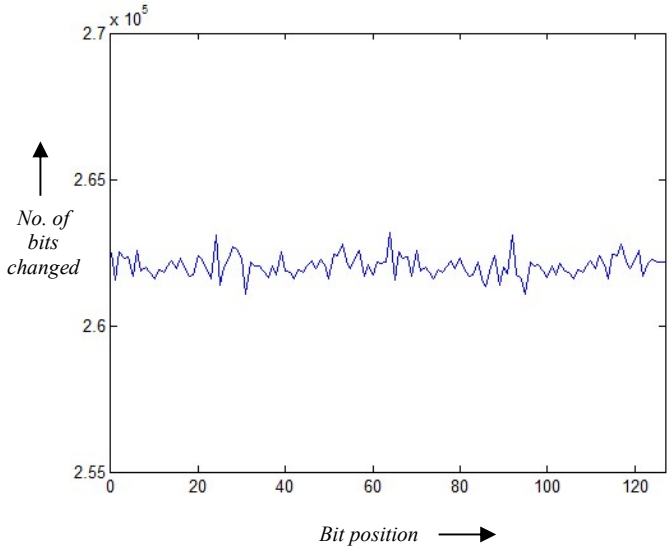


Fig. 47 Avalanche Property – Plot of number of bits changed in the Encrypted Water Lilies with one bit change at each position of the 128-bit key

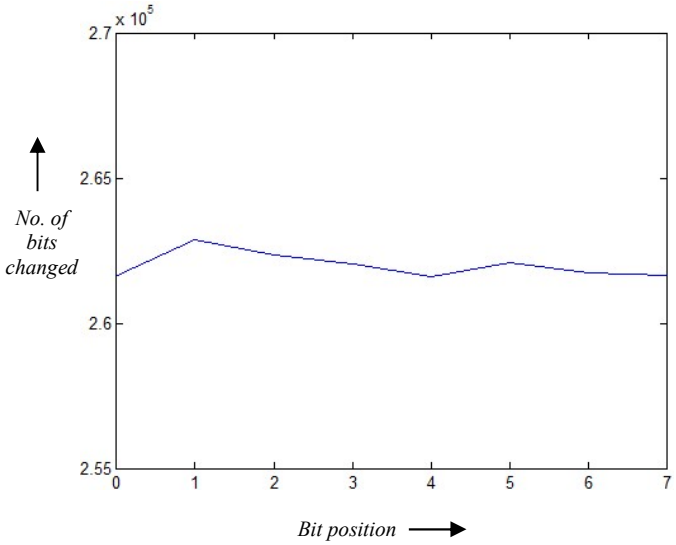


Fig. 48 Avalanche Property – Plot of number of bits changed in the Encrypted Water Lilies with one bit change per pixel at each of the 8 position

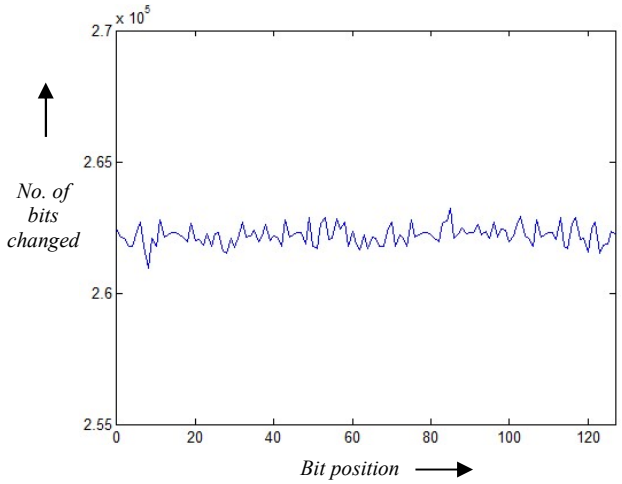


Fig. 49 Avalanche Property – Plot of number of bits changed in the Decrypted Water Lilies with one bit change at each position of the 128-bit key while decryption

NIST statistical test suite [217] observations are also taken to verify randomness of the cipher image obtained using the proposed work. *P-value* is ≥ 0.01, indicate that the sequence under test is random (at 1% significance level). Table 7 displays the observations of all the NIST tests on encrypted 256×256 grayscale Baboon image. Test status of all the tests emerged out be success which demonstate that the obtained cipher is completely random.

TABLE 7

RESULTS OF NIST TEST-SUITE FOR RANDOMNESS

Test Name	Adjustment Parameter	P-value	Test Status
Frequency Test	-	0.861854	Success
Block Frequency Test	Block length = 128	0.124819	Success
Run Test	-	0.966985	Success
Longest Run Test	-	0.615741	Success
Binary Matrix Rank Test	-	0.798075	Success
FFT Test	-	0.476308	Success
Non-overlapping Template Matching Test	Block length = 10	-	Success
Overlapping Template Matching Test	Block length = 10	0.361665	Success
Universal Statistical Test	-	0.776738	Success
Linear Complexity Test	Block length = 500	0.406574	Success
Serial Test (p-value1)	Block length = 16	0.971437	Success
Serial Test (p-value2)	Block length = 16	0.868488	Success
Approximate Entropy Test	Block length = 10	0.853303	Success
Cumulative Sums Test	-	0.650924	Success
Random Excursions Test	-	-	Success
Random Excursions Variant Test	-	-	Success

4.2.6 Resistance against known/chosen plaintext attacks & Differential Cryptanalysis

The proposed dynamic framework with multi-level dynamism will avert any possible breach into the cryptosystem with high strength because it will be much harder for the attacker to design an attack targeting the structure or design of per-round operations as the type of operations, the number of operations performed on each pixel in different rounds varies and is unknown to the attacker. Also, the type and number of per-round operations performed on the same pixel position will vary if the same key is applied with a slightly modified image since the sequence of encrypting pixels is also dynamically decided based the plaintext besides the key. This will offer added resistance against known/chosen plaintext, differential and impossible differential attacks.

4.3 A CHAOS-BASED PROBABILISTIC BLOCK CIPHER FOR IMAGE ENCRYPTION

Further, probabilistic encryption has been explored as another level of dynamism in encrypting visual content. Probabilistic encryption [124], [165] is an approach in which different cipher texts are generated each time same plaintext is encrypted using the same key. The idea of probabilistic encryption is simple and elegant. It states that the plaintext should have multiple encodings out of which one is selected randomly at a time. While doing the literature review, it is found that researchers have made significant contributions for probabilistic encryption in the area of public-key cryptography [124], [165]–[173], [218]–[226] but very few probabilistic symmetric encryption schemes have been reported [174]–[179]. And in fact, to the best of our knowledge, no practical probabilistic symmetric encryption scheme exists with customizable block-size to make it suitable for multimedia data like images. Hence, this gap has motivated us to extend the idea of randomization and a new probabilistic symmetric encryption scheme with customizable block-size was designed to make it workable:

- while treating the entire message as a single block, or
- be applied as a block cipher which can be operated in different block cipher modes (including native ECB mode).

The scheme uses chaos for generating key stream which is utilized at different levels to perform permutation and substitution operations. The scheme demonstrates desired levels of confusion and diffusion and is found suitable for encrypting images.

The proposed Probabilistic block cipher involves four rounds of operations and operates on customizable block-size. The customizable block-size offers flexibility to applications and ensures that the scheme can be used to encrypt any sized images in entirety or block by block using different cipher modes. Because of the probabilistic nature of the proposed scheme, it is suitable for application in the native ECB mode as well. This is a very significant achievement of the proposed work because the block ciphers designed using the traditional non-probabilistic approach with fixed block-sizes rely on different modes of operation (like CBC, CTR etc.) while encrypting bulky data like images so as to avoid propagation of redundancy of the plain image to the cipher image. Use of these modes adds to the computational cost as well as transmission of additional information (like initial vector) along with the key to the receiver which is definitely an added overhead. Further, relying on different modes of operation to compensate for the underlying weaknesses of the encryption scheme is not appreciable.

The proposed probabilistic scheme encrypts an N-bit plaintext into corresponding 2N-bit cipher text. The following figure Fig. 50 shows the block diagram of the proposed chaos-based probabilistic block cipher:

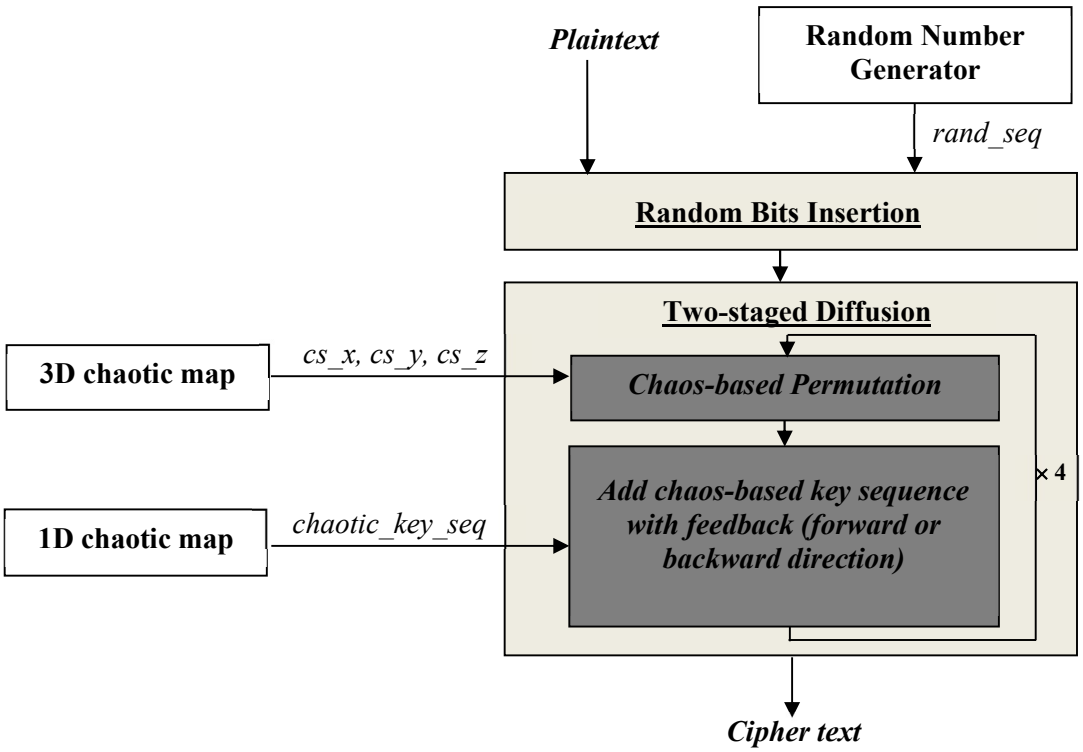


Fig. 50 Block diagram for the Proposed Chaos-based Probabilistic Block Cipher

Before explaining the operations of the proposed work, we first describe the inputs to the scheme below:

(a) N-bit plaintext represented as $p_0, p_1, p_2, p_3.....p_N$

(b) random sequence *rand_seq* is used for performing Random Bits Insertion.

(c) chaotic sequences *cs_x*, *cs_y*, *cs_z* are used for permuting diffused data values during diffusion stage I in each round. They are generated using a 3D chaotic map [216].

(d) chaotic sequence *chaotic_key_seq* is used to achieve diffusion as well as substitution simultaneously in diffusion stage II in each round. It is generated using logistic-tent map [40].

The proposed probabilistic block cipher employs the same chaotic maps to generate key stream utilized in the per-round substitution and permutation operations as used in the dynamic framework implementation i.e. Logistic-tent map and 3D-Chaotic Cat Map given by equations (8) & (9) in Section 4.2.3.

4.3.1 Key Description

A 256-bit key is used in the proposed scheme. The key is treated as 32 bytes key_1, key_2, … key_{32} and using these 32 bytes, six 8-byte words (namely temp1, temp2, .. temp6) are generated, out of which first two are used to compute the seed and parameter value r for the Logistic-Tent map ($r \in [3.57, 4]$) respectively, three are used to compute the seed value for the 3D chaotic map and all these values are computed to have 6 decimal precision. The last 8-byte word is used byte-wise in the two stages of diffusion of each of the four encryption rounds (i.e. two bytes in each round) to initialize the value of prev_byte (discussed in Section 4.3.2). Following pseudo-code describes the generation of the six 8-byte words from the 256-bit key treated as 32-bytes from key_1 to key_{32}:

for k = 1 to 8

$temp1(k) = ((key_k <<< (key_{16+k} \% 8)) \oplus key_{8+k})) <<< (key_{24+k} \% 8)$;

$temp2(k) = key_{16+k} \oplus ((key_{8+k} \oplus key_k) >>> (key_k \% 8))$;

$temp3(k) = key_{8+k} \oplus ((key_{16+k} \oplus key_{24+k}) <<< (key_k \% 8))$;

$temp4(k) = (key_{16+k} >>> (key_k \% 8)) \oplus (key_{24+k} >>> (key_{8+k} \% 8))$;

$temp5(k) = ((key_{8+k} >>> (key_k \% 8)) \oplus key_{24+k}) >>> (key_{16+k} \% 8)$;

$temp6(k) = (key_k <<< (key_{8+k} \% 8)) \oplus (key_{16+k} <<< (key_{24+k} \% 8))$;

end for

where, ⊕, %, <<<, >>> represents XOR, modulo, circular left shift, and circular right shift operations respectively.

4.3.2 Description of operations in the proposed Chaos-based Probabilistic Block Cipher

As shown earlier in Fig. 50, the proposed scheme comprises of two basic phases namely – Random Bits Insertion and four rounds of Two-staged Diffusion. They are as described below:

I. ***Random Bits Insertion Phase:*** In this phase, random bits are inserted after each plaintext bit. Using a random number generator, a random sequence *rand_seq* is generated, one random value for each bit of plaintext. If the random value is even then '0' is inserted otherwise '1' is inserted after the plaintext bit. Thus, this operation contributes to doubling the size of cipher text as compared to the plaintext i.e. for N-bit plaintext, the corresponding cipher text will comprise of 2N bits. This step also contributes in removing redundancy and making the distribution of 0s and 1s in the cipher more uniform.

It is this Random Bits Insertion phase which contributes to the probabilistic nature of the proposed encryption scheme. The following diffusion phase is entirely deterministic and reversible for facilitating decryption and the random bits inserted after each plaintext bit (in the Random Bits Insertion phase) are required to be simply removed during decryption, to ensure smooth retrieval of the plaintext at the receiver's end. Hence, there is no need for the receiver to have any knowledge of the random bits inserted during encryption.

II. ***Two-staged Diffusion:*** The output of the Random Bits Insertion phase is the input for the first round of two-staged diffusion phase and four rounds of two-staged diffusion are performed. This phase comprises of two stages. They are described below.

i. In the first stage, diffusion is achieved along with chaos-based permutation. Here, the input to this stage is treated in two halves. Let *no_of_bytes* represent number of bytes of input to this stage (which is actually 2n for n-byte plaintext). A 3D chaotic map is employed to generate three chaotic sequences *cs_x, cs_y*

and *cs_z*. Values in chaotic sequences *cs_x* and *cs_y* are integers lying in the interval [1, *no_of_bytes*] while those in sequence *cs_z* have values 0 or 1. Following are the steps of the first stage:

a) Two positions *x* and *y* are chosen using chaotic sequences *cs_x* and *cs_y* along with previous cipher-byte feedback. If same position x (or y) is already encountered then x (or y) is updated to sequentially next free location not yet encountered. For achieving this, next_free_position variable is maintained to store the least value of unused positions left and it is updated every-time its value is used to resolve a collision for x (or y) value.
b) Then, corresponding bytes of the two halves are XOR-ed and a new byte is generated.
c) The newly generated byte is placed at the position *x* while one of the two initial bytes is chosen using chaotic sequence *cs_z* and is placed at position *y*.

Let *r* be the round number and the i^{th} corresponding bytes from the two halves be represented by p'_i and p'_{i+n} where n is the number of bytes in the plaintext. Also, let p''_i represent the i^{th} byte of the output of this stage. For the four rounds, the value of prev_byte in this stage is initialized with the odd numbered bytes of temp6 i.e. $temp6_1$, $temp6_3$, $temp6_5$, $temp6_7$ respectively, where temp6 is one of the six 8-byte words generated using the 256-bit key (as described in Section 4.3.1). Following is the algorithm/pseudo-code for this stage:

ALGORITHM 6: Diffusion Phase (First Stage) of the proposed Probabilistic Block Cipher

INPUT: r (round number), n (number of bytes in the plaintext), no_of_bytes (number of bytes in intermediate cipher obtained after Random Pixel Insertion phase), p' (intermediate cipher bytes obtained after Random Pixel Insertion phase), temp6 (8-byte word generated from 256-bit key), cs_x, cs_y, cs_z (three chaotic sequences used in Diffusion Phase- First Stage)

1: prev_byte = $temp6_{2(r-1)+1}$
2: **for** i = 1 to n
3: x = ($cs_x_i \oplus$prev_byte) % no_of_bytes + 1;
4: x = update_if_repeated_position(x);

5: y = (cs_y_i ⊕ prev_byte) % no_of_bytes + 1;
6: y = update_if_repeated_position(y);
7: z = cs_z_i;
8: new_byte = p'$_i$ ⊕ p'$_{i+n}$;
9: p''$_x$ = new_byte;
10: p''$_y$ = p'$_{i+(z*n)}$;
11: prev_byte = new_byte;
12: **end for**

ii. In the second stage, diffusion is achieved along with adding chaos-based key sequence *chaotic_key_seq*. This stage involves XOR-ing of previous cipher-byte feedback and key sequence value with the current byte of input to this stage. This stage is run alternatively in forward (i.e. from first to last input byte) and backward direction (i.e. from last to first input byte). This is done to ensure effective diffusion, in fewer subsequent rounds, in case of minor changes done to the plaintext irrespective of position of change.

Let p''$_i$ and c_i represent the i^{th} byte of the input and output of this stage respectively. Also, let r represent the round number. For the four rounds, the value of prev_byte in this stage is initialized using the even numbered bytes of temp6 i.e. temp6_2, temp6_4, temp6_6, temp6_8 respectively, where temp6 is one of the six 8-byte words generated using the 256-bit key (as described in Section 4.3.1). Following is the algorithm/pseudo-code for this stage:

ALGORITHM 7: Diffusion Phase (Second Stage) of the proposed Probabilistic Block Cipher

INPUT: r (round number), no_of_bytes (number of bytes in intermediate cipher obtained after Random Pixel Insertion phase), p'' (intermediate cipher bytes obtained after First stage of Diffusion phase), temp6 (8-byte word generated from 256-bit key), chaotic_key_seq (chaotic sequences used in Diffusion Phase-Second Stage)

1: prev_byte = temp6_{2r};
2: **if** (r % 2 == 0)
3: **for** i = no_of_bytes down to 1
4: c_i = p''$_i$ ⊕ prev_byte⊕chaotic_key_seq$_i$;
5: prev_byte = c_i;

6: **end for**
7: **else**
8: **for** i = 1 to no_of_bytes
9: $c_i = p''_i \oplus$ prev_byte $\oplus$ chaotic_key_seq$_i$;
10: prev_byte = c_i;
11: **end for**
12: **end if**

Clearly, both the described stages are designed to achieve diffusion by ensuring that a single byte of cipher text gets contributed by multiple plaintext bytes. The first stage achieves diffusion along with permutation and partial substitution of the data bytes in a key dependent manner. And, the second stage is designed to diffuse minor change in the plaintext to the entire cipher text along with performing key dependent substitution. For effective and faster diffusion, both stages involve previous encrypted byte feedback so that minor changes in the plaintext get permeated in the cipher text at a fast rate. The output of two-staged diffusion phase becomes the input for the next round of diffusion operations and this goes on for four rounds after which the final cipher text is obtained. Since, the basic operation involved in both the diffusion stages is simple XOR and per-round diffusion operations are carefully designed to achieve desired security levels in only four rounds, hence the scheme offers high strength with efficiency.

4.3.3 Computational Complexity

All operations in the proposed scheme are primitive and can be implemented in hardware directly. Therefore, for evaluating the performance of the proposed scheme, the computational complexity of the proposed scheme is evaluated through evaluation of the number of operations involved during the different phases. Following are the details of the number of operations involved in different phases of the proposed scheme for encrypting a M×N plain image:

I. ***Random Bits Insertion Phase:*** Since there is bit level insertion, therefore there will be 8 insertions per byte and hence, for a M×N plain image, the total number of operations in this phase is 8MN.

II. ***Per-round Diffusion Phase:*** In the first stage of two-staged diffusion it is to be noted that, the addition of 1 while calculating x and y location values is just to ensure that the resultant x and y values fall in the range [1, no_of_bytes]. So, these addition operations may or may not be required as per platform used for implementation. Hence, while calculating the number of operations performed in this stage of the diffusion phase, these addition operations are not included as they are not logically required and were mere implementation limitation for MATLAB platform. Also, as per probability, updation of x (or y) value to sequentially next free location will happen half of the times. Also, for achieving permutation and partial substitution two bytes of plaintext are considered together. Taking into account all this, for operating on these two bytes being considered together, the first stage of diffusion phase per-round employs 3 XOR operations, 2 modulo operations, 2 comparison operations and 1 addition operation as per probability while updation of x (or y), 1 addition and 1 multiplication operation while setting the pixel byte at position y. Hence, the total number of per-round operations employed in this stage for encrypting a M×N plain image (whose intermediate size has become M×2N due to Random Bits Insertion phase) is 10(2MN)/2 = 10MN.

Further, in the second stage of diffusion phase, for each byte of the plaintext 2 XOR operations are involved. Hence, the total number of per-round operations employed in this stage for encrypting a M×N plain image (whose intermediate size has become M×2N due to Random Bits Insertion phase) is 2(2MN) = 4MN.

So, the total number of per-round operations in two-staged diffusion phase for encrypting a M×N plain image is 10MN + 4MN = 14MN. Evidently, first stage of the two-staged diffusion involves maximum number of operations as compared to other parts of the proposed scheme.

4.3.4 Observations & Security Analysis of the proposed Chaos-based Probabilistic Block Cipher for Image Encryption

The proposed probabilistic block cipher is implemented and tested using MATLAB R2011a on a computer systemhaving Windows 7 32-bit operating system, with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM. A variety of observations have been taken by applying the

proposed scheme on 256×256 grayscale images to observe the efficacy of the scheme in securing images. These observations include NPCR, UACI, correlation coefficient between original and encrypted image, histograms, deviation from uniform histogram and entropy of encrypted images including the encrypted image corresponding to plain-white original image, block-wise entropy variation in encrypted image and avalanche properties observations.

Experimentation has been conducted on a wide variety of different images, however, for the purpose of illustration results on standard images like Water Lilies, Baboon and Lena are presented. Results on plain -white image are also presented to demonstrate strength of our proposed encryption scheme on plain image with complete redundancy. Though, the observations have been taken on grayscale images but the scope of proposed work can be extended to the three RGB planes of the colored images. Hence, the results obtained for grayscale images hold true for colored images as well.

It is appropriate to highlight that the subsequent observations for NPCR, UACI, Correlation Coefficient and Avalanche Properties require a comparative analysis and, therefore, these observations have been taken keeping the contribution of the probabilistic step (i.e. Random Bits Insertion phase) constant so that the strength of the scheme operations can be proven in a neutral way while making these comparative observations.

NPCR, UACI and correlation coefficient observations are taken to prove the efficacy of the proposed work against differential cryptanalysis. To study the strength of the proposed scheme against statistical attacks correlation coefficient observations between the original image and corresponding cipher image are taken on several images. Table 8 shows the NPCR, UACI and Correlation coefficient observations for different 256×256 grayscale images including plain white image as well. To take these observations, a single pixel is randomly chosen each time and is complemented. Average value is recorded after taking multiple observations for each measure on the same image. The results obtained show that NPCR and UACI values are over 99% and 33% respectively and they achieve their respective desired expected values [197]. The observations demonstrate that the cipher image obtained using the proposed scheme is highly sensitive to changes in pixel of the plain image as minor as a single pixel and thus, the proposed scheme possess desired strength to resist differential attacks.

Further, correlation coefficient values (as provided in Table 8) are approaching zero which show that there is no observable correlation between the original image and the corresponding cipher image and hence the proposed scheme offers high strength against statistical analysis.

TABLE 8
NPCR, UACI & CORRELATION COEFFICIENT FOR CIPHER IMAGES CORRESPONDING TO DIFFERENT PLAINTEXTS

Grayscale Image	NPCR (%)	UACI (%)	Correlation Coefficient
Water Lilies	99.5830	33.5008	-2.2056×10^{-04}
Baboon	99.5988	33.4642	4.3247×10^{-05}
Lena	99.5808	33.4413	-5.6521×10^{-05}
Plain White	99.6043	33.4302	-14.7970×10^{-04}

The proposed probabilistic block cipher encrypted grayscale 256×256 Water Lilies image with histogram is shown in Fig. 51. Clearly, there is complete removal of redundancy in cipher image and a uniform histogram is obtained on encrypting the original image with the proposed scheme.

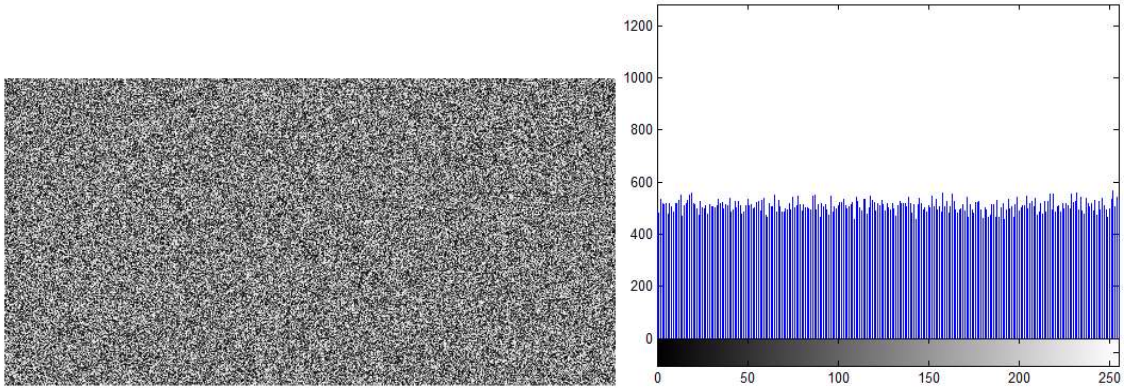


Fig. 51 Encrypted Grayscale Water Lilies Image with Histogram

Further, to prove the efficacy of the proposed scheme in removing redundancy existing in the plaintext image, observations are taken on plain white image. Fig. 52 shows that a nearly uniform histogram is obtained for the encrypted plain white image. This demonstrates the strength of the proposed scheme in completely removing redundancy existing in the plaintext image as the proposed scheme is capable of generating uniform distribution of intensities for a given single intensity input.

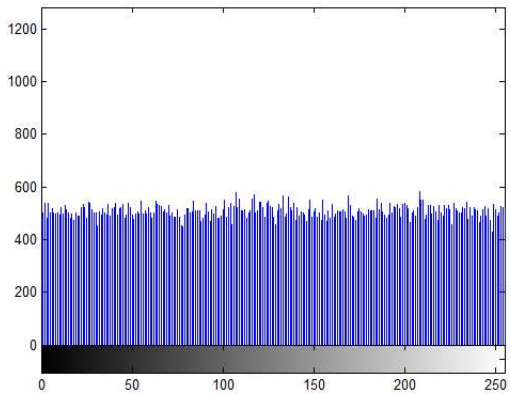


Fig. 52 Histogram for Encrypted White Image

Also, for performing histogram analysis, observations are taken for quality metric proposed in [227] i.e. deviation from uniform histogram. Table 9 shows the deviation from uniform histogram for different encrypted images including corresponding to that of plain white image. Very small value of deviation from uniform histogram again demonstrates that the histograms obtained for the corresponding encrypted images are nearly uniform and hence proves that redundancy of plaintext, in fact that of completely redundant image (plain white image), is completely removed from corresponding encrypted image.

Table 9 also represents the entropy values of the original images and the corresponding encrypted images. The observations show that entropy of the encrypted image is very close to the ideal value of 8 even for plain-white original image having entropy 0. This is an indicative of uniformly random intensity distribution in cipher image.

TABLE 9
ENTROPY VALUES FOR DIFFERENT PLAINTEXTS AND CORRESPONDING ENCRYPTED IMAGES ALONG WITH DEVIATION FROM UNIFORM HISTOGRAM

Grayscale Image	**Entropy (Original Image)**	**Entropy (Cipher Image)**	**Deviation from Uniform Histogram (Cipher Image)**
Water Lilies	7.2171	7.9986	0.0352
Baboon	7.2702	7.9984	0.0373
Lena	7.4312	7.9987	0.0349
Plain White	0	7.9984	0.0380

To demonstrate the uniformity of entropy across the cipher image, the encrypted image is broken into equal sized blocks and block-wise entropy is studied. Fig. 53 gives the plot displaying block-wise entropy variation for the encrypted 256×512 Water Lilies image which is broken into 64 equal sized blocks, each of size 32×64. The observation shows that the block-wise entropy is high and the variation is also not significant. This observation strengthens the claim that there is uniformly random intensity distribution, even at smaller levels of granularity, in the cipher image obtained using the proposed scheme.

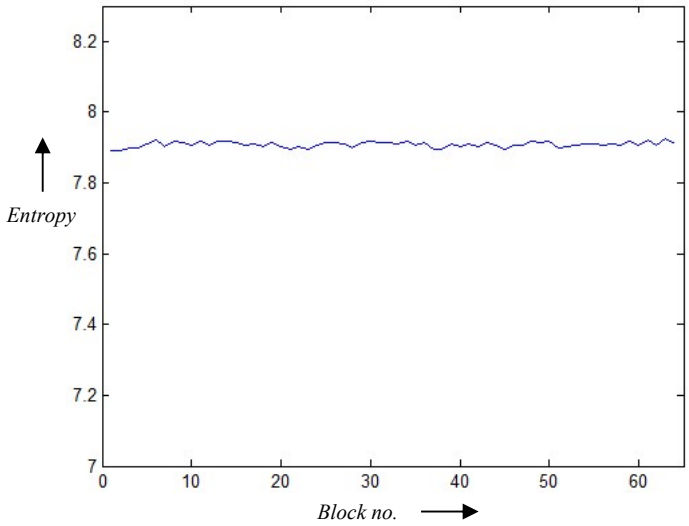


Fig. 53 Block-wise Entropy Plot of Encrypted Grayscale Water Lilies Image

The proposed probabilistic block cipher uses a 256-bit key making the key space of 2^{256}. The 32 bytes of the key are used to generate six 8-byte words as described in Section 4.3.1. Out of these six 8-byte word, three are used to compute the seed value for the 3D chaotic map used in the first stage of two-staged diffusion while two are used to compute the seed and parameter values for the logistic_tent map which is used in the second stage of two-staged diffusion. All these values are computed to have 6 decimal precision. The last 8-byte word is used byte-wise in the two stages of diffusion of each of the four encryption rounds (i.e. two bytes in each round) to initialize the value of prev_byte (discussed in Section 4.3.2). Each bit of the key contributes significantly in the cipher text bits uniformly as demonstrated by the following avalanche property observations taken by observing change in the number of cipher text or decrypted plaintext bits with one bit change in the key.

Observations on Avalanche properties are taken to study key sensitivity and to prove the strength of the proposed scheme against differential cryptanalysis. The plot of number of bits

changed in cipher with one bit change in the secret key show that irrespective of the position of the key bit changed, the change in the number of bits in cipher text is around 50%. This indicates that the proposed scheme possesses high confusion, high key sensitivity, and all key bits contribute uniformly and significantly to the cipher bits. Fig. 54 demonstrates this observation for encrypted 256×256 Water Lilies image.

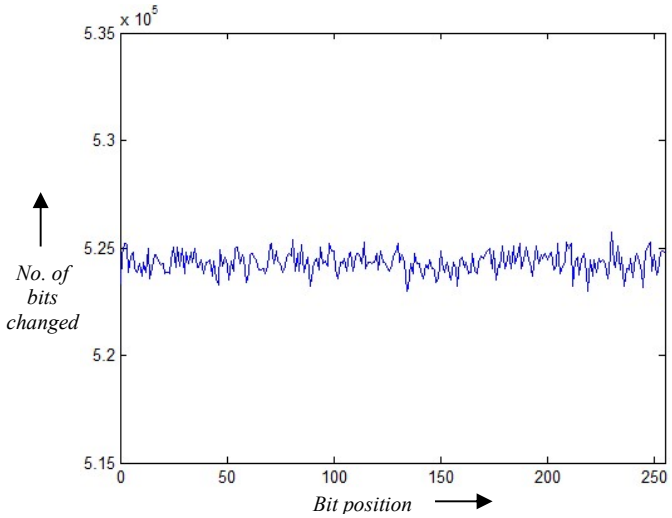


Fig. 54 Avalanche Property – Plot of number of bits changed in the Encrypted Water Lilies with one bit change at each position of the 256-bit key

Further, to strengthen the claim that the proposed scheme possesses high confusion and high key sensitivity, another observation is taken which involves observing the change in the number of bits of the decrypted image when decrypted with a key having one-bit change as compared to the key used during encryption. Fig. 55 shows the plot for number of bits changed in decrypted 256×256 Water Lilies image with one-bit change in the key. This plot also shows strong confusion property and high key sensitivity because irrespective of the position at which the key-bit is changed, the change in the decrypted image as compared to the original Water Lilies image is nearly 50% always.

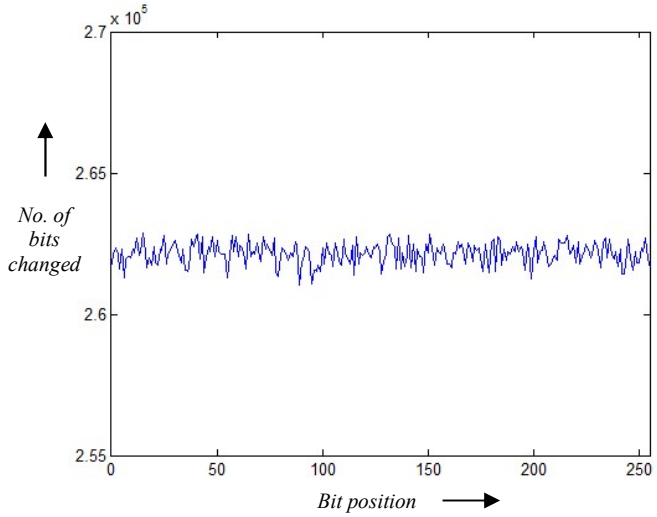


Fig. 55 Avalanche Property – Plot of number of bits changed in the Decrypted Water Lilies with one bit change at each position of the 256-bit key while decryption

Fig. 56 displays the plot for number of bits changed in cipher image with one bit changed per pixel in the original 256×256 Water Lilies image. Again, there is nearly 50% change in the cipher obtained with one-bit changed per pixel in the original image. This displays that all bit positions of pixels in the original image contribute appreciably to the cipher bits without any biases. This observations along with NPCR and UACI observations also show strong difussion property possessed by the proposed scheme.

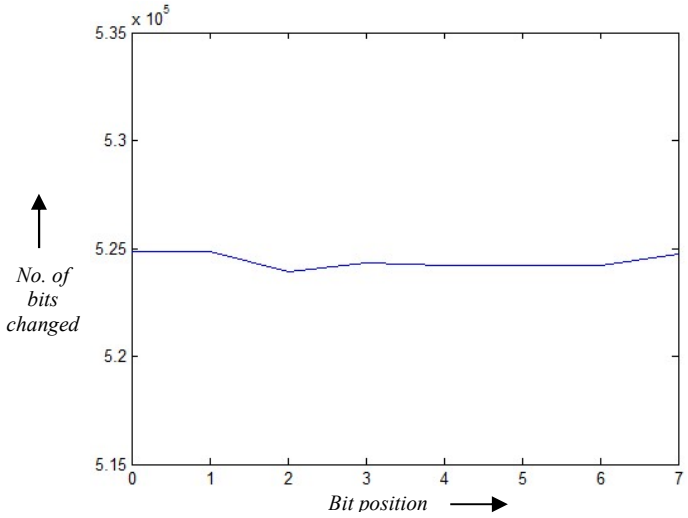


Fig. 56 Avalanche Property – Plot of number of bits changed in the Encrypted Water Lilies with one bit change per pixel at each of the 8 position

4.3.5 Resistance against Known/Chosen Plaintext, Ciphertext-only attacks & Differential Cryptanalysis

The proposed scheme is a probabilistic scheme involving use of randomization through its Random Bits Insertion Phase. Such probabilistic schemes possess higher security [124], [167] and are resistant to known/chosen plaintext attacks, ciphertext-only attacks and differential cryptanalysis because the cipher text changes each time the same plaintext is encrypted even using the same key due to the use randomization. Therefore, in principle, same plaintext generates different cipher texts and similarly same cipher text may correspond to more than one plaintext at different times. Hence, known/chosen plaintext attack, ciphertext-only attack and differential cryptanalysis cannot reveal any information about the key or plaintext when encrypted using the proposed probabilistic scheme. Thus, the proposed probabilistic encryption scheme possesses resistance against chosen plaintext, ciphertext-only attacks and differential cryptanalysis.

4.4 CONCLUDING REMARKS

Clearly, the above described proposed untraditional encryption schemes possess the desired security levels. Observations show that all these schemes possess strong avalanche properties displaying that high key sensitivity of the proposed schemes. Also, NPCR and UACI also attain their desired values displaying sensitivity of the schemes with minor changes in the plaintext which further demonstrate resistance against cryptanalytic attacks. The values of correlation coefficient approaching zero for all proposed schemes show no correlation between the plain image and the cipher image thereby demonstrating strength of the proposed schemes against statistical attacks. All the schemes demonstrate complete removal of redundancy in the cipher even with plain image having 100% redundancy i.e. plain white image. The single peaked histogram for such plain image generates a nearly uniform histogram for the cipher image obtained using the proposed schemes which shows the effectiveness of the proposed schemes in overcoming redundancy attributed to visual content like images. Further, NIST statistical test observations show that the generated cipher behaves as a random signal (noise) which again display the high strength offered by the proposed scheme.

Also, a very important achievement is that as the schemes have been designed to cater to the special needs of visual content like images, hence they support customizable block-sizes and employ very lightweight simple operations for achieving efficiency specifically for real time

applications or/and applications working in resource constrained environments. Due to customizable block-size the proposed schemes can work in native ECB mode or any other block cipher mode as per requirement which is not the case with traditional standard block ciphers like AES.

Further, chaos has been used as an integral component in the proposed dynamic framework and proposed probabilistic block cipher to provide desired levels of randomness in these schemes. The general criticism against use of chaos, i.e. the continuity attributed with chaotic functions and impact on the chaotic behavior on their discretization, have been addressed in our proposed schemes since the schemes are not static and involved dynamism at one or multiple levels ensuring that the overall impact on the cipher does not dependent only on chaos but also dynamically change with change in key/plaintext by view of change in operations performed or due to random bits inserted in case of the proposed Probabilistic block cipher. Therefore, this criticism against use of chaos has been taken care of in the proposed schemes.

Also, though all the proposed untraditional encryption schemes have been tested for their strength on images yet since videos are nothing but moving frames of images, hence, these ideas can be extended for securing videos as well.

CHAPTER 5

CRYPTANALYSIS OF CHAOS-BASED IMAGE ENCRYPTION SCHEMES REDUCIBLE TO EQUIVALENT MATHEMATICAL MODEL OF SET OF EQUATIONS

As discussed in previous chapters, since visual content has special characteristic like redundancy and bulkiness, researchers have identified a need for designing separate encryption algorithms catering to these special needs. Efficiency and complete removal of correlation among neighboring pixels have been two of the most common focus points in recent works addressing visual media security. Also, chaos has found significant contribution in encryption schemes for multimedia due to its favorable characteristics like random-like behavior, high sensitivity to initial conditions and parameters, ergodicity etc. Past two decades, have seen several developments in chaos-based cryptography especially for securing images but unfortunately many of them have been cryptanalyzed and have been proven to be insecure for practical usage. Hence, there is lot of scope of improvement in the way chaos has been currently used in designing encryption schemes.

A survey of cryptanalysis of various chaos-based image encryption schemes was carried out as discussed in Section 2.3 and it revealed that most of these cryptanalyzed image encryption schemes employ simple SP-Network involving permutation and/or substitution stages sometimes also repeated over multiple iterations. Due to the simple design of the encryption scheme weaknesses in them could be identified using simple known/chosen plaintext attacks. This is largely because of these encryption schemes have weak designs and there is blind reliance only on chaotic properties of key-stream for security without incorporation of operations that can establish intricate confusion and diffusion characteristics in the encryption process. In some schemes the permutation and/or substitution is performed at bit level while in others these are performed at the pixel level. Very often chaos-based image encryption schemes claim to possess large key-space based on the range and precision of the parameters and initial conditions of the chaotic functions being used as key for such schemes. But in many of the schemes, these claims of large key-spaces to resist cryptanalysis becomes largely futile because while designing image encryption schemes using chaos, one of the major concerns is resource

efficiency and many a times to make the scheme efficient entire reliance of security is kept on the chaotic key-stream being unpredictable while the weaknesses in the design of the encryption scheme design gets ignored by the scheme designers. Quite often, while performing key-sensitivity analysis many designers rely on the fact that change at a particular key-bit position generates a completely different cipher image as a sign of key-sensitivity while, ideally, to satisfy avalanche properties, change should be 50% to ensure unpredictability/randomness of the cipher image. Also, the contribution of each bit position of the key in this respect to avalanche properties is many times not accessed thereby leading to overestimation in the size of the key-space.

Largely these chaos-based image encryption schemes have their permutation and substitution stages in such a way that they are not interdependent and therefore cryptanalysis can be performed over such stages cracking one at a time. Further to discuss the most common way of cracking the permutation stage in these image encryption schemes is by identifying the chaotic key-stream used for performing the permutation which can be easily done on the basis of known/chosen plaintext attacks. To elaborate, this is done by observing the position of bit/pixel changed in the cipher image obtained by one bit/pixel change in the chosen plain image and repeating this for all pixel positions in the plain image in order to derive the permutation table. Similarly, the substitution stage also normally involves simple operations like XOR, addition under modulo etc. with the chaotic key-stream and/or previous pixel feedback. Again, the cryptanalyst can easily recover the underlying chaotic key-stream used during the substitution stage by employing known/chosen plaintext attacks. This is done by observing the changes in the cipher image obtained for one bit/pixel change in the chosen plain images having special characteristics like all black image, image having fixed average pixel intensity etc. based on the design of the encryption images repeatedly to derive the substitution key stream used during encryption. Once the underlying chaotic key-streams for permutation and substitution stages are derived, the claim of large key-space to resist cryptanalysis goes in vain. It is important to note that the encryption scheme that employ single or only few fixed number of rounds are particularly weaker as compared to others because there is a much higher scope of reducing such an encryption scheme to an equivalent mathematical model of linear equations which can be solvable in polynomial time. The temptation to make the image encryption schemes computationally less expensive while relying on the properties of chaos, increased the possibility of weaker underlying designs of the scheme. This rationalizes the current day relevance and motivation of cryptanalyzing existing chaos-based image encryption

schemes by trying to reduce them to a solvable equivalent mathematical model with a purpose to identify weak structures in them and replace them with structures offering higher security.

Moving forward in this direction, we cryptanalyzed a new image encryption scheme based on chaos proposed by Zhou et al. [40]. The image encryption algorithm [40] under study, involves use of a new 1D-chaotic system. As per the authors' claim, the proposed chaotic system linearly combines existing chaotic maps to generate maps with more complex chaotic characteristics like more uniform distribution of its density function, chaotic behavior for wider range of parameter values, higher values of lyapunov exponents etc. This encryption algorithm employs five steps namely - Random pixel insertion, Row separation, 1D substitution, Row combination and Image rotation. The chaotic system proposed by the authors is used to generate values which are consumed in the substitution step. It uses five parameters r_0, r_1, r_2, r_3, r_4 along with initial value $S_1(0,0)$ where r_0, r_1, r_2, r_3, r_4 range over (0,4] and $S_1(0,0)$ lie between 0 and 1. These parameters and initial value act as the key for the scheme. Zhou et al. claim that for 14 decimal precision of initial value, the key space for their algorithm is 10^{84} which is sufficiently large to counter brute force attack. On careful analysis, several issues have been identified in the image encryption algorithm under study, which are discussed subsequently in this chapter after giving a brief background and description of the original image encryption scheme.

5.1 DESCRIPTION OF IMAGE ENCRYPTION SCHEME PROPOSED BY ZHOU ET AL.

The image encryption algorithm under study as proposed by Zhou et al. uses a new 1D chaotic system. In fact, the authors proposed three hybrid 1D chaotic systems by linearly combining logistic map $L(r, X_n)$, tent map $T(r, X_n)$ and sine map $S(r, X_n)$, to improve their chaotic behaviors. The definitions of these chaotic systems are as follows:

The Logistic-Tent system

$$X_{n+1} = A_{LT}(r, X_n) = (L(r, X_n) + T((4-r),X_n)) \bmod 1 \quad (10)$$

where parameter $r \in (0,4]$

The Logistic-Sine system

$$X_{n+1} = A_{LS}(r, X_n) = (L(r, X_n) + T((4-r),X_n)) \bmod 1 \quad (11)$$

where parameter $r \in (0,4]$

The Tent-Sine system

$X_{n+1} = A_{TS}(r, X_n) = (T(r, X_n) + S((4-r),X_n)) \bmod 1$ (12)

where parameter $r \in (0,4]$

The authors further use Logistic-Tent system in a new 4-round image encryption algorithm proposed by them. Their scheme involves the following per-round operation steps:

a) *Random pixel insertion*: In this step, a randomly generated pixel is inserted at the beginning of each row of the image thereby changing the image dimension from M×N to M×(N+1). The random values inserted are to be used one-time only.

b) *Row separation:* In this step, the image is divided into M 1D arrays, each corresponding to a row of the original/input image. The 1D matrices are represented as R_i where $1 \leq i \leq M$.

c) *1D substitution:* Here, each of the R_is obtained from the previous step are substituted using the following substitution rule:

$$B_i(j) = \begin{cases} R_i(j) & \text{if } j = 1 \\ B_i(j-1) \oplus R_i(j) \oplus \left(\lfloor S_k(i,j) \times 10^{10} \rfloor \right) \bmod 256 & \text{otherwise} \end{cases} \quad (13)$$

where $\oplus$ represents XOR operation, $\lfloor a \rfloor$ represents floor(a) and $S_k(i,j)$ represents a pseudo-random sequence for the k^{th} round encryption, generated using the Logistic-Tent System with five parameters r_0, r_1, r_2, r_3, r_4 along with initial value $S_1(0,0)$ as the secret key. $S_k(i,j)$ is defined as follows:

$$S_k(i,j) = \begin{cases} S_1(0,0) & i = 0,\ j = 0,\ k = 1 \\ S_2(M,0) & i = 0,\ j = 0,\ k = 3 \\ S_{k-1}(N,0) & i = 0,\ j = 0,\ k = 2,4 \\ A_{LT}(r_0, S_k(i-1,0)) & i > 1,\ j = 0 \\ A_{LT}(r_k, S_k(i,j-1)) & i > 1,\ j > 0 \end{cases} \quad (14)$$

d) *Row combination:* This step clips off the random pixel inserted at the beginning of each row and combines the M 1D row matrices together to form 2D image pixel matrix again.

e) *Image rotation:* The obtained image in the previous step is rotated 90° in counter-clockwise direction in this step.

Image Rotation is the last operation performed in one round of the encryption process. The image obtained after this step forms the input to the next encryption round and the final cipher image is obtained after completion of four encryption rounds.

5.2 ISSUES IDENTIFIED IN ZHOU ET AL. IMAGE ENCRYPTION SCHEME

Following are the issues identified in the definition of Zhou et al. Image Encryption Scheme:

a) The definition of the pseudo-random sequence $S_k(i,j)$ used in 1D substitution step as specified in Eq. (5), does not handle the cases i = 1 and/or j = 1. Since the original definition is a recursive one, not defining $S_k(i,j)$ for i = 1 and/or j = 1 leads to no possible evaluation of $S_k(i,j)$ for subsequent values of i and/or j . So, we suggest a possible correction in this definition as given below:

$$S_k(i,j)=\begin{cases} S_1(0,0) & i=0,\ j=0,\ k=1 \\ S_2(M,0) & i=0,\ j=0,\ k=3 \\ S_{k-1}(N,0) & i=0,\ j=0,\ k=2,4 \\ A_{LT}\left(r_0, S_k(i-1,0)\right) & i>0,\ j=0 \\ A_{LT}\left(r_k, S_k(i,j-1)\right) & i\geq 0,\ j>0 \end{cases} \qquad (15)$$

b) In the definition of Tent map, Logistic-Tent and Tent-Sine systems as a linear combination of seed maps, in the equations for generating X_{n+1} the authors have erroneously specified the definitions over intervals $X_i < 0.5$ and $X_i \geq 0.5$, while apparently the definition should have been over intervals $X_n < 0.5$ and $X_n \geq 0.5$.

c) The permutation step is static and key-independent. Thus it contributes to predictable diffusion and does not contribute anything to enhance confusion in the cipher.

d) The number of rounds is fixed and small, again contributing to decipherable diffusion and confusion.

e) The encryption scheme has substitution-permutation structure which is considered to be a poorer design as compared to permutation-substitution from point of view of key-sensitivity [69].

f) Row-restricted previous pixel feedback in the 1D substitution step as the only measure to percolate changes done in the original image to the cipher image is one more issue. To explain, consider a change in pixel value at location (x,y) in the original image. As 1D substitution step involves previous pixel feedback, and performs substitution in different rows independently, hence, in this round only pixels subsequent to position (x,y) in the same row will get changed. There will be no change in pixels encrypted in other rows or pixels encrypted prior to position (x,y) in the same row. Clearly, in the subsequent rounds also the change percolation will be slow.

g) Another significant issue with the original scheme is the definition of its Random pixel insertion step. In this step it is stated that, using any random number generator, random pixels should be generated and inserted at the beginning of each row. Also, the random values are to be used one-time only to ensure unpredictability in encrypted images. The authors argued that because of Random pixel insertion step the encryption scheme can resist chosen plaintext attacks. They deliberated one-time use of random values as an underlying principle to generate completely random and different images on each encryption even with the same original image and same key. But there is a serious concern in practical feasibility of this one-time use of randomly generated pixels.

Since, the same random pixel values would be required during decryption at the receiver's end hence they should have been included as part of the secret key otherwise the cipher image becomes undecipherable at the receiver's end. But the composition of the secret key has been categorically stated by Zhou et al. in Section 6.1.1 of their work [40]. The secret key defined by the authors has no mention of the random pixels inserted in the per-round encryption process.

Even if it is assumed that the randomly generated pixels are made part of the key, still there is a serious issue. Clearly, for a M×N image, there will be M random pixels inserted in each round, thus, in all, for the four round encryption process 4M random values would be required to be communicated to the receiver as part of the secret key. This is a huge amount of information to be conveyed secretly to the receiver. The problems faced while practically using this encryption scheme will be similar to the ones faced by one-time pad

i.e. safe and secure communication of the key itself will become a huge challenge making it practically infeasible to use the scheme for real-time applications.

Thus, for practical purposes the algorithm will be required to use key-based generation of random values in the Random pixel insertion step instead of one-time used values. In this case the claim of generating a different cipher for the same original image with same key is nullified as same random values will be generated by the same key. Not only this, it is found that the scheme possesses serious weaknesses and cannot resist differential cryptanalysis in this case. It is observed that the claim of the authors on key space as large as 10^{84} is incorrect and in fact, when exposed to differential cryptanalysis the entire plaintext can be recovered without any knowledge regarding the key or equivalent key stream. Following section discusses the details of the differential cryptanalytic attack on the scheme under study.

5.3 Proposed Cryptanalysis Of Zhou et al. Image Encryption Scheme

Özkaynaka et al. [195] proposed a general attack scenario for analyzing security of any chaos based encryption scheme. The authors highlighted that as part of the attack it should be investigated that whether the encryption process can be expressed as a set of simpler mathematical equations so as to uncover any algebraic dependencies that may exist. Though, Özkaynaka et al. proposed the mentioned approach to enhance the security analysis of the encryption schemes while designing them, but it is felt that this attack scenario can be applied to attack existing cryptosystems as well. Extending this logic along with further improvements, we propose cryptanalysis on the image encryption scheme under study [40]. Firstly, an equivalent mathematical model has been formulated by us for the scheme under study, which is followed by differential cryptanalysis of the scheme using this model. Deduction of a mathematical model for the scheme under study and its subsequent cryptanalysis are discussed in detail below.

It is observed that the image encryption scheme under discussion can be visualized essentially as a substitution-permutation cipher because the row separation and row combination operations do not really manipulate the image at all. They are more of cosmetic operations which do not have a significant part to play in the encryption process. Investigation of the scheme reveals that there exist linear relationships among the cipher image pixels and the plain

image pixels. This is because the encryption process involves fixed permutation stage, which is not even key-dependent, followed by a simple XOR operation. These static relationships between the cipher image pixels and the contributing plain image pixels can be represented as a mathematical model using linear equations. To demonstrate the construction of the equivalent mathematical model, for simplicity, an example demonstrating encryption of a small 3×3 plain image is taken first. Following elaborates the construction of the mathematical model comprising of a set of simple linear equations representing cipher image pixels in terms of plain image pixels for a 3×3 image:

Let $I(i,j)$, $R_i(j)$, $B_i(j)$, $CI_i(j)$ represent the $(i,j)^{th}$ pixel of the plain image, input image per round prior to the 1D substitution step, intermediate cipher image per round obtained after 1D substitution step, and final cipher image respectively. Also, let p_i, p_i', p_i'', p_i''' represents key-dependent random pixels inserted in the i^{th} row (i.e. $R_i(1)$) in the 1^{st}, 2^{nd}, 3^{rd}, and 4^{th} rounds respectively. Clearly, for the first round $R_i(j) = I(i,j-1)$ for all i, $j>1$ and $j<=4$. So, on applying encryption process, the intermediate cipher pixels at the end of the first round are:

$B_1(1) = p_1 = a_{11}$

$B_1(2) = p_1 \oplus I(1,1) \oplus (\lfloor S_1(1,2) \times 10^{10} \rfloor) \bmod 256$

$= a_{12} \oplus I(1,1)$

(where, $a_{12} = a_{11} \oplus (\lfloor S_1(1,2) \times 10^{10} \rfloor) \bmod 256$)

$B_1(3) = p_1 \oplus I(1,1) \oplus (\lfloor S_1(1,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(1,2) \oplus (\lfloor S_1(1,3) \times 10^{10} \rfloor) \bmod 256$

$= a_{13} \oplus I(1,1) \oplus I(1,2)$

(where, $a_{13} = a_{12} \oplus (\lfloor S_1(1,3) \times 10^{10} \rfloor) \bmod 256$)

$B_1(4) = p_1 \oplus I(1,1) \oplus (\lfloor S_1(1,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(1,2) \oplus (\lfloor S_1(1,3) \times 10^{10} \rfloor) \bmod 256 \oplus I(1,3) \oplus (\lfloor S_1(1,4) \times 10^{10} \rfloor) \bmod 256$

$= a_{14} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3)$

(where, $a_{14} = a_{13} \oplus (\lfloor S_1(1,4) \times 10^{10} \rfloor) \bmod 256$)

$B_2(1) = p_2 = a_{21}$

$B_2(2) = p_2 \oplus I(2,1) \oplus (\lfloor S_1(2,2) \times 10^{10} \rfloor) \bmod 256$

$= a_{22} \oplus I(2,1)$

(where, $a_{22} = a_{21} \oplus (\lfloor S_1(2,2) \times 10^{10} \rfloor) \bmod 256$)

$B_2(3) = p_2 \oplus I(2,1) \oplus (\lfloor S_1(2,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(2,2) \oplus (\lfloor S_1(2,3) \times 10^{10} \rfloor) \bmod 256$

$= a_{23} \oplus I(2,1) \oplus I(2,2)$

(where, $a_{23} = a_{22} \oplus (\lfloor S_1(2,3) \times 10^{10} \rfloor) \bmod 256$)

$B_2(4) = p_2 \oplus I(2,1) \oplus (\lfloor S_1(2,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(2,2) \oplus (\lfloor S_1(2,3) \times 10^{10} \rfloor) \bmod 256 \oplus$
$I(2,3) \oplus (\lfloor S_1(2,4) \times 10^{10} \rfloor) \bmod 256$

$= a_{24} \oplus I(2,1) \oplus I(2,2) \oplus I(2,3)$

(where, $a_{24} = a_{23} \oplus (\lfloor S_1(2,4) \times 10^{10} \rfloor) \bmod 256$)

$B_3(1) = p_3 = a_{31}$

$B_3(2) = p_3 \oplus I(3,1) \oplus (\lfloor S_1(3,2) \times 10^{10} \rfloor) \bmod 256$

$= a_{32} \oplus I(3,1)$

(where, $a_{32} = a_{31} \oplus (\lfloor S_1(3,2) \times 10^{10} \rfloor) \bmod 256$)

$B_3(3) = p_3 \oplus I(3,1) \oplus (\lfloor S_1(3,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(3,2) \oplus (\lfloor S_1(3,3) \times 10^{10} \rfloor) \bmod 256$

$= a_{33} \oplus I(3,1) \oplus I(3,2)$

(where, $a_{33} = a_{32} \oplus (\lfloor S_1(3,3) \times 10^{10} \rfloor) \bmod 256$)

$B_3(4) = p_3 \oplus I(3,1) \oplus (\lfloor S_1(3,2) \times 10^{10} \rfloor) \bmod 256 \oplus I(3,2) \oplus (\lfloor S_1(3,3) \times 10^{10} \rfloor) \bmod 256 \oplus$
$I(3,3) \oplus (\lfloor S_1(3,4) \times 10^{10} \rfloor) \bmod 256$

$= a_{34} \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

(where, $a_{34} = a_{33} \oplus (\lfloor S_1(3,4) \times 10^{10} \rfloor) \bmod 256$)

After clipping off the first column and rotating 90° in counter-clockwise direction, the input for the second round 1D substitution step becomes:

$R_1(1) = p_1'$

$R_1(2) = B_1(4) = a_{14} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3)$

$R_1(3) = B_2(4) = a_{24} \oplus I(2,1) \oplus I(2,2) \oplus I(2,3)$

$R_1(4) = B_3(4) = a_{34} \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

$R_2(1) = p_2'$

$R_2(2) = B_1(3) = a_{13} \oplus I(1,1) \oplus I(1,2)$

$R_2(3) = B_2(3) = a_{23} \oplus I(2,1) \oplus I(2,2)$

$R_2(4) = B_3(3) = a_{33} \oplus I(3,1) \oplus I(3,2)$

$R_3(1) = p_3'$

$R_3(2) = B_1(2) = a_{12} \oplus I(1,1)$

$R_3(3) = B_2(2) = a_{22} \oplus I(2,1)$

$R_3(4) = B_3(2) = a_{32} \oplus I(3,1)$

Calculating the new value of Bs as per second round of encryption, we get:

$B_1(1) = R_1(1) = p_1' = b_{11}$

$B_1(2) = B_1(1) \oplus R_1(2) \oplus (\lfloor S_2(1,2) \times 10^{10} \rfloor) \bmod 256$

$= p_1' \oplus a_{14} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus (\lfloor S_2(1,2) \times 10^{10} \rfloor) \bmod 256$

$= b_{12} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3)$

(where, $b_{12} = b_{11} \oplus a_{14} \oplus (\lfloor S_2(1,2) \times 10^{10} \rfloor) \bmod 256$)

$B_1(3) = B_1(2) \oplus R_1(3) \oplus (\lfloor S_2(1,3) \times 10^{10} \rfloor) \bmod 256$

$= b_{12} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus a_{24} \oplus I(2,1) \oplus I(2,2) \oplus I(2,3) \oplus (\lfloor S_2(1,3) \times 10^{10} \rfloor) \bmod 256$

$= b_{13} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3)$

(where, $b_{13} = b_{12} \oplus a_{24} \oplus (\lfloor S_2(1,3) \times 10^{10} \rfloor) \bmod 256$)

$B_1(4) = B_1(3) \oplus R_1(4) \oplus (\lfloor S_2(1,4) \times 10^{10} \rfloor) \bmod 256$

$= b_{13} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3) \oplus a_{34} \oplus I(3,1) \oplus I(3,2) \oplus I(3,3) \oplus (\lfloor S_2(1,4) \times 10^{10} \rfloor) \bmod 256$

$= b_{14} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3) \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

(where, $b_{14} = b_{13} \oplus a_{34} \oplus (\lfloor S_2(1,4) \times 10^{10} \rfloor) \bmod 256$)

$B_2(1) = R_2(1) = p_2' = b_{21}$

$B_2(2) = B_2(1) \oplus R_2(2) \oplus (\lfloor S_2(2,2) \times 10^{10} \rfloor) \bmod 256$

$= b_{21} \oplus a_{13} \oplus I(1,1) \oplus I(1,2) \oplus (\lfloor S_2(2,2) \times 10^{10} \rfloor) \bmod 256$

$= b_{22} \oplus I(1,1) \oplus I(1,2)$

(where, $b_{22} = b_{21} \oplus a_{13} \oplus (\lfloor S_2(2,2) \times 10^{10} \rfloor) \bmod 256$)

$B_2(3) = B_2(2) \oplus R_2(3) \oplus (\lfloor S_2(2,3) \times 10^{10} \rfloor) \bmod 256$

$= b_{22} \oplus I(1,1) \oplus I(1,2) \oplus a_{23} \oplus I(2,1) \oplus I(2,2) \oplus (\lfloor S_2(2,3) \times 10^{10} \rfloor) \bmod 256$

$= b_{23} \oplus I(1,1) \oplus I(1,2) \oplus I(2,1) \oplus I(2,2)$

(where, $b_{23} = b_{22} \oplus a_{23} \oplus (\lfloor S_2(2,3) \times 10^{10} \rfloor) \bmod 256$)

$B_2(4) = B_2(3) \oplus R_2(4) \oplus (\lfloor S_2(2,4) \times 10^{10} \rfloor) \bmod 256$

$= b_{23} \oplus I(1,1) \oplus I(1,2) \oplus I(2,1) \oplus I(2,2) \oplus a_{33} \oplus I(3,1) \oplus I(3,2) \oplus (\lfloor S_2(2,4) \times 10^{10} \rfloor)$ mod 256

$= b_{24} \oplus I(1,1) \oplus I(1,2) \oplus I(2,1) \oplus I(2,2) \oplus I(3,1) \oplus I(3,2)$

(where, $b_{24} = b_{23} \oplus a_{33} \oplus (\lfloor S_2(2,4) \times 10^{10} \rfloor)$ mod 256)

$B_3(1) = R_3(1) = p_3' = b_{31}$

$B_3(2) = B_3(1) \oplus R_3(2) \oplus (\lfloor S_2(3,2) \times 10^{10} \rfloor)$ mod 256

$= b_{31} \oplus a_{12} \oplus I(1,1) \oplus (\lfloor S_2(3,2) \times 10^{10} \rfloor)$ mod 256

$= b_{32} \oplus I(1,1)$

(where, $b_{32} = b_{31} \oplus (\lfloor S_2(3,2) \times 10^{10} \rfloor)$ mod 256)

$B_3(3) = B_3(2) \oplus R_3(3) \oplus (\lfloor S_2(3,3) \times 10^{10} \rfloor)$ mod 256

$= b_{32} \oplus I(1,1) \oplus a_{22} \oplus I(2,1) \oplus (\lfloor S_2(3,3) \times 10^{10} \rfloor)$ mod 256

$= b_{33} \oplus I(1,1) \oplus I(2,1)$

(where, $b_{33} = b_{32} \oplus a_{22} \oplus (\lfloor S_2(3,3) \times 10^{10} \rfloor)$ mod 256)

$B_3(4) = B_3(3) \oplus R_3(4) \oplus (\lfloor S_2(3,4) \times 10^{10} \rfloor)$ mod 256

$= b_{33} \oplus I(1,1) \oplus I(2,1) \oplus a_{32} \oplus I(3,1) \oplus (\lfloor S_2(3,4) \times 10^{10} \rfloor)$ mod 256

$= b_{34} \oplus I(1,1) \oplus I(2,1) \oplus I(3,1)$

(where, $b_{34} = b_{33} \oplus a_{32} \oplus (\lfloor S_2(3,4) \times 10^{10} \rfloor)$ mod 256)

After clipping off the first column and rotating 90° in counter-clockwise direction, the input for the third round 1D substitution becomes:

$R_1(1) = p_1''$

$R_1(2) = B_1(4) = b_{14} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3) \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

$R_1(3) = B_2(4) = b_{24} \oplus I(1,1) \oplus I(1,2) \oplus I(2,1) \oplus I(2,2) \oplus I(3,1) \oplus I(3,2)$

$R_1(4) = B_3(4) = b_{34} \oplus I(1,1) \oplus I(2,1) \oplus I(3,1)$

$R_2(1) = p_2''$

$R_2(2) = B_1(3) = b_{13} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3)$

$R_2(3) = B_2(3) = b_{23} \oplus I(1,1) \oplus I(1,2) \oplus I(2,1) \oplus I(2,2)$

$R_2(4) = B_3(3) = b_{33} \oplus I(1,1) \oplus I(2,1)$

$R_3(1) = p_3''$

$R_3(2) = B_1(2) = b_{12} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3)$

$R_3(3) = B_2(2) = b_{22} \oplus I(1,1) \oplus I(1,2)$

$R_3(4) = B_3(2) = b_{32} \oplus I(1,1)$

Similar calculations for the third and fourth round transforming values for $B_i(j)$ in respective rounds show that during diffusion in the encryption process, at several occasions the same original image pixel, say I(s,t), gets XORed twice while contributing to an intermediate cipher image pixel. This nullifies the contribution of I(s,t) completely in the cipher image pixel. After complete encryption process, the final cipher image can be represented as the following set of linear equations:

$CI_1(1) = B_1(4) = d_{14} \oplus I(3,3) \oplus I(3,1) \oplus I(1,3) \oplus I(1,1)$

$CI_1(2) = B_2(4) = d_{24} \oplus I(3,3) \oplus I(1,3)$

$CI_1(3) = B_3(4) = d_{34} \oplus I(3,1) \oplus I(3,2) \oplus I(3,3) \oplus I(1,1) \oplus I(1,2) \oplus I(1,3)$

$CI_2(1) = B_1(3) = d_{13} \oplus I(3,3) \oplus I(3,1)$

$CI_2(2) = B_2(3) = d_{23} \oplus I(3,3)$

$CI_2(3) = B_3(3) = d_{33} \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

$CI_3(1) = B_1(2) = d_{12} \oplus I(1,3) \oplus I(2,3) \oplus I(3,3) \oplus I(1,1) \oplus I(2,1) \oplus I(3,1)$

$CI_3(2) = B_2(2) = d_{22} \oplus I(1,3) \oplus I(2,3) \oplus I(3,3)$

$CI_3(3) = B_3(2) = d_{32} \oplus I(1,1) \oplus I(1,2) \oplus I(1,3) \oplus I(2,1) \oplus I(2,2) \oplus I(2,3) \oplus I(3,1) \oplus I(3,2) \oplus I(3,3)$

From the above set of linear equations it is evident that the cipher image pixels are contributed by non-uniform number of plain image pixels. Some cipher image pixel gets contributed by only one plain image pixel, some other get contributed by two plain image pixels and so on. This non-uniformity in contribution of plain image pixels to cipher image pixels is targeted by us during cryptanalysis, whose details are discussed below.

After obtaining the equivalent mathematical model for the encryption scheme, now, we demonstrate differential cryptanalysis to retrieve the original plain image. Consider two 3×3 images I_1 and I_2, where image I_1 is composed of all zero pixels and I_2 refers to the image which is required to be completely retrieved through cryptanalysis. As part of the differential cryptanalysis, we XOR the cipher images corresponding to the two images I_1 and I_2 pixel by pixel to get the differential image ΔCI. Clearly, the cipher image pixel at position (2,2) depends only on plain image pixel at position (3,3), therefore retrieving it is trivial from the differential image ΔCI. Further, we define linear equations to calculate other pixel values of the original plain image, using the previously derived mathematical model of the cipher image. The detailed calculations for retrieving all other pixel values of the original plain image I_2 are as given below:

$$\Delta CI_2(2) = d_{23} \oplus I_1(3,3) \oplus d_{23} \oplus I_2(3,3)$$

$$= I_2(3,3) \quad (\because I_1(3,3) = 0)$$

$$\Delta CI_1(2) \oplus I_2(3,3) = d_{24} \oplus I_1(3,3) \oplus I_1(1,3) \oplus d_{24} \oplus I_2(3,3) \oplus I_2(1,3) \oplus I_2(3,3)$$

$$= I_2(1,3) \quad (\because I_1(1,3) = I_1(3,3) = 0)$$

$$\Delta CI_3(2) \oplus I_2(1,3) \oplus I_2(3,3)$$

$$= d_{22} \oplus I_1(1,3) \oplus I_1(2,3) \oplus I_1(3,3) \oplus d_{22} \oplus I_2(1,3) \oplus I_2(2,3) \oplus I_2(3,3) \oplus I_2(1,3) \oplus I_2(3,3) = I_2(2,3)$$

$$(\because I_1(1,3) = I_1(2,3) = I_1(3,3) = 0)$$

$$\Delta CI_2(1) \oplus I_2(3,3)$$

$$= d_{13} \oplus I_1(3,3) \oplus I_1(3,1) \oplus d_{13} \oplus I_2(3,3) \oplus I_2(3,1) \oplus I_2(3,3) = I_2(3,1) \quad (\because I_1(3,1) = I_1(3,3) = 0)$$

$$\Delta CI_2(3) \oplus I_2(3,1) \oplus I_2(3,3)$$

$$= d_{33} \oplus I_1(3,1) \oplus I_1(3,2) \oplus I_1(3,3) \oplus d_{33} \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3) \oplus I_2(3,1) \oplus I_2(3,3)$$

$$= I_2(3,2) \quad (\because I_1(3,1) = I_1(3,2) = I_1(3,3) = 0)$$

$$\Delta CI_1(1) \oplus I_2(3,3) \oplus I_2(3,1) \oplus I_2(1,3)$$

$$= d_{14} \oplus I_1(3,3) \oplus I_1(3,1) \oplus I_1(1,3) \oplus I_1(1,1) \oplus d_{14} \oplus I_2(3,3) \oplus I_2(3,1) \oplus I_2(1,3) \oplus I_2(1,1) \oplus I_2(3,3) \oplus I_2(3,1) \oplus I_2(1,3)$$

$= I_2(1,1)$ ($\because I_1(1,1) = I_1(1,3) = I_1(3,1) = I_1(3,3) = 0$)

$\Delta CI_1(3) \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(1,3)$

$= d_{34} \oplus I_1(3,1) \oplus I_1(3,2) \oplus I_1(3,3) \oplus I_1(1,1) \oplus I_1(1,2) \oplus I_1(1,3) \oplus d_{34} \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(1,2) \oplus I_2(1,3) \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(1,3)$

$= I_2(1,2)$ ($\because I_1(1,1) = I_1(1,2) = I_1(1,3) = I_1(3,1) = I_1(3,2) = I_1(3,3) = 0$)

$\Delta CI_3(1) \oplus I_2(1,3) \oplus I_2(2,3) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(3,1)$

$= d_{12} \oplus I_1(1,3) \oplus I_1(2,3) \oplus I_1(3,3) \oplus I_1(1,1) \oplus I_1(2,1) \oplus I_1(3,1) \oplus d_{12} \oplus I_2(1,3) \oplus I_2(2,3) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(2,1) \oplus I_2(3,1) \oplus I_2(1,3) \oplus I_2(2,3) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(3,1)$

$= I_2(2,1)$ ($\because I_1(1,1) = I_1(1,3) = I_1(2,1) = I_1(2,3) = I_1(3,1) = I_1(3,3) = 0$)

$\Delta CI_3(3) \oplus I_2(1,1) \oplus I_2(1,2) \oplus I_2(1,3) \oplus I_2(2,1) \oplus I_2(2,3) \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3)$

$= d_{32} \oplus I_1(1,1) \oplus I_1(1,2) \oplus I_1(1,3) \oplus I_1(2,1) \oplus I_1(2,2) \oplus I_1(2,3) \oplus I_1(3,1) \oplus I_1(3,2) \oplus I_1(3,3) \oplus d_{32} \oplus I_2(1,1) \oplus I_2(1,2) \oplus I_2(1,3) \oplus I_2(2,1) \oplus I_2(2,2) \oplus I_2(2,3) \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3) \oplus I_2(1,1) \oplus I_2(1,2) \oplus I_2(1,3) \oplus I_2(2,1) \oplus I_2(2,3) \oplus I_2(3,1) \oplus I_2(3,2) \oplus I_2(3,3)$

$= I_2(2,2)$ ($\because I_1(1,1) = I_1(1,2) = I_1(1,3) = I_1(2,1) = I_1(2,2) = I_1(2,3) = I_1(3,1) = I_1(3,2) = I_1(3,3) = 0$)

Though, the differential cryptanalysis is demonstrated on a 3×3 image, it is apparent that the differential image of any dimension M×N can be represented as a set of M.N linear equations which are solvable in $O((M.N)^3)$ time. In fact, faster methods also exist in literature for solving set of linear equations [228]. Clearly, for reasonable sized images, $O((M.N)^3)$ time is much smaller than the high security claim of the authors regarding key-space as large as 10^{84}.

Now, we propose a method to cryptanalyse any general M×N cipher image encrypted by the scheme under study. As earlier, a differential attack is used to retrieve the complete plain image without any requirement of knowledge regarding the key. Following are the steps to perform cryptanalysis, where we make use of O(M.N) chosen plain images and a differential image ΔCI obtained by XORing the cipher of plain black image C_0 with the cipher image C (of the plain image to be recovered) :

i) Firstly, the cipher image for all zero pixels is obtained, say C_0.

ii) Calculate the differential image $\Delta CI = C \oplus C_0$, where C is the cipher image under attack (to retrieve the corresponding plain image I).

iii) Construct M.N plain images, say I_{ij} ($1 \leq i \leq M$ and $1 \leq j \leq N$) with all pixels as zeros except for one pixel in each image I_{ij}, i.e. the pixel at position (i,j) which is given value 1. Then, obtain the corresponding cipher images C_{ij}.

iv) For each $1 \leq i \leq M$ and $1 \leq j \leq N$, compare C_0 and C_{ij} to identify all the pixel positions (i', j') where $C_0(i', j') \neq C_{ij}(i', j')$ ($1 \leq i' \leq M$ and $1 \leq j' \leq N$) and construct information sets *Contribution_To* and *Contributed_By* for each pixel position. $Contributed\_By_{i',j'}$ is a set of positions (i,j)s such that cipher image pixel at position (i',j') gets contributed by plain image pixels at all pixel positions (i,j)s. $Contribution\_To_{i,j}$ is a set of positions (i',j')s such that plain image pixel at position (i,j) gives contribution to all pixel positions (i',j')s in the cipher image.

v) Using the information obtained in *Contributed_By*, identify the position (s',t') which is contributed by a single plain image pixel at position say (s,t). So, the pixel at position (s',t') in the differential image is the plain image pixel at position (s,t) i.e. $I(s,t) = \Delta CI(s',t')$. So, one plain image pixel is recovered.

vi) Now, using the information contained in *Contribution_To* for position (s,t) identify the other positions in (differential) cipher image, say (q',r'), to which plain image pixel I(s,t) contributes to. Then, perform XOR of I(s,t) with each such $\Delta CI(q',r')$ to nullify contribution of I(s,t). Also, using information in *Contributed_By* check if $\Delta CI(q',r')$ was being contributed by only 2 plain image pixels such that by performing the XOR operation with I(s,t) another plain image pixel, say I(q,r), has been recovered whose location (q,r) is again be identified using *Contributed_By* for position (q',r').

vii) Continue performing the previous step (step vi) to recover plain image pixels using cipher image pixels being contributed by 3, 4 , 5 … plain image pixels (in this order) till entire plain image is recovered.

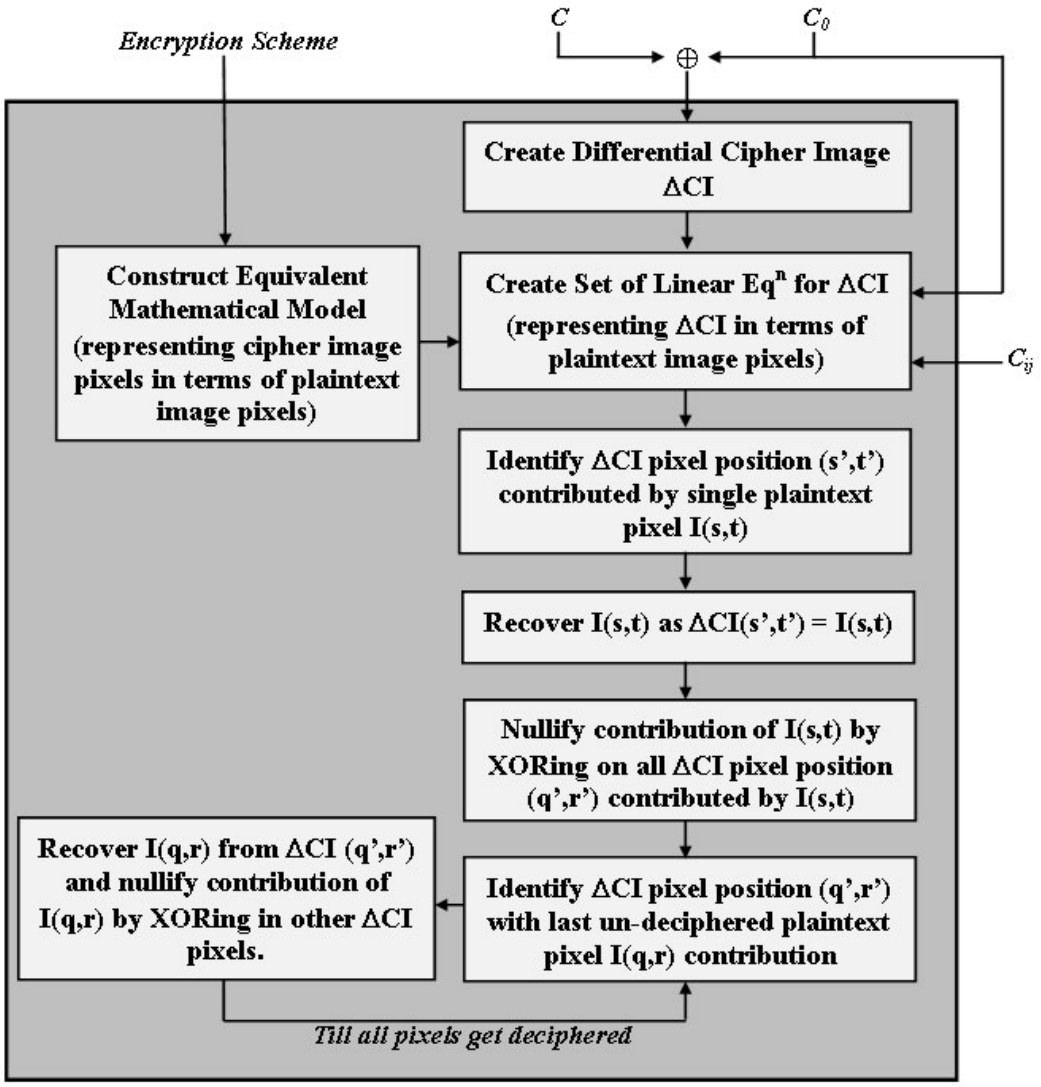


Fig. 57 Block Diagram for Proposed Cryptanalysis of Zhou et al. Image Encryption Scheme for M×N image

The above figure Fig. 57 displays outline for the proposed cryptanalysis of M×N image. For better clarity and smooth implementation, following is the algorithm/pseudo-code used for cryptanalyzing any general M×N image:

ALGORITHM 8: Cryptanalysis Algorithm

INPUT: M (height), N (width), C_{ij} (for $1 \le i \le M$ and $1 \le j \le N$; cipher for all black image with i,j^{th} pixel as 1), C_0 (cipher for plain black image), C (cipher image corresponding to plain image to be recovered)

1: **for** i = 1: M

2: **for** j = 1: N

3: $\Delta CI(i,j) = C(i,j) \oplus C_0(i,j)$;

```
4:          is_pixel_deciphered(i,j) = 0;
5:      end for
6:   end for
7:   v=1;
8:   for i' = 1: M
9:       for j' = 1: N
10:           contributed_by_{i',j'} = Ø;
11:           contributed_by_count(v,1) = 0;
12:           contributed_by_count(v,2) = i';
13:           contributed_by_count(v,3) = j';
14:           contributed_by_pixels_accounted(i',j') = 0;
15:           v = v+1;
16:      end for
17: end for
18: u=1;
19: for i = 1: M
20:    for j = 1: N
21:       contribution_to_{ij} =  Ø;
22:       contribution_to_count(u,1) = 0;
23:       contribution_to_count(u,2) = i;
24:       contribution_to_count(u,3) = j;
25:       v=1;
26:       for i' = 1: M
27:           for j' = 1: N
28:              if (C_{ij} (i',j') ≠ C_0 (i',j')) then
29:                 contribution_to_{ij} = contribution_to_{ij} ∪ {(i',j')};
30:                 contribution_to_count(u,1) = contribution_to_count(u,1) + 1;
31:                 contributed_by_{i',j'} = contributed_by_{i',j'} ∪ {(i,j)};
32:                 contributed_by_count(v,1) = contributed_by_count(v,1) + 1;
33:              end if
34:              v = v+1;
35:           end for
36:       end for
37:       u = u+1;
38:    end for
39: end for
40: contributed_by_count_sorted = sort_by_count (contributed_by_count);
41: s' = contributed_by_count_sorted (1,2);
42: t' = contributed_by_count_sorted (1,3);
```

```
43: [s,t] = retrieve_next_pixel_position_from_set(contributed_by_s't');
44: deciphered_image (s,t) = ΔCI(s',t');
45: Q = Ø;
46: is_pixel_deciphered(s,t) = 1;
47: contributed_by_pixels_accounted(s',t') = contributed_by_pixels_accounted(s',t') + 1;
48: deciphered_pixel_count = 1;
49: enqueue(Q,(s,t));
50: while (deciphered_pixel_count < M*N)
51:    [s,t] = dequeue(Q);
52:    x = (s-1)*width+t;
53:    for z = 1:contribution_to_count(x,1)
54:          [q',r'] = retrieve_next_pixel_position_from_set(contribution_to_s,t);
55:          ΔCI(q',r') = ΔCI(q',r') ⊕ deciphered_image(s,t);
56:          contributed_by_pixels_accounted(q',r') = contributed_by_pixels_accounted(q',r') + 1;
57:         x1=(q'-1)*width+r';
58:         if (contributed_by_pixels_accounted(q',r') == contributed_by_count (x1, 1)-1) then
59:           [q,r] = retrieve_last_contributing _pixel_position(q',r');
60:           deciphered_image(q, r) = ΔCI(q',r');
61:           is_pixel_deciphered(q, r) = 1;
62:           deciphered_pixel_count = deciphered_pixel_count+1;
63:           enqueue(Q,(q,r));
64:        end if
65:     end for
66: end while
```

The above algorithm represents the cryptanalysis method to retrieve a general M×N image from its cipher. It uses data structure set for representing 'Contribution_to' and 'Contributed by' information for each pixel position. And, data structure queue is used to record the list of newly deciphered plain image pixel positions (whose contribution in cipher image pixels is not yet nullified by XORing) at any instant of time. Values at these newly deciphered pixel positions are further used one by one to decipher more plain image pixels subsequently. The *enqueue* and *dequeue* operations are same as normal queue operations. The operation *retrieve_next_pixel_position_from_set(A)* is an operation on set A to retrieve the next pixel position (which is not already read) belonging to the set A. And, the operation *retrieve_last_contributing_pixel_position(x',y')* searches the position of the last un-deciphered pixel position (say (x,y)) contributing in (differential) cipher pixel at position (x',y')). This operation uses information contained in the set Contributed_by$_{x',y'}$ to find the last pixel position

(of the original image contributing in cipher pixel position (x',y')) remaining un-deciphered in this set.

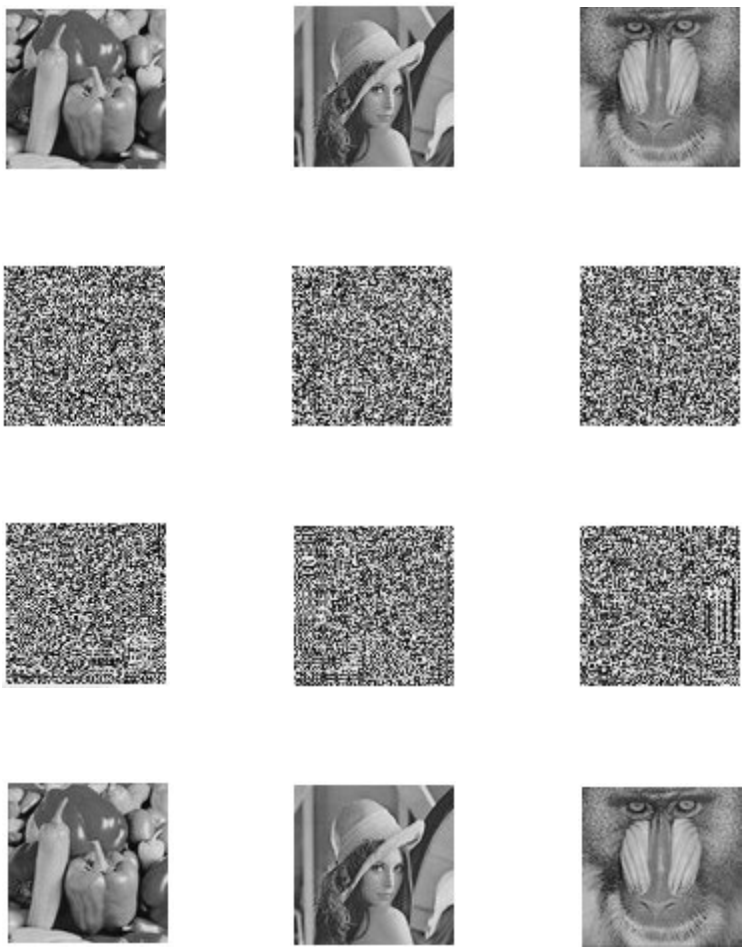
It is evident that as the proposed cryptanalysis algorithm does not make any assumption about pixel values in the original plain image I, hence, the proposed work can retrieve any M×N plain image completely from its corresponding cipher image without knowledge regarding the key. Further, clearly, the time complexity for deriving the equivalent set of linear equations (for M×N cipher image), is dependent on the time complexity of generation of sets Contribution_To and Contributed_By. This is $(O(M.N)^3)$ as we have used O(M.N) chosen plain imagess and against each chosen plain image a comparison $C_0(i', j') \neq C_{ij}(i', j')$ is made, for every i' and j', where $1 \leq i' \leq M$ and $1 \leq j' \leq N$. Further, to finally decipher pixels, Contributed_by is referred to find (differential) cipher image pixel position having contribution from 1, 2, 3 ….. plain image pixels (in this order) till entire plain image is recovered. To fasten this step, a separate field to capture count of contributing plain image pixels is maintained. Sorting is performed on this count field using linear time algorithm like radix sort. Thus, choosing (differential) cipher image pixel position in the said sequential order takes O(M.N) time. Further, for each deciphered pixel corresponding Contribution_to information is looked into to perform XOR operation to decipher more plain image pixels, which is again $O((M.N)^2)$, making overall time complexity of deciphering of entire plain image to be $O((M.N)^3)$.

5.4 OBSERVATIONS FOR THE PROPOSED CRYPTANALYSIS OF ZHOU ET AL. IMAGE ENCRYPTION SCHEME

Experimental verification has been done to strengthen our claims of successful cryptanalysis of a general M×N cipher image encrypted using the image encryption algorithm proposed by Zhou et al. The original image encryption algorithm and our proposed cryptanalysis are implemented on a machine with Windows 7 32-bit operating system with an Intel® core™ 2Duo CPU @ 2.00GHz and 4GB RAM using MATLAB R2011a. MATLAB is chosen for implementation of the attack because it is generally found suitable and convenient for processing images.

The method proposed in the previous section, to represent M×N cipher image as a set of linear equations and to achieve successful differential attack, requires creation and use of *Contribution_To* and *Contributed_By* information sets. For this we use (M.N)×(M.N) matrices

in our implementation requiring $O((M.N)^2)$ memory space. Use of dynamic data structures like sparse matrix implemented using linked-list approach could have provided more memory efficient implementations but as MATLAB does not have a direct support for such dynamic structures, hence, normal 2D matrices were chosen instead. Due to memory limitations, we limited the verification of the proposed attack on grayscale images of size 32×32, 64×64 and 80×80, but the attack is valid for any M×N sized image as the proposed cryptanalysis algorithm does not make any assumptions on the image size. Following figure Fig. 58 (a), (b) and (c) displays the 80×80 original grayscale plain image, corresponding encrypted images, differential images and recovered images (obtained after proposed differential cryptanalysis) of standard Peppers, Water Lilies and Lena images respectively.



(a) (b) (c)

Fig. 58 Original Grayscale plain image (row 1), corresponding encrypted images (row 2), differential images (row 3) and recovered images obtained after proposed differential cryptanalysis (row 4) (a) Peppers, (b) Lena, (c) Baboon

The observations of the experimental verification show that, in agreement with our claims, the proposed cryptanalysis is able to experimentally recover the complete plain image without requirement of any knowledge regarding the key.

5.5 Proposed Suggestions for Improvements In Zhou et al. Scheme & Security Analysis

5.5.1 Proposed Improvements

As stated earlier, the image encryption scheme under study relies completely on the improved properties of the hybrid chaotic system and use of one-time pad like random pixel insertion. One-time use of values during Random pixel insertion step is not practically feasible as it requires 4M bytes of information to be transmitted securely to the receiver to ensure possible decryption, where M is the number of rows of the image being encrypted. Further, complete reliance on chaotic properties with very few rounds of encryption to ensure strength is a major weakness. While focusing more on better chaotic properties of the used hybrid chaotic system, the authors neglected verification about whether the scheme possesses desired confusion, diffusion properties and this is what has been exploited in our proposed differential cryptanalysis. To overcome the weakness and other flaws in the system as highlighted in Section 5.2, following are some suggestions to improve the overall strength of the image encryption algorithm proposed by Zhou et al. [40]:

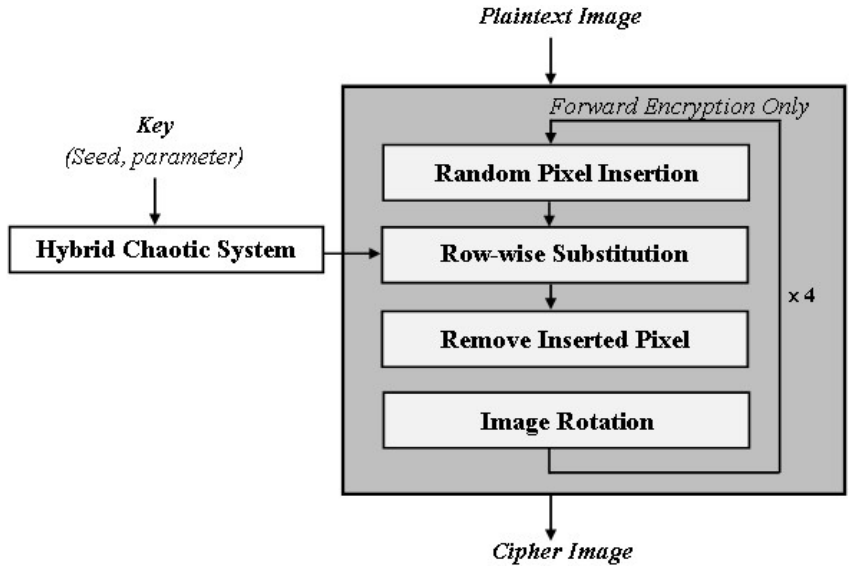
1. Use of key and plaintext dependent permutation stage [182], [187], [229], [230] instead of Image rotation step and performing it prior to the substitution stage to make it a permutation-substitution design instead of a weaker substitution-permutation one [69].

2. Key-dependence of number of rounds [231] can also be introduced, with some lower and upper limit as per resource availability and security requirements, to resist theoretical reduction of the scheme to equivalent mathematical model.

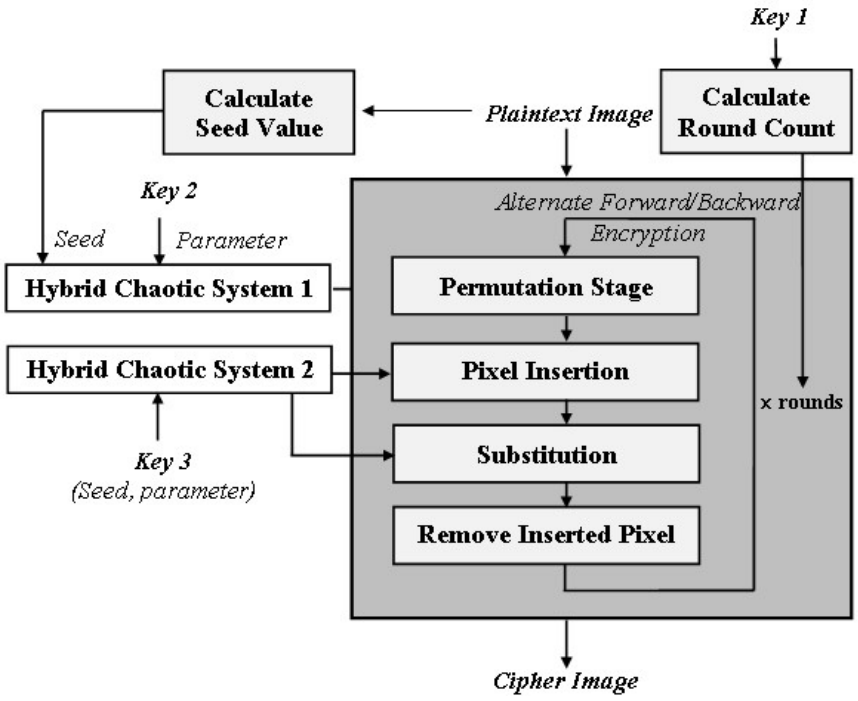
3. Further, to enhance diffusion properties in lesser number of rounds, alternate forward and backward/reverse encryption [230], [232] of image can be used, i.e. from first pixel to last and last to first, in subsequent rounds instead of only forward encryption.

4. The substitution stage should be defined to include inter-row feedback instead of performing substitution on rows independent of each other.

For a clearer comparison, the following figure Fig. 59 (a) and (b) presents the block diagram for the design of Zhou et al. Image Encryption Scheme and the modified Zhou et al. scheme with our proposed improvements respectively.



(a)



(b)

Fig. 59 Block Diagram (a) Zhou et al. Image Encryption Scheme, (b) Modified Zhou et al. Scheme with our proposed improvements

5.5.2 Security Analysis of the modified scheme Zhou et al. with Proposed Improvements

We now present an analysis of the strength of the scheme with proposed improvements. Instead of one fixed permutation through 90° counter-clockwise image rotation at the end of each round, introduction of a k-bit key-dependent chaotic permutation stage along with plaintext dependent seed value of chaotic map, performed at the start of each round will ensure that there will be 2^k different dynamically changing permutation vectors possible instead of one. This will make the scheme resistant against theoretical reduction to a fixed mathematical model of linear equations. This is because as per the original definition, the fixed 90° counter-clockwise image rotation step was contributing only in diffusing the cipher image but that diffusion was fixed which we exploited to reduce the scheme to a set of easily solvable linear equations. But, with our proposed improvement, the key and plaintext dependent permutation stage will contribute to confusion as well as unpredictable diffusion. This makes it infeasible to theoretically reduce the scheme in a set of linear equations by the attacker in absence of the key and also makes the scheme resistant against known/chosen plaintext attacks. This modification also improves the design from a weaker substitution-permutation structure to a more key-sensitive permutation-substitution structure.

Further, we also suggested key-dependent round count to add to the difficulty of theoretical cryptanalysis. By doing this, now the attacker will be unaware of the number of rounds of encryption operations performed to generate the cipher. This will all the more make it difficult to construct a mathematical model for the scheme with intent to break it. Further, as both the above mentioned improvements involve key-dependency, hence, key-space also increases thereby strengthening the scheme against brute-force attacks as well.

Also, as stated in Section 5.2, due to previous pixel feedback restricted within a row, change percolation rate is not significant. To overcome this design issue, another suggested improvement is to perform forward and backward encryption in alternate rounds along with the substitution stage that include inter-row feedback. This improvement along with key and plaintext dependent permutation stage will ensure that any minor change in any pixel of the image gets diffused across the complete cipher image affecting each and every pixel, in maximum two rounds due to forward and backward encryption in alternative rounds.

5.6 CONCLUDING REMARKS

This chapter covered our study on an image encryption algorithm proposed by Zhou et al. [40] and following are the weaknesses identified in the algorithm:

- Improper definition of the chaotic pseudo-random sequence generator function used in substitution step.
- Mistakes in the definition of the tent map and 1D chaotic system using tent map as one of the seed maps.
- Static permutation achieved using fixed 90° rotation in counter-clockwise direction at the end of each round contributes nothing to overall confusion as this step is key-independent.
- Use of fixed four number of rounds is very less to achieve desired confusion-diffusion properties,
- Weaker substitution-permutation design of the scheme.
- Due to row restricted previous pixel feedback, change percolation rate is not significant.
- One-time use of random values used in pixel insertion step is infeasible. If for practical viability, the one-time use condition is dropped, the cipher design is found to be too weak to resist cryptanalysis.

Keeping the weaknesses in mind, cryptanalysis was attempted successfully with key-dependent random pixel insertion. The claim of cipher's high strength against brute-force attack as a result of key-space as large as 10^{84}, proves to be shallow in this case, as we are able to demonstrate a differential plaintext attack which could recover the entire plain image with no knowledge regarding the secret key. It is shown that in general, any M×N cipher image can be reduced to a set of M.N linear equations solvable in $O((M.N)^3)$ time as any set of n-linear equations is solvable in $O(n^3)$ time. For simplicity, firstly a mathematical demonstration is given to explain the attack on a 3×3 image. It demonstrates that the entire original image can be recovered back using just a single differential image (obtained by XORing the cipher image with the cipher image of all zero pixel plain image). Further, for cryptanalysis of a general M×N image, we propose a method to automate representation of M×N cipher image as a set of linear equations using O(M.N) chosen plain images. Further, we describe how to retrieve the entire plain image through an automated differential attack. Algorithm for constructing the said mathematical

model and performing cryptanalysis of a general M×N image is also provided. The proposed cryptanalysis approach is verified experimentally and the results on 32×32, 64×64 and 80×80 images show complete recovery of original plain image without any knowledge regarding the secret key or the equivalent key-stream. This shows poor confusion and diffusion characteristics of the image encryption scheme under study because the differential image is proved to be completely independent of the key. Also, as the differential cipher image is found to be independent of the key, hence the cryptanalysis will be successful irrespective of the chaotic map (among the three hybrid chaotic systems proposed by Zhou et al. or any other) used to generate key stream in the substitution step.

Further, to overcome the above stated weaknesses we propose some improvements like key and plaintext dependent permutation stage instead of a mere fixed rotation, permutation-substitution structure instead of substitution-permutation one, key-dependent number of rounds, alternate forward/backward encryption and inter-row feedback in substitution stage. Security analysis of the improved scheme is also presented to demonstrate enhancement of strength over the existing encryption scheme proposed by Zhou et al.

In future, based on the suggestions provided in Section 5.5, a new image encryption scheme will be developed along with its theoretical, statistical, and experimental security analysis to demonstrate its strength over the existing Zhou et al. scheme [40]. Also, more existing encryption schemes for visual content will be identified which possess the scope to be modeled as system of equations, with an intent to cryptanalyze them by solving the obtained set of equations. This can unfold loop-holes in such schemes and help in identifying weak structures that should be avoided while designing new stronger encryption schemes.

CHAPTER 6

CONCLUSION

Voluminous amount of sensitive digital information is being exchanged every moment through penetrable networks in today's world. As highlighted earlier also, with the advancements in the digital and mobile technology along with emergence of concept of smart devices forming new reality of Internet of Things (IoT), there has been a significant shift in the type of transmitted content. The transmissions are no more limited to text-based data; they contain significant percentage of multimedia-based content. Traditional symmetric ciphers like AES, DES, IDEA etc. have been focusing on securing textual data, and are not found suitable for meeting the special resource efficiency requirements and catering the intrinsic properties of redundancy and bulkiness of visual content like images, videos etc. Also, the traditional symmetric key encryption approach has been the use of static operations irrespective of the plaintext and the secret key. This restricts the horizon of the traditional encryption schemes for their suitability/applicability to cater the additional requirements of multimedia including visual content. Thus, there is a need to design new encryption schemes to deal with the especial needs of multimedia including visual content. It has been largely observed that the focus of researchers proposing encryption schemes for visual content has been limited to one of the two key aspects pivotal to security of such visual content i.e. cost efficiency and strength, in-turn compromising on the others.

Though several researchers have proposed encryption schemes for securing multimedia including visual content, yet till date we do not have any standard proposed for addressing the special needs of multimedia. Therefore, the area of designing new encryption schemes for multimedia is a very relevant area of research in today's context. Another major issue which requires focus is making multimedia encryption schemes flexible and adaptable to suit dynamically changing needs of applications especially in the light of meeting real-time requirements and resource constrained environments of hand-held devices being used as end points for communications. Adaptability of encryption schemes as per changing requirements is a concept which is also in-tune with the upcoming 5G technology. Therefore, a need is identified for lightweight adaptable encryption schemes to secure multimedia with complete

removal of redundancy making them suitable for real-time and resource-constrained environments. Also, use of quantum computers in future is being widely explored among researchers, and therefore designs of multimedia encryption schemes offering high strength for such future applications is again an open research challenge today. Further, new multimedia encryption schemes are being frequently proposed by researchers, and this has attracted the attention of another group of researchers to focus on cryptanalysis of such schemes so as to discover weak structures and designs and improve upon them to make the schemes stronger. Significant work is being done in the area of cryptanalysis of multimedia encryption schemes by researchers and there is a lot of future scope in this area as well.

This thesis focuses on securing visual content especially images, which form a very significant component of modern day communications, with an intent to address the above mentioned issues of handling computational efficiency with high security and adaptability through use of unconventional designs of the encryption schemes. This thesis proposes multiple untraditional encryption schemes for securing visual content like images offering both efficiency as well as high strength. Some of these schemes also offer adaptability/flexibility to strike a balance between the trade-offs of computational expense and security as per application requirements. The thesis also demonstrates a cryptanalysis technique for a kind of existing chaos-based image encryption schemes reducible to solvable equivalent mathematical model, with an aim to identify weak structures leading to their reduction in equivalent mathematical model and further propose improved designs to enhance the security. The contribution of this thesis work is divided in four folds.

Firstly, role of use of chaos has been studied to have intrinsic cryptographic capabilities which are apt for achieving avalanche properties desired by any cryptosystem, and subsequently light chaotic-primitives are proposed to be used in encryption schemes for securing visual content so as to ensure the encryption process is computationally efficient while still providing desired levels of security. The proposed chaotic-primitives employ very simple cost-effective bitwise operations, but with the use of chaos, these primitives offer strong confusion and diffusion properties when used in encryption schemes.

Secondly, standard block ciphers like AES and PRESENT, which in their native form are not practically suitable for encrypting visual content in ECB mode, are customized to make them suitable for application in securing visual content by both maintaining/enhancing security and

reducing the incurred computational cost. The designed chaotic-primitives designed have also been used to customize AES for making it suitable to encrypt visual content. The proposed chaos-based customizations not only make the improvised standard schemes possess strong security parameters which in some cases are even better than the original scheme, but also make them suitable for application on visual content like images of any size in the native ECB mode and that to by incurring much lesser computational cost. The approach for customizing the standard scheme like AES has been to first identify the most time-consuming operation, which in this case was the Mix Columns operation, and then replace it with much lighter chaotic-primitive which actually enhanced the confusion property by involving an extra key-dependent operation in every round and also resulted in reduction of computational cost. While improving the ultra-lightweight block cipher PRESENT, though introduction of chaos-dependent operation added to extra computation, yet, the computational cost was reduced by reducing the number of rounds by identifying that better security levels are achieved in lesser number of rounds in the improvised PRESENT block cipher.

Thirdly, untraditional approach of introducing dynamism in encryption process is explored and multiple encryption schemes involving dynamism at different levels have been proposed. Encrypting visual content using dynamism by conditionally changing operations performed during per-round encryption and changing SBox used for substitution, is demonstrated by way of proposing three variants customizing conditional encryption based block cipher for securing visual content. Further, chaos-based dynamic framework is proposed where multiple levels are identified/proposed at which dynamism can be introduced like the type and number of operations performed per-round of encryption, the order/sequence of processing pixels, number of rounds of encryption etc. Results shown on a typical implementation of the proposed dynamic framework, with dynamism introduced in type, number of operations performed per-round and key/plaintext dependent sequence of processing pixels, demonstrate efficacy of the proposed framework in ensuring security while maintaining low computational expense. The generated cipher image satisfies the NIST randomness tests and is resistant to known/chosen plaintext attacks and differential cryptanalysis because though the encryption process is deterministic but the number and kind of operations employed for any particular secret key changes dynamically and hence are unknown to the attacker to perform cryptanalytic attacks. The difficulty is further increased for the attacker because the order/sequence of pixels being processed during encryption is also plaintext and key-dependent, thus making the proposed dynamic encryption framework resistant against any traditional cryptanalytic attack.

Extending this untraditional approach, in another work Probabilistic Encryption has been used to encrypt visual content thereby generating different cipher image for same image with same key at different times making it a very strong scheme which can resist different cryptanalytic attacks effectively and the scheme is also computationally efficient and works with customizable block size. Since the cipher image obtained for the same plain image with the same key varies randomly each time encryption is performed, it is impossible to perform cryptanalysis by the attacker. This work is one of its kinds as no such probabilistic symmetric-key encryption scheme practically suitable for visual content is found in literature to the best of our knowledge.

The use of these untraditional approaches of dynamic and/or probabilistic encryption offer very promising approaches that find utmost significance especially in today's world which is heading towards 5G networks, where adjusting to the dynamically changing requirements of the network is one of the primary necessitates for the offered services.

Fourthly and lastly, cryptanalysis of chaos-based existing image encryption scheme was carried out with an aim to identify weak structures/designs in such existing schemes which make them reducible to equivalent solvable mathematical models and propose improvements to enhance security. The Zhou et al. scheme [40] was identified to possess some weaknesses which could be exploited to break the said scheme. It was identified that the said scheme used fixed permutation and fixed small number of rounds which resulted in a weak design because of which the cipher image of size M×N could be expressed as a set of M.N linear equations easily solvable $O(M.N)^3$ time. Improvements like key and plaintext-dependent permutation stage instead of a mere fixed rotation, permutation-substitution structure instead of substitution-permutation one, key-dependent number of rounds, alternate forward/backward encryption and inter-row feedback in substitution stage are also suggested to enhance the security of the scheme and such similar schemes.

In future, the applicability of the encryption schemes proposed in this thesis work, can be verified on other forms of visual content and multimedia. Also, this thesis work has opened up a new paradigm of encryption schemes exploiting the scope of dynamism and use of probabilistic approach in the symmetric-key encryption as a new way forward for securing multimedia because the traditional schemes are computationally expensive, use exploitable

static operations, and are not directly suitable for the special needs of multimedia content. Further, use of unconventional designs along with chaos to achieve desired dynamism/randomness is also promising from the aspect of future quantum computers because chaos intrinsically offers cryptographic properties which have immense potential for utilization in quantum cryptography especially for visual content, though the same is not experimentally verified in this thesis work due to limited time and other constraints. But, it remains open for researchers, in future, to exploit use of chaos with untraditional approaches of dynamism and probabilistic encryption for developing and verifying efficacy of such encryption schemes for security applications in quantum computers for multimedia and even otherwise.

Also, more existing encryption schemes for visual content can be identified with static properties thereby possessing a scope to be modeled as system of equations, with intent to cryptanalyze them by solving the obtained set of equations. This can unfold loop-holes in such schemes and help in identifying weak structures that should be avoided while designing new stronger encryption schemes.

Thus, it may be concluded that, this thesis provides a deep insight on the development and analysis of encryption schemes for efficiently securing visual content, extendable to other forms of media/multimedia, by customizing standard schemes and using unconventional approaches for encryption. Clearly, this thesis work also opens up a new direction of research in the form of untraditional approaches using dynamism and probabilistic encryption because with the changing trends and vast usage of different forms of media, the traditional static schemes do not offer desired security with cost efficiency. Due to time restrictions, the efficacy and strength of all the proposed encryption schemes have been tested on visual content specifically images but this research can further be extended to other forms of media/ multimedia in future.

BIBLIOGRAPHY

[1] B. Furht, *Encyclopedia of Multimedia*, Springer, 2005.

[2] T.M. Savage and K.E. Vogel, *An Introduction to Digital Multimedia*, Jones and Bartlett Learning, 2008.

[3] N. Chapman and J. Chapman, *Digital Multimedia*, John Wiley and Sons, 2009.

[4] Z. Li and M. S. Drew, *Fundamentals of Multimedia*, Pearson Prentice Hall, 2004.

[5] D.C. Kay and J.R. Levine, *Graphics File Formats*, McGraw-Hill, 1995.

[6] R.C. Gonzalez and R.E. Woods, *Digital Image Processing, Third Edition*, Prentice Hall, 2007.

[7] A. Oppenheim, J. Buck and R Schafer, *Discerete-Time Signal Processing*, 2nd edition, Prentice-Hall, 1998.

[8] W. Stallings, *Cryptography & Network Security Principles and Practices*, Third Edition, Pearson Education, 2004.

[9] A. Menezes, P. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC-Press, 1996.

[10] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," 1999. [Online]. Available: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

[11] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, Volume 4727,* P. Paillier and I. Verbauwhede, Ed., Springer, Berlin, Heidelberg, 2007, pp. 450-466.

[12] V. Rohokale and R. Prasad, "Cyber Security for Intelligent World with Internet of Things and Machine to Machine Communication," *Journal of Cyber Security*, vol. 4, pp. 23-40, 2015, doi: 10.13052/jcsm2245-1439.412.

[13] T. Meskanen, V. Niemi and N. Nieminen, "How to Use Garbling for Privacy Preserving Electronic Surveillance Services," *Journal of Cyber Security*, vol. 4, pp. 41–64, 2015, doi: 10.13052/jcsm2245-1439.413.

[14] M. Abomhara and G. M. Køien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *Journal of Cyber Security*, vol. 4, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[15] A. Elmangoush and T. Magedanz, “Adaptable Protocol Selection for Reliable Smart City Services,” *Journal of Cyber Security*, vol. 6, no.1, pp. 57–76, 2017, doi: 10.13052/jcsm2245-1439.613.

[16] C. E. Shannon, “Communication theory of secrecy system,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[17] C. Alexopoulos, Nikolaos G. Bourbakis and N. Ioannou, “Image encryption method using a class of fractals,” *Journal of Electronic Imaging*, vol. 4, no. 3, 1995, doi: 10.1117/12.208654.

[18] N. G. Bourbakis, “Image data compression-encryption using G-scan patterns,” in *Proc. 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, Orlando, FL, USA, 1997, pp. 1117-1120 vol. 2, doi: 10.1109/ICSMC.1997.638099.

[19] S. S. Maniccam and N. G. Bourbakis, “SCAN based lossless image compression and encryption,” in *Proc. of 1999 International Conference on Information Intelligence and Systems (Cat. No. PR00446)*, Bethesda, MD, USA, 1999, pp. 490-499, doi: 10.1109/ICIIS.1999.810321.

[20] S. S. Maniccam and N. G. Bourbakis, “Lossless image compression and encryption using SCAN,” *Pattern Recognition*, vol. 34, vol. 6, pp. 1229–1245, 2001.

[21] C. Chen and R. Chen, “Encryption and Decryption Using SCAN Methodology,” in *Proc. of Seventh International Conference on Parallel and Distributed Computing Applications and Technologies 2006 (PDCAT '06)*, 2006, pp. 61-66.

[22] R. M. Rad, A. Attar and R. E. Atani, “A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR,” *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 6, pp. 275-290 , 2013, doi: 10.14257/IJSIP.2013.6.5.25.

[23] N. Bourbakis and A. Dollas, “SCAN-based compression-encryption-hiding for video on demand,” *MultiMedia IEEE*, vol. 10, no. 3, pp. 79-87, 2003.

[24] R. Chen and S. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 413-426, 2010.

[25] R. Chen, J. Lai and S. Horng, "Novel Stream Cipher Using SCAN and Variable Ordered Recursive CA Substitutions and Its DSP+FPGA Implementation," *Journal of Networks*, vol. 5, pp. 75-87, 2010.

[26] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems,* Addison-Wesley Publishing, 1989.

[27] A. N. Pisarchik and M. Zanin, "Chaotic Map Cryptography and Security, Encryption: Methods, Encryption: Methods," *Encryption: Methods, Software and Security*, Nova Science Publishers Inc., 2010, pp. 1-28.

[28] G. Alvarez and S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006.

[29] T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map," in *Proc. of Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science 0547*, Springer-Verlag, Berlin, 1991, pp. 127-140.

[30] J. Fridrich, "Symmetric Ciphers based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[31] S. Lian, J. Sun and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 351, no.2-4, pp. 645–661, 2005.

[32] S. Lian, J. Sun and Z. Wang, "A block cipher based on a suitable use of chaotic standard map," *Chaos, Solitons & Fractals*, vol.26, no. 1, pp. 117–129, 2005.

[33] Y. Mao, G. Chen and S. Lian, "A novel fast image encryption scheme based on the 3D Chaotic Baker Map," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[34] M. Francois, T. Grosges, D. Barchiesi and R. Erra, "Image Encryption Algorithm Based on a Chaotic Iterative Process," *Applied Mathematics*, vol. 3, pp. 1910-1920, 2012.

[35] M. Gschwandtner, A. Uhl and P. Wild, “Transmission Error and Compression Robustness of 2D Chaotic Map Image Encryption Schemes,” *Journal of Information Security*, vol. 1, pp. 1-16, 2009.

[36] H. Chen, C. Wei, C. Tien and C. Chen, “An Efficient and Fast Chaos-Based Encryption Scheme for Images,” *Storage Management Solutions*, Issue 3, pp. 15-32, 2013.

[37] A. Kadir, A. Hamdulla and W. Q. Guo, “Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN,” *Optik*, vol. 125, pp. 1671-1675, 2014.

[38] K. Gupta and S. Silakari, “New Approach for Fast Color Image Encryption Using Chaotic Map,” *Journal of Information Security*, vol. 2, pp. 139-150, 2011.

[39] Q. Alsafasfeh and A. A. Arfoa, “Image Encryption Based on the General Approach for Multiple Chaotic Systems,” *Journal of Signal and Information Processing*, vol. 2, no. 3, pp. 238-244, 2011, doi: 10.4236/jsip.2011.23033.

[40] Y. Zhou, L. Bao and C. L. Philip Chen, “A new 1D chaotic system for image encryption,” *Signal Processing*, vol. 97, pp. 172-182, 2014.

[41] C. L. Philip Chen , T. Zhang and Y. Zhou, “Image Encryption Algorithm Based on A NewCombined Chaotic System,” in *Proc. 2012 IEEE International Conference on Systems, Man, and Cybernetics*, 2012, doi: 10.1109/ICSMC.2012.6378120.

[42] Y. Cao, “A New Hybrid Chaotic Map and Its Application on Image Encryption and Hiding,” *Mathematical Problems in Engineering*, vol. 2013, 2013, Art. no. 728375, doi: 10.1155/2013/728375.

[43] N. Ramadan, H.H. Ahmed, S.E. Elkhamy and F.E. Abd El-Samie, “Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map,” *American Journal of Signal Processing*, vol. 6, no. 1, pp. 1-13, 2016.

[44] R. Boriga, A.C. Dăscălescu and A.V. Diaconu, “A New One-Dimensional Chaotic Map and Its Use in a Novel Real-Time Image Encryption Scheme,” Advances in Multimedia, vol. 2014, 2014, Art. no. 409586, doi: 10.1155/2014/409586.

[45] X. Zhang and Y. Cao, “A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme,” *The Scientific World Journal*, vol. 2014, 2014, Art. no. 713541, doi: 10.1155/2014/713541.

[46] N.F. Elabady, H.M. Abdalkader, M.I. Moussa and S.F. Sabbeh, “Image encryption based on new one-dimensional chaotic map”, in *Proc. 2014 International Conference on Engineering and Technology (ICET)*, Cairo, 2014, pp. 1-6, doi: 10.1109/ICEngTechnol.2014.7016811.

[47] O.A. Saraereh, Q. Alsafasfeh and A. Arfoa, “Improving a New Logistic Map as a New Chaotic Algorithm for Image Encryption,” *Modern Applied Science*, vol. 7, no. 12, 2013, doi:10.5539/mas.v7n12p24.

[48] S.E. Borujeni and M.S. Ehsani, “Modified Logistic Maps for Cryptographic Application,” Applied Mathematics, vol. 6, pp. 773-782, 2015.

[49] M. Maqableh, “A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map,” *Journal of Software Engineering and Applications*, vol. 8, pp. 635-659, 2015.

[50] L. Rui, “New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map,” *The Open Cybernetics & Systemics Journal*, vol. 9, pp. 210-216, 2015.

[51] Z. Hua, Y. Zhou and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Information Sciences*, vol. 480, pp. 403–419, 2019.

[52] M. Essaid, I. Akharraz, A. Saaidi and A. Mouhib, “Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps,” *Journal of Information Security and Applications*, vol. 47, pp. 173-187, 2019.

[53] F. Zhao, C. Li, C. Liu and Y. Song, “Color image encryption algorithm based on hyperchaotic and security analysis,” *Journal of Electronic Imaging*, vol. 28, no. 4, 2019, doi: 10.1117/1.JEI.28.4.043011.

[54] C. Li, F. Zhao, C. Liu, L. Lei and J. Zhang, “A Hyperchaotic Color Image Encryption Algorithm and Security Analysis,” *Security and Communication Networks*, vol. 2019, 2019, Art. no. 8132547, doi: 10.1155/2019/8132547.

[55] J. Thiyagarajan, B. Murugan and A. G. N. Gounder, “A Chaotic Image Encryption Scheme with Complex Diffusion Matrix for Plain Image Sensitivity,” *Serbian Journal of Electrical Engineering*, vol. 16, no. 2, pp. 247-265, June 2019, doi: 10.2298/SJEE1902247T.

[56] A.X. Zhang, L. Wang, Z. Zhou and Y. Niu, "A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals," *IEEE Access*, vol. 7, pp. 74734-74746, 2019, doi: 10.1109/ACCESS.2019.2921309.

[57] H. Li, Y.Wang and Z.Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," *Optics and Lasers in Engineering*, vol. 115, pp. 197-207, 2019.

[58] S. Xu, Y. Wang, J. Wang and M. Tian, "Cryptanalysis of Two Chaotic Image Encryption Schemes Based on Permutation and XOR Operations," in *Proc. 2008 International Conference on Computational Intelligence and Security*, Suzhou, 2008, pp. 433-437, doi: 10.1109/CIS.2008.146.

[59] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption based on hyper-chaos," *Physics Letters A*, vol. 372, pp. 5973-5978, 2008.

[60] S. Li, C. Li, G Chen, N. G. Bourbakis and K. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication*, vol. 23, pp. 212–223, 2008.

[61] C. Li and K. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing*, vol. 91, pp. 949–954, 2011.

[62] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Processing*, vol. 118, pp. 203–210, 2016.

[63] J. C. Yen and J.I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation," *IEE Proceedings. – Vision, Image and Signal Processing*, vol. 147, no. 2, pp. 167–175, 2000.

[64] E.Y. Xie, C. Li, S. Yu and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2017.

[65] A. Jolfaei and X. Wu, "On the security of permutation-only image encryption scheme," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, 2016, doi: 10.1109/TIFS.2015.2489178.

[66] S. Singh, M. Ahmad and D. Malik, "Breaking an image encryption scheme based on chaotic synchronization phenomenon," in *Proc. 2016 Ninth International Conference on Contemporary Computing (IC3)*, Noida, pp. 1–4, 2016, doi:10.1109/IC3.2016.7880215.2016.

[67] C. Li, D. Lin and J. Lü, “Cryptanalyzing an image-scrambling encryption algorithm of pixel bits,” *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017, doi:10.1109/MMUL.2017.3051512.

[68] D.S. Laiphrakpam, M.S. Khumanthem, “Cryptanalysis of symmetric key image encryption using chaotic Rossler system,” *Optik*, vol. 135, pp. 200–209, 2017.

[69] B. Wang, Y. Xie, C. Zhoua, S. Zhoua and X. Zhenga, “Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps,” *Optik*, vol. 127, pp. 3541–3545, 2016.

[70] K. Zhou, M. Xu, J. Luo, H. Fan and M. Li, “Cryptanalyzing an image encryption based on a modified Henon map using hybrid chaotic shift transform,” *Digital Signal Processing*, vol. 93, pp. 115-127, 2019, doi: 10.1016/j.dsp.2019.07.013.

[71] W. Feng, Y. He, H. Li and C. Li, “Cryptanalysis of the integrated chaotic systems based image encryption algorithm,” *Optik*, vol. 186, pp. 449-457, 2019.

[72] M. Li, K. Zhou, H. Ren and H. Fan, “Cryptanalysis of Permutation–Diffusion-Based Lightweight Chaotic Image Encryption Scheme Using CPA,” *Applied Sciences*, vol. 9, no. 3, 2019, Art. no. 494, doi: 10.3390/app9030494.

[73] K. W. Wong, W. S. Yap, B. M. Goi and D. C. K. Wong, “Differential Cryptanalysis on Chaotic Based Image Encryption Scheme,” *IOP Conference Series: Materials Science and Engineering*, vol. 495, 2019, Art. no. 012041, doi: 10.1088/1757-899x/495/1/012041.

[74] S. Kartalopoulos, “Chaotic quantum cryptography: The ultimate for network security,” in *Proc. of 2010 International Conference on Optical Communication Systems (OPTICS)*, Athens, 2010.

[75] A. D. Stojanovic, R. V. Ramos and P. S. Matavulj, “Authenticated B92 QKD protocol employing synchronized optical chaotic systems,” *Optical and Quantum Electronics*, vol. 48, pp. 285, 2016.

[76] G. Geetha, “New Directions in Quantum Chaotic Crypto Schemes,” in *Proc. of 2012 International Conference on Computing Sciences*, pp. 316-321, 2012, doi: 10.1109/ICCS.2012.47.

[77] A. Akhshani, “Quantum Chaotic Cryptography: A New Approach,” Ph.D. dissertation, Universiti Sains Malaysia, Malaysia, 2015.

[78] S. Behnia, P. Ayubi and W. Soltanpoor, “Image encryption based on quantum chaotic map and FSM transforms,” in Proc. *2012 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, Rome, 2012, pp. 1-6, doi: 10.1109/NETWKS.2012.6381669.

[79] A. Akhshani, S. Behnia, A. Akhavan, S-C. Lim and Z. Hassan, “An Image Encryption Approach Using Quantum Chaotic Map,” in *Proc. of 2013 2nd International Conference on Advances in Computer and Information Technology - ACIT*, 2013, pp. 171-176, doi:10.3850/978-981-07-6261-2_36.

[80] R. V. Ramos and R. F. Souza, “Using Chaotic Dynamics in Quantum Cryptographis Systems: Chaotic Cryptography and Repeaters,” *Journal of Optical Communication*, vol. 22, no. 3, pp. 90-94, 2001, doi:10.1515/JOC.2001.22.3.90.

[81] R. V. Ramos, “Quantum-Chaotic Cryptography,” 2017. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1703/1703.06512.pdf.

[82] R. J. Chen and J. L. Lai, “Image security system using recursive cellular automata substitution,” *Pattern Recognition*, vol. 40, no. 5, pp. 1621–1631, 2007, doi: 10.1016/j.patcog.2006.11.011.

[83] R. J. Chen and S. J. Horng, “Novel SCAN-CA-based images security system using SCAN and 2-D von Neumann cellular automata,” *Signal Processing*, vol. 25, no. 6, pp. 413–426, 2010, doi: 10.1016/j.image.2010.03.002.

[84] J. Jin, “An image encryption based on elementary cellular automata,” *Optics and Lasers in Engineering*, vol. 50, no. 12, pp.1836-1843, 2012.

[85] X. Wang and D. Luan, “A novel image encryption algorithm using chaos and reversible cellular automata,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013, doi: 10.1016/j.cnsns.2013.04.008.

[86] X. Zhang, C. Wang, S. Zhong and Q. Yao, “Image encryption scheme based on balanced two dimensional cellular automata,” *Mathematical Problems in Engineering*, pp. 1-10, 2013.

[87] T. Chen, “Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling,” *Optics & Laser Technology*, vol. 84, pp. 118–133, 2016.

[88] D. Tralic and S. Grgic, “Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation,” *Radio Engineering*, vol. 25, no. 3, pp. 548-555, 2016.

[89] Y. Wang, Y. Zhao, Q. Zhou and Z. Lin, “Image encryption using partitioned cellular automata,” *Neurocomputing*, vol. 275, pp. 1318-1332, 2018.

[90] L.M. Adleman, “Molecular computation of solutions to combinatorial problems,” *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[91] C. T. Clelland, V. Risca, and C. Bancroft, “Hiding messages in DNA microdots,” *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[92] A. Gehani, T. LaBean, and J. Reif, “DNA-based cryptography,” in *Proc. of the DIMACS Workshop V on DNA Based Computers*, American Mathematical Society, 1999, vol. 54, pp 233–249.

[93] N. Kang, “A pseudo DNA cryptography method,” 2009. [Online]. Available: http://arxiv.org/abs/0903.2693.

[94] Q. Zhang, L. Guo and X. Wei, “Image encryption using DNA addition combining with chaotic maps,” *Mathematical and Computer Modelling*, vol. 52, pp. 2028–2035, 2010.

[95] J. Zhang, D. Fang and H. Ren, “Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps,” *Mathematical Problems in Engineering*, vol. 2014, 2014, Art. no. 917147, doi: 10.1155/2014/917147.

[96] H. Liu, X. Wang and Abdurahman Kadir, “Image encryption using DNA complementary rule and chaotic maps,” *Applied Soft Computing*, vol. 12, pp. 1457–1466, 2012.

[97] C. Song and Y. Qiao, “A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos,” *Entropy*, vol. 17, pp. 6954-6968, 2015, doi:10.3390/e17106954.

[98] L. Liu, Q. Zhang and X. Wei, “A RGB image encryption algorithm based on DNA encoding and chaos map”, *Computers and Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[99] Q. Zhang and X. Wei, “A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system,” *Optik*, vol. 124, no. 23, pp. 6276–6281, 2013.

[100] T. T. Zhang, S. J. Yan, C. Y. Gu, R. Ren and K. X. Liao, “Research on Image Encryption Based on DNA Sequence and Chaos Theory,” *IOP Conf. Series: Journal of Physics: Conf. Series*, vol. 1004, 2018, Art. no. 012023, doi: 10.1088/1742-6596/1004/1/012023.

[101] S. Zhou, B. Wang, X. Zheng and C. Zhou, “An Image Encryption Scheme Based on DNA Computing and Cellular Automata,” *Discrete Dynamics in Nature and Society*, vol. 2016, 2016, Art. no. 5408529, doi: 10.1155/2016/5408529.

[102] S. Paul, P. Dasgupta, P. K. Naskar and A. Chaudhuri, “Secured image encryption scheme based on DNA encoding and chaotic map,” *Review of Computer Engineering Studies*, vol. 4, no. 2, pp. 70-75, 2017, doi: 10.18280/rces.040206.

[103] Q. Zhang, X. Xue and X. Wei, “A Novel Image Encryption Algorithm Based on DNA Subsequence Operation,” *The Scientific World Journal*, vol. 2012, 2012, Art. no. 286741, doi:10.1100/2012/286741.

[104] A. Rehman, X. Liao, A. Kulsoom and S. A. Abbas, “Selective encryption for gray images based on chaos and DNA complementary rules,” *Multimedia Tools & Applications*, vol. 74, pp. 4655–4677, 2015, doi: 10.1007/s11042-013-1828-7.

[105] Y. Liu, J. Tang, and T. Xie, “Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map,” *Optics and Laser Technology*, vol. 60, pp. 111–115, 2014.

[106] L. Zeng and R. Liu, “Cryptanalyzing a novel couple images encryption algorithm based on DNA subsequence operation and chaotic system,” *Optik*, vol. 126, no. 24, pp. 5022-5025, 2015.

[107] C. Pang, “An Image Encryption Algorithm Based on Discrete Wavelet Transform and Two Dimension Cat Mapping,” in *Proc. International Conference on Networks Security, Wireless Communications and Trusted Computing,* 2009, pp. 711-714, doi: 10.1109/NSWCTC.2009.191.

[108] J. Wang, “Image Encryption Algorithm Based on 2-D Wavelet Transform and Chaos Sequences,” in *Proc. International Conference on Computational Intelligence and Software Engineering*, 2009, pp. 1-3, doi: 10.1109/CISE.2009.5362955.

[109] Z. Yu, Z. Zhe, Y. Haibing, P. Wenjie and Z. Yunpeng, “A chaos-based image encryption algorithm using wavelet transform,” in *Proc. 2nd International Conference on Advanced Computer Control*, Shenyang, 2010, pp. 217-222, doi: 10.1109/ICACC.2010.5486684.

[110] J. Lai, S. Liang and D. Cui, “A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Chaotic System,” in *Proc. International Conference on Multimedia Communications*, Hong Kong, 2010, pp. 24-27, doi: 10.1109/MEDIACOM.2010.30.

[111] Y. Wang and S. Zhou, “A novel image encryption algorithm based on fractional Fourier transform,” in *Proc. International Conference on Computer Science and Service System (CSSS)*, Nanjing, 2011, pp. 72-75, doi: 10.1109/CSSS.2011.5974982.

[112] G. Bhatnagar, Q.M. Jonathan Wua and B. Raman, “Discrete fractional wavelet transform and its application to multiple encryption,” *Information Sciences*, vol. 223, pp. 297–316, 2013.

[113] S. Liu, Y. Song and J. Yang, “Image Encryption Algorithm Based on Wavelet Transforms and Dual Chaotic Maps,” *Journal of Software*, vol. 9, pp. 458-465, 2014.

[114] P. Shanthi, “Chaotic Based Image Cryptography Using Wavelet Transform,” *International Journal of Engineering Research in Computer Science and Engineering*, vol. 5, no. 3, pp.90-97, 2018, doi: 01.1617/vol5/iss3/pid94531.

[115] O. A. Alkishriwo, “An image encryption algorithm based on chaotic maps and discrete linear chirp transform,” *Almadar Journal for Communications Information Technology and Applications*, vol. 5, no. 1, pp. 14-19, 2018.

[116] L. Bao, Y. Zhou and C. L. Philip Chen, “Image encryption in the wavelet domain,” in *Proc. of SPIE 8755, Mobile Multimedia/Image Processing, Security, and Applications* 2013, vol. 8755, pp. 1-12, doi: 10.1117/12.2015725.

[117] G. Bhatnagar and Q. M. J. Wu, “Selective image encryption based on pixels of interest and singular value decomposition,” *Digital Signal Processing*, vol. 22, pp. 648–663, 2012.

[118] S. Som and S. Sen, “A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos,” *Procedia Technology*, vol. 10, pp. 663 – 671, 2013.

[119] N. Taneja, B. Ramanb and I. Gupta, “Selective image encryption in fractional wavelet domain,” *International Journal of Electronics and Communications (AEÜ)*, vol. 65, pp. 338–344, 2011.

[120] S. Sasidharan and D. S. Philip, “A fast partial image encryption scheme with wavelet transform and RC4,” *International Journal of Advances in Engineering & Technology*, vol. 1, no. 4, pp.322-331, 2011.

[121] X. Liu and A. M. Eskicioglu, “Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions,” in *Proc. of International Conference on Communications, Internet and Information Technology (CIIT 2003)*, 2003, pp. 17–19.

[122] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq and J.J. Quisquater, “Overview on Selective Encryption of Image and Video: Challenges and Perspectives,” *EURASIP Journal on Information Security*, vol. 2008, 2008, Art. no. 179290, doi: 10.1155/2008/179290.

[123] L. M. Jawad and G. Sulong, “A Survey on Emerging Challenges in Selective Color Image Encryption Techniques,” *Indian Journal of Science and Technology*, vol 8, no. 27, 2015, doi: 10.17485/ijst/2015/v8i27/71241.

[124] S. Goldwasser and S. Micali, “Probabilistic Encryption,” *Journal of Computer and System Sciences*, vol. 28(2), pp. 270-299, 1984.

[125] K. Faraoun, “Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption,” *The International Arab Journal of Information Technology*, vol. 7, no. 3, pp. 231-240, 2010.

[126] N.K. Pareek, V. Patidar and K.K. Sud, “Cryptography using multiple one-dimensional chaotic maps,” *Nonlinear Science and Numerical Simulation*, vol.10, pp.715-723, 2005.

[127] J. Wei, X. Liao, K. Wong and T. Zhou, “Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps,” *Nonlinear Science and Numerical Simulation*, vol. 12, pp. 814-822, 2007.

[128] I. S. I. Abuhaiba, A. Y. AlSallut, H.H. Hejazi and H.A. AbuGhali, "Cryptography Using Multiple Two-Dimensional Chaotic Maps," *International Journal of Computer Network and Information Security*, vol. 8, pp. 1-7, 2012, doi: 10.5815/ijcnis.2012.08.01.

[129] X. Wang and Y. Qing, "A block encryption algorithm based on dynamic sequences of multiple chaotic sequences of multiple chaotic systems," *Science and Numerical Simulation*, vol.14, pp. 574-581, 2009.

[130] K. Sakthidasan and B.V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images," *International Journal of Information and Education Technology*, vol. 1, no. 2, 2011.

[131] Y. Zhou and L. Bao, C.L. Philip Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, pp. 3039–3052, 2013.

[132] J. Vahidi and M. Gorji, "The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos," *Journal of Mathematics and Computer Science*, vol. 9, pp. 451-457, 2014.

[133] H. H. Ngo, X. Wu, P. Dung Le, C. Wilson and B. Srinivasan, *Dynamic Key Cryptography and Applications,* International Journal of Network Security, vol. 10, pp. 161-174, 2010, doi: 10.6633/IJNS.201005.10(3).01.

[134] Y. Harmouch and R.E. Kouch, "A New Algorithm for Dynamic Encryption," *International Journal of Innovation and Applied Studies*, vol. 10, no. 1, pp. 305-312, 2015.

[135] Y. Cao, "A New Hybrid Chaotic Map and Its Application on Image Encryption and Hiding," *Mathematical Problems in Engineering*, vol. 2013, 2013, Art. no. 728375, doi: 10.1155/2013/728375.

[136] X. Y. Wang, S. X. Gu and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, pp. 126–134, 2015.

[137] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[138] J.S. Armand EyebeFouda, J. Y. Effa, S. L. Sabat and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 578-588, 2014.

[139] J.S. Armand EyebeFouda, J. Y. Effa and M. Ali, "Highly secured chaotic block cipher for fast image encryption," *Applied Soft Computing*, vol. 25, pp. 435–444, 2014.

[140] L. Wang, H. Song and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, 2016.

[141] X. Chai, K. Yang and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 9907-9927, 2017.

[142] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S8 permutation," *Journal of Intelligent and Fuzzy Systems*, vol.33, no. 6, pp. 3753-3765, 2017.

[143] J. Ahmad, M. A. Khan, S. O. Hwang and J. S. Khan, "A compression, sensing and noise-tolerant image encryption scheme based on chaotic maps and othogonal matrices," *Neural Computing and Applications*, vol. 28(S-1), pp. 953-967, 2017.

[144] J. S. Khan, J. Ahmad and M. A. Khan, "TD-ERCS map-based confusion and diffusion of autocorrelated data," *Nonlinear Dynamics*, vol. 87, pp. 93-107, 2017.

[145] N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, pp. 926-934, 2006.

[146] S. Dhall and S.K. Pal, "Design of a new block cipher based on conditional encryption," in *Proc. of 7th International Conference on Information Technology: New Generations (ITNG 2010),* 2010, pp. 714–718, doi: 10.1109/ITNG.2010.90.

[147] K. Korstanje and L. Keliher, "Weak keys and plaintext recovery for the Dhall-Pal Block Cipher," in *Proc. 2015 IEEE Symposium on Computers and Communication (ISCC),* 2015, pp. 816-821, doi:10.1109/ISCC.2015.740561.

[148] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," *Fast Software Encryption, Cambridge Security Workshop Proceedings*

(December 1993), LNCS, vol. 809, pp. 191-204, 1994, doi: 10.1007/3-540-58108-1_24.

[149] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, John Wiley & Sons, 1999.

[150] I. Hussain, T. Shah and M. A. Gondal, "Image encryption algorithm based on PGL (2, GF(2^8)), S-boxes, and TD-ERCS chaotic sequence," *Nonlinear Dynamics*, vol. 70, no. 1, pp. 181-187, 2012.

[151] A. Anees, A. M. Siddiqui and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 3106-3118, 2014.

[152] J. Ahmad and S.O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, pp. 1839-1850, 2015.

[153] J. S. Khan, M. A. Khan, J. Ahmad and S.O. Hwang, W. Ahmed, "An Improved Image Encryption Scheme Based on a Non-Linear Chaotic Algorithm and Substitution Boxes," *Informatica*, vol. 28, no. 4, pp. 629-649, 2017.

[154] G. N. Krishnamurthy and V. Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box," *International Journal of Computer Science and Network Security*, vol. 8, no. 9, pp. 388-398, 2008.

[155] I. Abd-ElGhafar, A. Rohiem, A. Diaa and F. Mohammed, "Generation of AES key dependent S-boxes using RC4 algorithm," in *Proc. of 13th International Conference on Aerospace Sciences & Aviation Technology (ASAT–13)*, 2009, doi: 10.21608/asat.2009.23497.

[156] B. Subramanyan, V. M. Chhabria and T. G. Sankarbabu, "Image Encryption Based On AES Key Expansion," in *Proc. of 2011 Second International Conference on Emerging Applications of Information Technology,* 2011, doi: 10.1109/EAIT.2011.60.

[157] H. M. El-Sheikh and O. A. El-Mohsen, "A New Approach for Designing Key-Dependent S-Box Defined over GF (2^4) in AES," *International Journal of Computer Theory and Engineering*, vol. 4, no. 2, 2012.

[158] J. Juremi, R. Mahmod, S. Sulaiman and J. Ramli, “Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key,” *International Journal of Cyber-Security and Digital Forensics*, pp. 183-188, 2012.

[159] E. M. Mahmoud, A. A. El Hafez, T. A. Elgraf and A. Zekry, “Dynamic AES -128 with Key- Dependent S-Box,” *International Journal of Engineering Research and Applications (IJERA),* vol. 3, pp. 1662-1670, 2013.

[160] C. Pradhan and A.K. Bisoi, “Chaotic Variations on AES Algorithm,” *International Journal of Chaos, Modelling and Simulation*, vol. 2, no. 2, 2013, doi: 10.5121/ijccms.2013.2203. [Online]. Available: https://arxiv.org/abs/1307.3057.

[161] S. Arrag, A. Hamdoun, A. Tragha and S. E. Khamlich, “Implementation of Stronger AES by using Dynamic S-Box Dependent of Master Key,” *Journal of Theoretical and Applied Information Technology*, vol. 53, no. 2, pp. 196-204, 2013.

[162] M. Dara and K. Manochehr, “A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key,” *World Applied Sciences Journal*, vol. 28 no. 12, pp. 2003-2009, 2013.

[163] M. B. Parthasarathy and B. Srinivasan, “Increased Security in Image Cryptography using Wavelet Transforms,” *Indian Journal of Science and Technology*, vol. 8, no. 12, 2015, doi: 10.17485/ijst/2015/v8i12/62433.

[164] L. R. Knudsen, “Dynamic Encryption,” *Journal of Cyber Security*, vol. 3, pp. 357-370, 2015.

[165] S. Goldwasser and S. Micali, “Probabilistic Encryption & how to play mental poker keeping all partial information secret,” in *Proc. of 14th Annual ACM Symposium on Theory of Computing*, 1982, pp. 365-377.

[166] G. J. Fuchsbauer, “An Introduction to Probabilistic Encryption,” *Osijek Mathematical List*, vol. 6, no. 1, 2006.

[167] R. L. Rivest and A. T. Sherman, “Randomized Encryption Techniques,” *Advances in Cryptology: Proceedings of Crypto 82*, pp. 145-163, 1983.

[168] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[169] M. Blum and S. Goldwasser, "An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information," *Advances in Cryptology: Proceedings of CRYPTO 1984, LNCS*, vol. 196, pp. 289-299, 1985.

[170] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," *Advances in Cryptology — EUROCRYPT '98, LNCS*, vol. 1403, pp. 308-318, 1998.

[171] T. Okamoto, S. Uchiyama and E. Fujisaki, "EPOC: Efficient Probabilistic Public-Key Encryption," Submission to *IEEE P1363a*, 1998. [Online]. Available: http://grouper.ieee.org/groups/1363//StudyGroup/contributions/epoc.pdf.

[172] T. Okamoto and D. Pointcheval, "EPOC-3: Efficient Probabilistic Public-Key Encryption (Version 2)," Submission to *IEEE P1363a*, 2000. [Online]. Available: http://grouper.ieee.org/groups/1363//StudyGroup/contributions/epoc3v2.pdf.

[173] E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," *Journal of Cryptology*, vol. 26, no. 1, pp. 80-101, 2013, doi:10.1007/s00145-011-9114-1.

[174] S. Papadimitriou, T. Bountis, S. Mavroudi and A. Bezerianos, "A probabilistic symmetric encryption scheme for very fast secure communication based on chaotic systems of difference equations," *International Journal of Bifurcation and Chaos*, vol. 11, no. 12, pp. 3107–3115, 2001.

[175] S. Li, X. Mou, B. L. Yang, Z. Ji and J. Zhang, "Problems with a probabilistic encryption scheme on chaotic systems," *International Journal of Bifurcation and Chaos*, vol. 13, no. 10, pp. 3063-3077, 2003.

[176] K. C. Leung, S. L. Li, L. M. Cheng and C. K. Chan, "A Symmetric Probabilistic Encryption Scheme Based On CHNN Without Data Expansion," *Neural Processing Letters*, vol. 24, no. 2, pp. 93-105, 2006.

[177] D. Guo, L.M. Cheng and L.L. Cheng, "A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks," *Applied Intelligence*, vol. 10, no. 1, pp. 71–84, 1999.

[178] B. D. Reddy, V. V. Kumari and K. Raju, "Randomized symmetric block encryption," in *Proc. First International Conference on Security of Internet of Things (SecurIT '12)*, 2012, pp. 222-226, doi: 10.1145/2490428.2490460.

[179] B. D. Reddy, V. V. Kumari and K. Raju, "A New Symmetric Probabilistic Encryption Scheme based on random numbers," in *Proc. First International Conference on Networks & Soft Computing (ICNSC 2014),* 2014, pp. 267-272, doi: 10.1109/CNSC.2014.6906672.

[180] P. Ratha, D. Swain, B. Paikaray and S. Sahoo, "An optimized encryption technique using an arbitrary matrix with probabilistic encryption," in *Proc. of 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)*, *Procedia Computer Science*, vol. 57, pp. 1235–1241, 2015.

[181] K. A. N. Reddy and B. Vishnuvardhan, "The Probabilistic Encryption Algorithm Using Linear Transformation," *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI)*, vol. 2, AISC, vol. 338, pp. 389-395, 2015.

[182] G. Tu, X. Liao and T. Xiang, "Cryptanalysis of a color image encryption algorithm based on chaos," *Optik*, vol. 124, pp. 5411–5415, 2013.

[183] X. Wang, L. Teng and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, pp. 1101–1108, 2012.

[184] B.Wang, X. Wei and Q. Zhang, "Cryptanalysis of an image cryptosystem based on logistic map," *Optik*, vol. 124, pp. 1773–1776, 2013.

[185] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010.

[186] H. Hermassi, R. Rhouma and S. Belghith, "Security analysis of image cryptosystems only or partially based on a chaotic permutation," *The Journal of Systems and Software*, vol. 85, pp. 2133–2144, 2012.

[187] L. Zhao, A. Adhikari, D. Xiao and K. Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, pp. 3303–3327, 2012.

[188] F. Özkaynaka, A. B. Özer and S. Yavuz, "Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, pp. 4946–4948, 2012.

[189] C. Zhu, “A novel image encryption scheme based on improved hyperchaotic sequences,” *Optics Communications*, vol. 285, pp. 29–37, 2012.

[190] B. Norouzi and S. Mirzakuchaki, “Breaking an image encryption algorithm based on the new substitution stage with chaotic functions,” *Optik*, vol. 127, pp. 5695–5701, 2016.

[191] Z. Parvin, H. Seyedarabi and M. Shamsi, “A new secure and sensitive image encryption scheme based on new substitution with chaotic function,” *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10631-10648, 2016.

[192] L. Chen and S. Wang, “Differential cryptanalysis of a medical image cryptosystem with multiple rounds,” *Computers in Biology and Medicine*, vol. 65, pp. 69–75, 2015.

[193] C. Fu, W. Meng , Y. Zhan, Z. Zhu, F.C.M. Lau , C. K. Tse and H. Ma, “An efficient and secure medical image protection scheme based on chaotic maps,” *Computers in Biology and Medicine*, vol. 43, pp. 1000–1010, 2013.

[194] L. Zhang, Z. Zhu, B. Yang, W. Liu, H. Zhu and M. Zou, “Cryptanalysis and Improvement of an Efficient and Secure Medical Image Protection Scheme,” *Mathematical Problems in Engineering*, vol. 2015, 2015, Art. no. 913476, doi: 10.1155/2015/913476.

[195] F. Özkaynaka and A. B. Özer, “Cryptanalysis of a new image encryption algorithm based on chaos,” *Optik*, vol. 127, pp. 5190–5192, 2016.

[196] X. Wang, J. Zhao and H. Liu, “A new image encryption algorithm based on chaos,” *Optics Communications*, vol. 285, pp. 562–566, 2012.

[197] Y. Wu, J. P. Noonan and S. Agaian, “NPCR and UACI randomness tests for image encryption,” *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2011.

[198] A.F. Webster and S.E. Tavares, “On the Design of S-Boxes, in Proc. of Conference on the Theory and Application of Cryptographic Techniques,” *Advances in Cryptology -CRYPTO ’85 Proceedings, CRYPTO 1985*, LNCS, vol. 218, pp. 523-524, 1986.

[199] S. Lian, D. Kanellopoulos and G. Ruffo, “Recent Advances in Multimedia Information System Security,” *Informatica*, vol. 33, pp. 3–24, 2009.

[200] Z. Su, G. Zhang and J. Jiang, "Multimedia Security: A Survey of Chaos-Based Encryption Technology," in *Multimedia - A Multidisciplinary Approach to Complex Issues*, Ioannis Karydis, Ed., IntechOpen, 2012, doi: 10.5772/36036. [Online] Available: https://www.intechopen.com/books/multimedia-a-multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology.

[201] Z. Gong, P. Hartel, S. Nikova and B. Zhu, "Towards Secure and Practical MACs for Body Sensor Networks," in *Proc. of the 10th International Conference on Cryptology in India (INDOCRYPT 2009),* LNCS, vol. 5922, pp. 182-198, 2009.

[202] O. Özen, K. Varıcı, C. Tezcan and Ç. Kocair, "Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT," in *Proc. 14th Australasian Conference on Information Security and Privacy (ACISP 2009)*, LNCS, vol. 5594, pp. 90-107, 2009.

[203] R.C.-W. Phan, "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)," *Information Processing Letters*, vol. 91, no. 1, pp. 33-38, 2004.

[204] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *Proc. ASIACRYPT 2009,* Advances in Cryptology – ASIACRYPT 2009, pp. 1-18, 2009, doi:10.1007/978-3-642-10366-7_1.

[205] A. Biryukov and D. Khovratovich, I. Nikolić, "Distinguisher and related-key attack on the full AES-256," in *Proc. CRYPTO'09*, Advances in Cryptology - CRYPTO 2009, pp. 231-249, 2009, doi: 10.1007/978-3-642-03356-8_14.

[206] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich and A. Shamir, "Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds," in *Proc. EUROCRYPT 2010*, Advances in Cryptology – EUROCRYPT 2010, pp. 299-319, 2010, doi:10.1007/978-3-642-13190-5_15.

[207] G. Paul and J. Irvine, "Practical Attacks on Security and Privacy Through a Low-Cost Android Device," *Journal of Cyber Security*, vol. 4, pp. 33–52, 2016, doi: 10.13052/jcsm2245-1439.422.

[208] K. Herland, H. Hämmäinen and P. Kekolahti, “Information Security Risk Assessment of Smartphones Using Bayesian Networks,” *Journal of Cyber Security*, vol. 4, pp. 65–86, 2016,doi: 10.13052/jcsm2245-1439.424.

[209] K. S. Ofori, O. Larbi-Siaw, E. Fianu, R. E. Gladjah and E. O. Y. Boateng, “Factors Influencing the Continuance Use of Mobile Social Media:The Effect of Privacy Concerns,” *Journal of Cyber Security*, vol. 4, pp. 105–124, 2016, doi: 10.13052/jcsm2245-1439.426.

[210] F. Jing and H. Fei, “FAN transform in image scrambling encryption application,” in *Proc. of 2009 International Conference on Wireless Communications and Signal Processing*, Nanjing, 2009, pp. 1-4, doi: 10.1109/WCSP.2009.5371644.

[211] B. Li and J. Xu, “Period of Arnold transformation & its application in image scrambling,” *Journal of Central South University of Technology*, vol. 12, no. 1, pp. 278–282, 2005.

[212] V. Rohokale and R. Prasad, “Cyber Security for Intelligent World with Internet of Things and Machine to Machine Communication,” *Journal of Cyber Security*, vol. 4, pp. 23-40, 2015, doi: 10.13052/jcsm2245-1439.412.

[213] T. Meskanen, V. Niemi and N. Nieminen, “How to Use Garbling for Privacy Preserving Electronic Surveillance Services,” *Journal of Cyber Security*, vol. 4, pp. 41–64, 2015, doi: 10.13052/jcsm2245-1439.413.

[214] M. Abomhara and G. M. Køien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *Journal of Cyber Security*, vol. 4, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[215] A. Elmangoush and T. Magedanz, “Adaptable Protocol Selection for Reliable Smart City Services,” *Journal of Cyber Security*, vol. 6, no. 1, pp. 57–76, 2017, doi: 10.13052/jcsm2245-1439.613.

[216] A. Kanso and M. Ghebleh, “A novel image encryption algorithm based on a 3D chaotic map,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[217] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M.Vangel, D. Banks, A. Heckert, J. Dray, S.Vo and L.E. Bassham III, “A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random

Number Generators for Cryptographic Applications," NIST Special Publication, Gaitherburg, 2010. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

[218] L. Harn and T. Kiesler, "An efficient probabilistic encryption scheme," *Information Processing Letters*, vol. 34, no. 3, pp. 123-129, 1990.

[219] J. Benaloh, "Dense Probabilistic Encryption," in *Proc. Workshop on Selected Areas of Cryptography*, 1994, pp. 120–128.

[220] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," in *Proc. 18th Annual International Cryptology Conference on Advances in Cryptology*, 1998, pp. 13-25.

[221] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Proc. EUROCRYPT '99,* Advances in Cryptology: Proceedings of EUROCRYPT '99, LNCS, vol. 1592, pp. 223-238, 1999, doi: 10.1007/3-540-48910-X_16.

[222] G. Castagnos, "An efficient probabilistic public-key cryptosystem over quadratic fields quotients," *Finite Fields and Their Applications*, vol. 13, no. 3, pp. 563-576, 2007, doi: 10.1016/j.ffa.2006.05.004.

[223] B. Wang, Q. Wu and Y. Hu, "A knapsack-based probabilistic encryption scheme," *Information Sciences*, vol. 177, pp. 3981–3994, 2007.

[224] I. Damgard, M. Jurik and J. B. Nielsen, "A Generalization of Paillier's Public-Key System with Applications to Electronic Voting," *International Journal of Information Security*, vol. 9, no. 6, pp. 371-385, 2010, doi:10.1007/s10207-010-0119-9.

[225] L. Fousse, P. Lafourcade and M. Alnuaimi, "Benaloh's Dense Probabilistic Encryption Revisited," in *Proc. Progress in Cryptology – AFRICACRYPT 2011*, Proceedings of AFRICACRYPT 2011, LNCS, vol. 6737, pp. 348-362, 2011.

[226] V. A. Roman'kov, "New probabilistic public-key encryption based on the RSA cryptosystem," *Groups Complexity Cryptology*, vol. 7, no. 2, pp. 153–156, 2015, doi: 10.1515/gcc-2015-0016.

[227] I. F. Elashry, O. S. Faragallah , A. M. Abbas , S. El-Rabaie and F. E. Abd El-Samie, "A New Method for Encrypting Images with Few Details Using Rijndael and RC6 Block Ciphers in the Electronic Code Book Mode," *Information Security Journal: A*

Global Perspective, vol. 21, no. 4, pp. 193-205, 2012, doi: 10.1080/19393555.2011.654319.

[228] https://web.stanford.edu/~montanar/RESEARCH/BOOK/partE.pdf (date of last access 18th August 2019)

[229] X. Wang and H. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Optics Communications*, vol. 342, pp. 51–60, 2015.

[230] G. Gu and J. Ling, "A fast image encryption method by using chaotic 3D cat maps," *Optik*, vol. 125, pp. 4700–4705, 2014.

[231] G. Zhou, D. Zhang, Y. Liu, Y. Yuan and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[232] X. Tong, "The novel bilateral – Diffusion image encryption algorithm with dynamical compound chaos," *The Journal of Systems and Software*, vol. 85, pp. 850– 858, 2012.