STUDY AND DEVELOPMENT OF AMBTC BASED DATA HIDING METHODS

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

MASTER OF TECHNOLOGY

in

ARTIFICIAL INTELLIGENCE

by

KUSHAGRA GUPTA
(2K22/AFI/11)

Under the Supervision of

Dr. RAJEEV KUMAR
Assistant Professor, Department of Computer Science and Engineering
Delhi Technological University

Department of Computer Science and Engineering

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

June, 2024

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGMENT

I wish to express my sincerest gratitude to **Dr. Rajeev Kumar** for his continuous guidance and mentorship that he provided during research work. He showed me the path to achieving targets by explaining all the tasks to be done and explained to me the importance of this work as well as its industrial relevance. He was always ready to help me and clear our doubts regarding any hurdles in this project. Without his constant support and motivation, this work would not have been successful.

Place: Delhi **KUSHAGRA GUPTA**

Date: 31.05.2024

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **Kushagra Gupta 2K22/AFI/11**, of **M.Tech. (AI)**, hereby certify that the work which is being presented in the thesis entitled "**Study and Development of AMBTC based Data Hiding Methods**" in partial fulfillment of the requirement for the award of the degree of Master of Technology in Artificial Intelligence, submitted in the Department of Computer Science and Engineering, Delhi Technological University is an authentic record of my own work carried out during the period from to under the supervision of **Dr. Rajeev Kumar**.

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

Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor **Signature of External Examiner**

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE BY THE SUPERVISOR

Certified that **Kushagra Gupta (2K22/AFI/11)** has carried out their research work presented in this thesis entitled "**Study and Development of AMBTC based Data Hiding Methods**" for the award of **Master of Technology in Artificial Inteelligence** from the Department of Computer Science and Engineering, Delhi Technological University, Delhi under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

(Dr. RAJEEV KUMAR)

(Assistant Professor)
(Department of Computer Science and Engineering)
(Delhi Technological University)

Date:31.05.2024

ABSTRACT

Recently, Absolute Moment Block Truncation Coding (AMBTC) based data hiding methods have got popularity due to their real-time compression capability while enabling the covert communication. This capability prompt the researchers which in turn resulted in the development of both irreversible and reversible data hiding methods. In this research work, firstly a bibliometric analysis is performed over previous works, and then afterward a new adaptive AMBTC-based RDHEI technique is proposed. For bibliometric analysis over AMBTC-based data hiding methods, documents published between 2005 to 2023 in Web of Science have been considered for evaluation. The analysis is mainly done with the help of VoSViewer software. VoSViewer allows analysis based on several indices like co-authorship analysis, keyword occurrence analysis, citation analysis, co-citation analysis, etc.

After conducting a bibliometric analysis over previous research works on AMBTC-based data hiding methods, it was clear that there was some imbalance between embedding capacity and image reconstruction. So, this research work proposed a novel reversible data hiding method that utilizes adaptive AMBTC for large payload embedding. The approach begins by segmenting the image into blocks and classifying these blocks into saved and hiding blocks based on their complexity. The hiding blocks are then encoded using the AMBTC technique and further divided into multiple sub-categories based on the resulting quantization levels. The encoding of each hiding block is subsequently refined to minimize the discrepancy between the original and reconstructed images while preserving the compression ratio. Although this refined encoding produces bit-planes and quantization levels of varying sizes, it significantly expands the available space within the cover image, allowing for substantial payload embedding while ensuring complete recoverability of the original image. Experimental results demonstrate that the proposed method surpasses current state-of-the-art AMBTC-based data hiding techniques in both embedding capacity and image quality, while ensuring the original image contents' privacy.

LIST OF PUBLICATIONS

- Kushagra Gupta and Rajeev Kumar,“A Statistical Landscape Analysis of AMBTC based Data Hiding Methods” accepted to be published in “1st International Conference on Advances in Computing, Communication and Networking- ICAC2N” to be held on December 16 - 17, 2024 at ITS ENGINEERING COLLEGE, GREATER NOIDA, UP, India.
- Kushagra Gupta and Rajeev Kumar, “Adaptive AMBTC based Reversible Data Hiding in Encrypted images” accepted to be published in “ The 15th International IEEE Conference on Computing, Communication and Networking Technologies (ICCCNT)” to be held on June 24 - 28, 2024 at IIT - Mandi, Himachal Pradesh, India.

TABLE OF CONTENTS

List of Tables

List of Figures

Chapter 1

INTRODUCTION

Data hiding, a fundamental pillar of information security, refers to the practice of embedding secret messages or information within digital media like images, audio, or video files. This concealed data remains imperceptible for the casual observation, making it an effective tool for various applications like Digital watermarking, Authenticity and, integrity verification of digital dcouments. Data hiding techniques enhance security by embedding confidential information within various digital media formats such as images and videos [1]. These techniques can be broadly classified into irreversible data hiding (IDH) [2, 3], and reversible data hiding (RDH) [4, 5, 6]. While IDH methods permanently alter the original cover medium during the embedding process, RDH techniques enable the complete restoration of the original medium after the hidden data has been extracted.

This distinctive feature of RDH has garnered significant attention in fields where maintaining the integrity of the original content is crucial. For instance, in digital forensics, RDH allows investigators to extract hidden evidence without compromising the authenticity of the original evidence [7]. In medical imaging, RDH can be used to embed patient information or diagnostic details within images without affecting their clinical interpretation [8]. Military communications can leverage RDH to ensure secure transmission of covert messages while preserving the integrity of the cover images for intelligence purposes.

The ability of RDH techniques to seamlessly integrate data hiding with the preservation of original content has led to a surge in research and development in this area. By striking a balance between data confidentiality and content fidelity, RDH offers promising solutions for diverse applications where data security and integrity are paramount.

A good data-hiding algorithm should aim for high image quality with high Embedding capacity. However, it is to be noted that both the metrics are diagonal to each other. To address this concern in a sense, researchers have tried to integrate the compression methods with data hiding methods. This integration has led to development of more efficient data hiding methods with better embedding efficiency [4]. More specifically, in situations where network bandwidth is expensive or scarce, compressing the information before embedding or compressing the marked or cover media can shorten transmission times and bandwidth requirements. For this, several compression techniques such as Joint Photographic Experts Group(JPEG) [9], Graphics Interchange Format (GIF) [10], and block truncation coding (BTC) [11], LZW [12], etc. have been increasingly being used in data hiding context.

Among them, Absolute Moment Block Truncation Coding (AMBTC) which is an enhanced variant of BTC is an effective compression-based technique. The AMBTC technique splits the image into non-overlapping blocks initially, and then calculates the bit-plane and quantization levels to best represent each block. This technique generally uses a straightforward bit replacement scheme to insert the secret data into the bit planes of image blocks. As a result, the AMBTC based data hiding approaches greatly increase the embedding capacity. This has led to the development of hundreds of AMBTC based data hiding methods [13].

1.1 Problem Statement

Existing data hiding methods utilizing AMBTC often struggle to achieve a balance between high embedding capacity, maintaining visual quality of the stego image. Traditional approaches may either sacrifice image quality to accommodate more data or limit embedding capacity to maintain fidelity. This trade-off poses a significant challenge in developing effective and efficient data hiding solutions for real-world applications where both data security and image integrity are crucial.

Specifically, the problem lies in the fixed quantization levels and uniform block treatment used in many Interpolative AMBTC-based methods. These approaches fail to adapt to the varying complexity levels within an image, leading to either over-quantization in smooth regions (degrading image quality) or under-quantization in complex regions (limiting embedding capacity).

The challenge, therefore, is to develop a data hiding scheme that:

Maximizes embedding capacity without sacrificing the visual quality of the stego image. Adapts to the varying complexity levels within an image to optimize quantization and embedding strategies. Leverages the potential of all image blocks for data hiding, maximizing overall capacity. By addressing these challenges, a more efficient and adaptive data hiding solution can be developed, enabling secure and seamless embedding of confidential information within digital images without compromising their visual integrity.

1.2 Project Objective

1. To perform a Statistical Bibliometric analysis over AMBTC based Data Hiding Methods.
2. To develop a novel reversible data hiding method that utilizes adaptive AMBTC in Encrypted Images.

Chapter 2

BIBLIOMETRIC ANALYSIS

This study delves into the body of work on AMBTC-based data hiding to provide a comprehensive understanding of research trends, collaboration patterns, and recent breakthroughs in the field. Co-authorship analysis, keyword analysis, and citation analysis are just a few of the varied techniques used in the analysis [7, 14, 15]. This was used on a Web of Science (WOS) dataset that was meticulously selected and included the years 2005–2023. These complicated connections were made easier to see by creating perceptive bibliometric maps with the help of the open-source software VoSViewer.

2.1 Overview

2.1.1 Data collection source and strategy

The Web of Science (WoS), a well-known online database with a broad range of academic publications, including peer-reviewed journals and conference proceedings, has been mined for the data needed for this work.

A focused search on the WoS was carried out on March 25, 2024, in order to find pertinent research articles related to the given subject. The search terms used in the search were ((RDH OR hidden OR steganograph* OR watermark* OR RDHEI) (Topic) and ((Block Truncation Coding) OR BTC OR AMBTC OR absolute moment block truncation coding") (Topic)). The search was conducted from 2005 to 2023. The search resulted in the identification of a dataset containing 142 documents. These documents formed the basis for subsequent bibliometric analysis.

2.1.2 Annual publications

An annual progression of research publications of AMBTC based Data Hiding methods in the WoS is presented in Fig 2.1. According to Fig 2.1, since 2005 there were only two to six publications in each year. But from 2017 onwards, there can be seen a gradual upturn in the number of publications.

This increment in publications signifies the wide use of Reversible data-hiding techniques in the industry. And, the annual citation diagram in Fig 2 also confirms the increased use of Reversible Data hiding techniques.

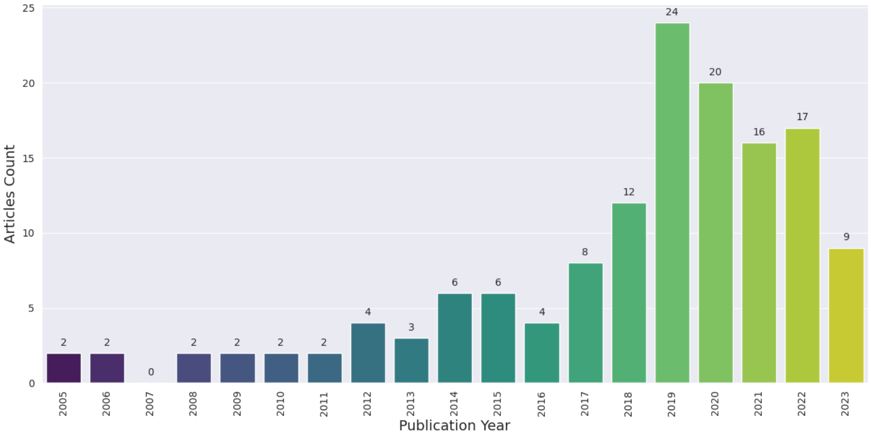


Figure 2.1: Yearly (from 2005 to 2023) publications trend

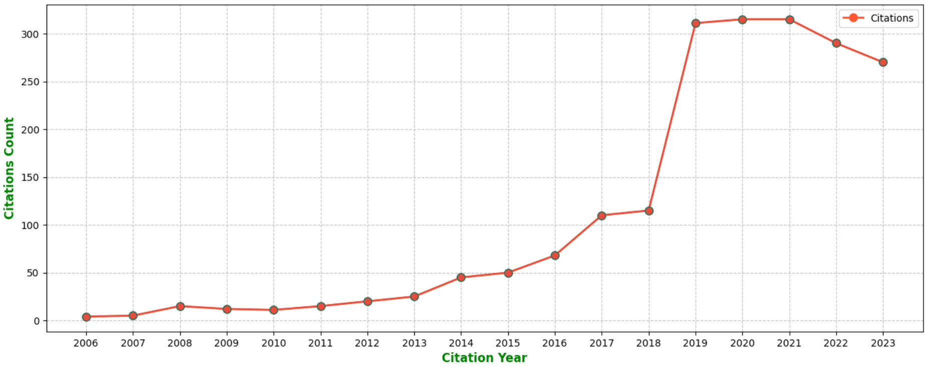


Figure 2.2: Yearly (from 2006 to 2023) citations trend

2.1.3 Annual Citations

Figure 2.2 illustrates the annual citations received by publications on AMBTC-based data hiding methods from 2006 to 2023. Initial years (2006-2010) saw modest citations (5-20 annually). A gradual increase in citations began in 2011. Citations peaked between 2019-2021, highlighting significant recognition of work in reversible data hiding.

2.1.4 Article type

Since the WoS contains a wide variety of publications, the analysis to gain insights about distribution of the articles based on their types of the obtained corpus of 142 documents is presented in Fig 2.3. The analysis shows that the research articles made up the largest cluster of 138 documents(out of 142). Then, four Early access documents created the second largest group, followed by three Review Articles, two Proceeding papers, and one correction paper out of 142 total documents.

It is to be noted that research articles report the findings of original research studies in a standard format, early access documents are articles accepted by a journal but

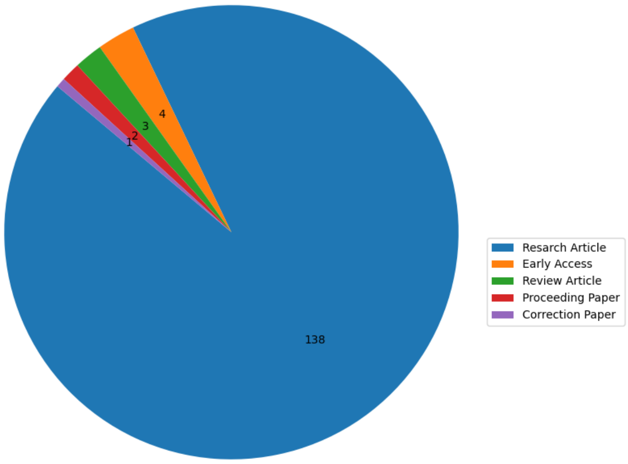


Figure 2.3: Article Types

still awaiting final formatting. Review articles offer a critical summary of research on a specific topic, rather than presenting new findings. Proceeding papers are research presented at academic conferences, and correction papers are used to correct major errors in previously published research.

2.1.5 Publishing sources

Fig 2.4 depicts the top publishing sources of reserach related to AMBTC based data hiding methods. In the Fig 2.4, “Multimedia Tools and Applications” secures the first spot after publishing 40 documents, it constitutes 28.2 % of total documents. The second position is achieved by “APPLIED SCIENCES” with 11 documents (7.8%) followed by “IEEE Access” with a publication count of 9 (6.4%). Moreover, several important sources are “SYMMETRY”, “KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS”, “ELECTRONICS” and “FUNDAMENTAL INFORMATICAE” with publication counts of 8, 7, 5 and 3, respectively.

2.1.6 Productive researchers and organizations

Fig. 2.6 highlights the most influential authors in AMBTC-based data hiding research. From the Fig. 2.6, It can cleraly seen that “Chang, Ching-Chun” leads the field with an impressive 35 documents. “Lin, Chia-Chen” follows closely with 25 documents. Other significant contributors include “Yang, Ching-Nung” (13 documents), “Kim, Chenshik” (12 documents), “Hong, Wein” (11 documents), and “Hu, Yu-Chen” (9 documents).

As far as productive organization are concerned, Fig. 2.7 showcases the distribution, where “Feng Chia University” (Taiwan) tops the list with 36 documents, closely followed by “Providence University” (Taiwan). Notable contributions also come from “National Dong HWA University” (Taiwan), “Sejong University” (South Korea), and

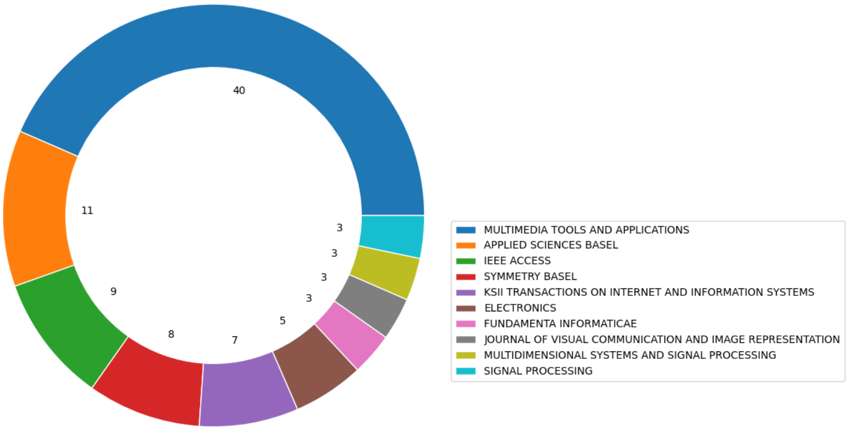


Figure 2.4: Top Journals in the domain

"Asia University" (Taiwan) with 14, 13, and 7 documents, respectively.

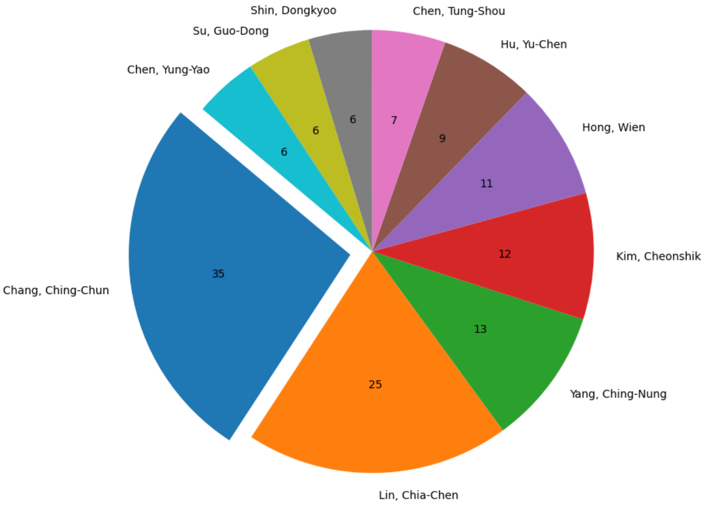


Figure 2.5: Top contributing authors

2.1.7 Country trends

Fig. 2.7 highlights the geographic distribution of publications. Taiwan emerges as the most prolific contributor with 94 publications. China follows with 62. South Korea, India, and Vietnam also demonstrate significant research output with 18, 16, and 6 publications, respectively. The presented results about Top 10 countries reflect a diverse geographic spread, with five from Asia, two from Europe, and one each from Africa, North America, and Australia. This geographic diversity highlights the widespread interest in AMBTC-based data hiding research across the globe.

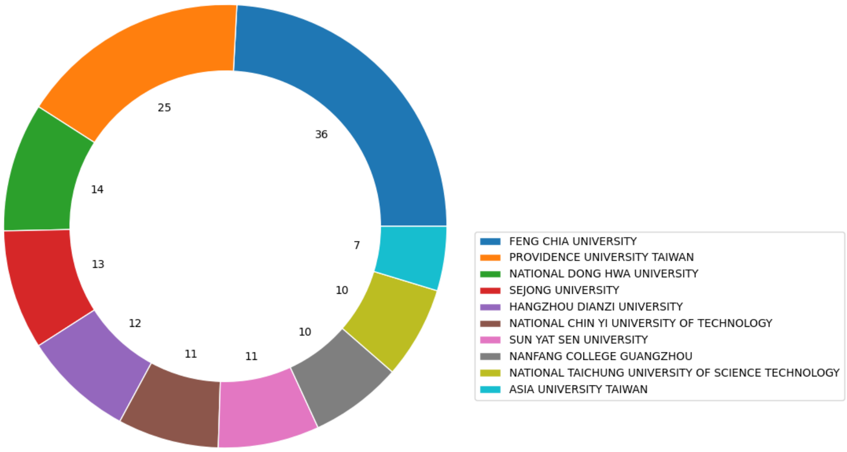


Figure 2.6: Top contributing organizations

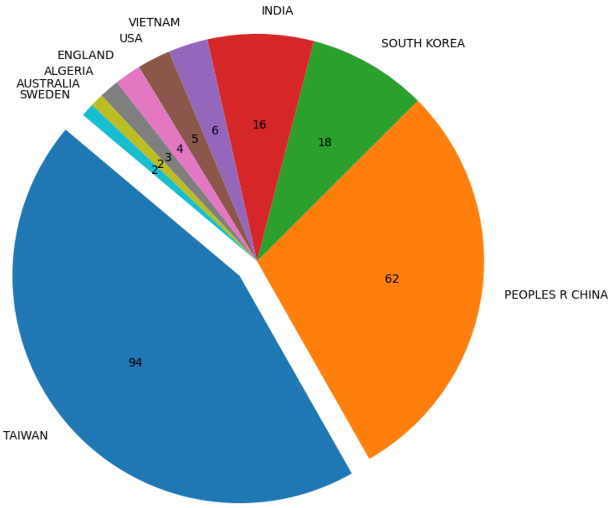


Figure 2.7: Country-wise publications

2.2 Co-authorship analysis

2.2.1 Author co-author linkages

For identifying author co-author linkages, VosViewer made a thorough analysis of a dataset of 142 documents. In the analysis, and a total of 236 authors were identified. For a smoother analysis, large documents(documents having more than 25 authors) were ignored. During this research, authors having a minimum of 3 documents and 2 citations each are considered for evaluation along with a Full counting method. All the above criteria are fulfilled by 35 authors, out of them only 21 authors are in a closed co-authorship connection.

The obtained results showcasing Author, documents published, citations received, and Link strength (counting of total co-authored publications), are summarized in Ta-

Table 2.1: Authors co-author linkages

Rank	Author	Documents	Citations	Link Strength
1	Chang, Chin-Chen	35	478	44
2	Lin, Chia-Chen	26	284	40
3	Hong, Wien	13	182	21
4	Kim, Cheonshik	12	165	18
5	Yang, Ching-Nung	11	209	18
6	Hu, Yu-Chen	9	122	9
7	Chen, Tung-Shou	6	128	9
8	Leng, Lu	6	118	11
9	Su, Guo-Dong	6	60	12
10	Chen, Yung-Yao	6	54	2
11	Zhou, Xiaoyu	6	33	13
12	Guo, Jing-Ming	5	155	0
13	Tai, Wei-Liang	5	120	8
14	Shin, Dongkyoo	5	86	10
15	Malik, Aruna	5	71	5
16	Kumar, Rajeev	5	64	5

ble 1. It is to be noted that only the authors having the highest co-authorship linkages are present in the Table 1, where Chang, Chin-Chen emerges at the top of the list with 35 documents, 478 citations, and 44 link strengths. Next in the line is Lin, Chia-Chen with 26 documents, 284 citations, and 40 link strength. It can further be noted that the list contains two researchers from India namely Aruna Malik(5 documents, 71 citations) and Rajeev Kumar(5 documents, 64 citations).

The co-authorship network map is presented in Fig. 2.8. In the Fig. 2.8, there are several author networks and each network is represented using a different color. An author having a higher publications count is represented using a larger node and a thicker connection link signifies a strong linkage. Moreover, the Fig. 2.8 has 6 colored clusters, where Green-colored cluster has the presence of Chang, Chin-Chen along with Wang, Xuand other researchers. Similarly, the Yellow cluster shows the presence of Lin, Chia - Chen along with Tai, Wei-Liang, and 2 other authors. 3rd Researcher in Table 2, Hong, Wien is present in Red Cluster along with Zhou, Xiaoyu, and 3 authors. 6th ranked author Hu, YU-Chen dominated the blue cluster along with Chen, Yung-Yao, and the other 3 authors. On the other hand, the Violet cluster has only the presence of Nguyen, thai-son. The Sky-blue cluster contains Sum Guo-Dong.

2.2.2 Organizational co-author linkages

For identifying organizational co-author linkages, VosViewer search was applied to 142 documents and as a result, 120 organizations were identified. For better analysis, documents co-authored by more than 25 organizations were ignored. For this research,

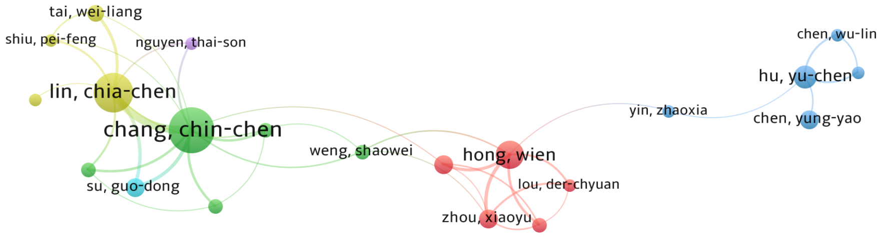


Figure 2.8: Author co-author networks

organizations having a minimum of 3 documents and 2 citations each were considered for evaluation along with a Full counting method. Out of 120 institutions, 36 organizations satisfied above defined requirements.

Table 2 defines the co-authorship linkages between the top 10 organizations. The details presented in Table 2, are Organization, Country, documents published, citations received, and Link strength(counting of total co-authored publications). As evident from Table 2, seven organizations are from Taiwan, two from China, and one from South Korea. “Fen Chia University” from Taiwan floats on the top of the list with 37 documents and 505 citations. Then, it is followed by “Providence University” with 25 documents and 376 citations. Two universities from China are present at rank 5 and 6. “Sejong University” from South Korea made it to the list at fourth spot.

The organization co-authorship network map is present in Fig. 2.9. The whole network is represented using 5 different clusters. A larger node denotes the organization with a higher publication count. Feng Chia University, the top contributor, stands out within the Red Cluster alongside eight other organizations. The Blue Cluster features Providence University (ranked 2nd) and Chinese Culture University, among others. The Yellow Cluster includes National Dong Hwa University (3rd) and Sejong University (4th), along with three additional organizations. Sun Yat-Sen University dominates the Green Cluster, while Asia University is a key player in the Violet Cluster.

2.2.3 Country co-author linkages

For identifying country co-author linkages, VosViewer search was applied to 142 documents and as a result, 16 countries were identified. For better analysis, documents co-authored by more than 25 countries were rejected. To get a wider view of the anal-

Table 2.2: Organization co-author linkages

Rank	Organization	Country	Documents	Citations	Link Strength
1	Feng Chia University	Taiwan	37	505	71
2	Providence University	Taiwan	25	376	44
3	Natl Dong Hwa University	Taiwan	14	261	22
4	Sejong University	South Korea	13	174	20
5	Hangzhou Dianzi University	China	12	89	30
6	Sun Yat Sen University	China	11	197	12
7	Natl Chin Yi University of Technology	Taiwan	11	34	18
8	Natl Taichung University of Science & Technology	Taiwan	10	86	19
9	Natl Taiwan University of Science & Technology	Taiwan	7	157	4
10	Asia University	Taiwan	7	67	11

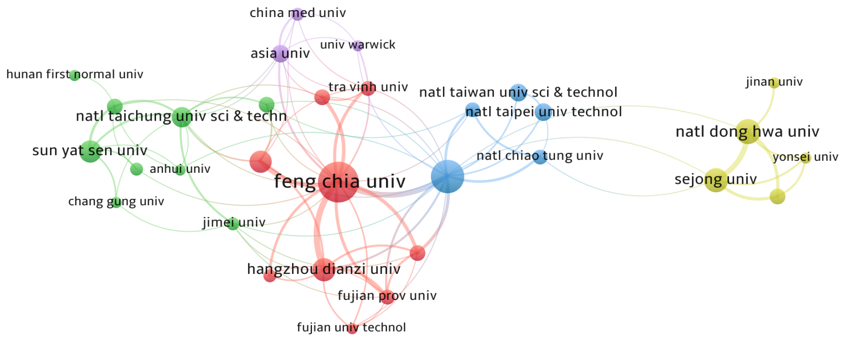


Figure 2.9: Organization co-author networks

ysis, countries having at least 1 document published and having at least 1 citation each will be considered. The Full counting method was used during this analysis. Out of 16 countries, 13 satisfied the above requirements. Table 3, contains the countries with the top ten highest total link strength. Out of the top 10 countries, five countries belong to Asia, two countries belong to Europe, one belongs to Africa, one belongs to North America and one is Australian. In Table 3, Taiwan pops at the top of the list with 94 documents and 64 link strength. Then China comes to the second spot. India comes in the fourth position with 16 documents. England and Sweden grab 7th and 10th position in the list. Australia marks its presence with 2 documents in the list.

The country co-authorship network map is present in Fig. 2.10. The whole network is represented using three different clusters. A larger node denoted the country having a higher number of publications. The Red cluster contains the top 4 ranked countries Taiwan, China, South Korea, and India along with Turkey and Indonesia. The Green cluster is dominated by Vietnam, the USA along Australia. Blue Cluster contains two countries Algeria and England.

Table 2.3: Country co-author linkages

Rank	Country	Documents	Citations	Link Strength
1	Taiwan	94	1379	67
2	Peoples R China	62	829	56
3	South Korea	18	246	23
4	India	16	119	1
5	Vietnam	6	89	7
6	USA	5	66	9
7	England	4	74	6
8	Algeria	3	45	2
9	Australia	2	26	4
10	Sweden	2	3	2

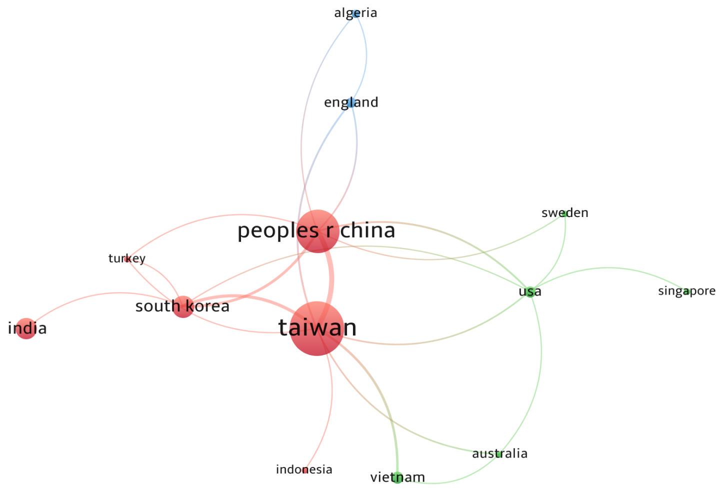


Figure 2.10: Country co-author networks

2.3 Keyword co-occurrences

In any field of research, the co-occurrence of keywords in published articles offers significant insights into associated topical trends and critical areas of study focus. A study of the co-occurrence of keywords in the domain of AMBTC based Data Hiding Methods, is presented in the following paragraphs.

For the Keyword co-occurrences, VosViewer made a thorough analysis of a dataset of 142 documents from the year 2005 to 2024. A total of 415 keywords were identified. During this research, keywords having at least 3 occurrences were considered for evaluation along with a Full counting method. All the above criteria are fulfilled by 61 keywords, in a closed connection network.

The Keyword co-occurrence list is tabulated in Table 4. “Steganography” keywords come at the top of the list with 47 occurrences and a total link strength of 187. Rank 2

Table 2.4: Keywords co-occurrence linkages

Rank	Keyword	Occurrences	Link Strength
1	Steganography	47	187
2	Ambtc	45	188
3	Data Hiding	43	146
4	Scheme	33	145
5	Block Truncation Coding	28	84
6	Watermarking	27	118
7	Reversible Data Hiding	25	85
8	Image Authentication	20	86
9	Tamper Detection	18	78
10	Absolute Moment Block Truncation Coding	15	54

is achieved by “AMBTC” with 45 occurrences and 188 link strength. “Reversible Data Hiding” comes at Rank 7 in the list with 25 occurrences and 85 link strength. The list is terminated by the “Absolute Moment Block Truncation Coding” keyword with 15 occurrences. The Keyword co-occurrence network map is present in Fig. 2.11. The whole network is represented using four different clusters. A larger node denoted the keyword having a higher number of occurrences. The Red cluster shows the presence of the “Steganography” keyword along with other top keywords like “AMBTC”, “Data Hiding” and “Scheme”. The Green cluster is led by ’‘Watermarking” keyword, along with “Image Authentication” and “Temper detection”. The blue cluster contains the “Reversible Data Hiding” keyword along with “Absolute Moment Block Truncation Coding”. The yellow cluster contains keywords like “Image compression”, “Algorithm” etc.

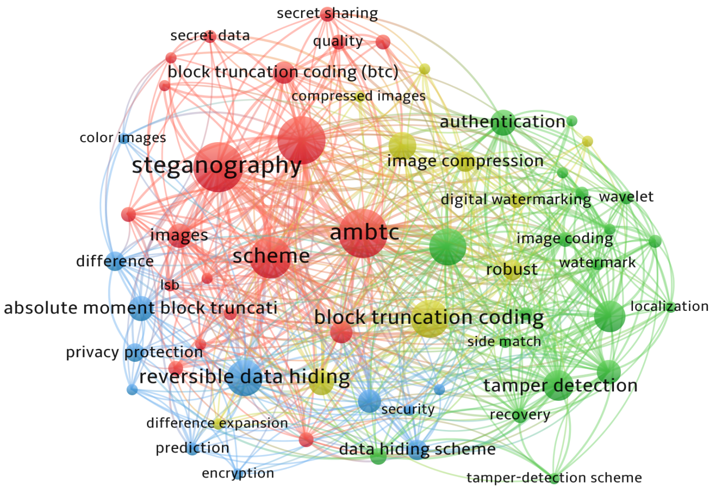


Figure 2.11: Keywords co-occurrence networks

Table 2.5: Author citation linkages

Rank	Author	Citations	Documents	Link Strength
1	Chang, Chin-Chen	478	35	554
2	Lin, Chia-Chen	284	26	405
3	Yang, Ching-Nung	209	11	145
4	Hong, Wien	182	13	299
5	Kim, Cheonshik	165	12	162
6	Guo, Jing-Ming	155	5	27
7	Sun, Wei	150	4	166
8	Chen, Tung-Shou	128	6	172
9	Hu, Yu-Chen	122	9	159
10	Tai, Wei-Liang	120	5	148

2.4 Citation analyses

Citation analysis is a powerful approach that, using citations as a basis, reveals the relationships between different participants in a certain study topic. These connections between countries, organizations, sources, papers, and researchers and explained in the subsections that follow. Within the study topic under investigation, these analyses provide fascinating details about important and cooperative relationships.

2.4.1 Author citation linkages

VosViewer made a detailed analysis of a dataset of 142 documents, and a total of 236 authors were recognized. To have a better analysis of citations between researchers, documents having more than 25 authors were ignored. During this research, authors having a minimum of 3 documents and 2 citations each are considered for evaluation along with a Full counting method. All the above criteria are fulfilled by 35 authors.

Table 5 tabulated the details of the most cited authors such as author name, number of citations received, documents published, and total link strength. Chang, Chin-Chen topped the list with the highest citation of 478, 35 documents, and 554 link strength. Then, Lin, Chia-Chen comes to the second spot with 284 citations and 26 documents. The List is terminated by Tai, Wei-Liang with 120 citations after having 5 documents.

Figure 2.12 displays the citation linkage network between authors working on Reversible data hiding. Citation map has total four clusters(Green, Red, Yellow, and Blue) with different colors. Green cluster group the most cited authors Yin Zhaoxia(Rank 1) Zhang Xinpeng(Rank 2), and Tang Zhenjun(Rank 6). Similarly third most cited author is present in the Red cluster groups along with Ma bin and He Wenguang. Yellow cluster has the fourth most cited author Rajeev Kumar along with Samayveer Singh, Neeraj Kumar, and Ki-Hyun, Similarly, Blue colored cluster has the presence of Pan Zhibin along with other authors such as Zhang Xiaoran, Zhou Quan, Fan Guojn, and Gao Erdun.

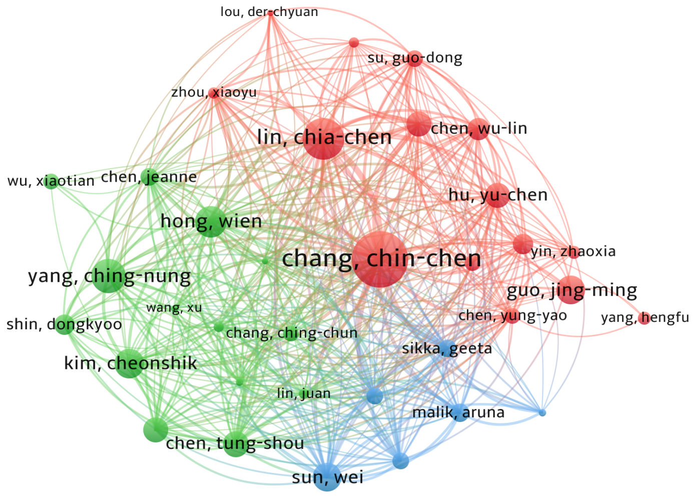


Figure 2.12: Author citation networks

2.4.2 Documents Citation linkages

The entire corpus of 142 published documents that were taken for the purpose of 'A Statistical Landscape Analysis of AMBTC based Data Hiding Methods' was subjected to a thorough VoSViewer analysis. In order to analyze citations among documents with at least five citations apiece, the full counting approach was used. A total of 89 documents satisfied this requirement, out of which 84 created the biggest network of citation links. Table 6 lists the 10 most often cited documents. This table includes Article name, author name, Journal name, Publishing year, Citations received and total links. As evident from the Table 6, 'Lossless data hiding for color images based on block truncation coding'[16] received the highest number of 94 citations and was published in 'Pattern Recognition' journal in year 2008. It is followed by 'Non-uniform Watermark Sharing Based on Optimal Iterative BTC for Image Tampering Recovery'[17] with 73 citations.

The documents citation network map is depicted in Fig. 2.13, where the whole network is represented in 11 different clusters. A higher citation document is represented using a bigger node. The main nodes of the yellow cluster are the articles published by Chang et al.[16] (Rank 1) and Qin et al.[17] (rank 2), whereas the major nodes of the orange cluster are the documents published by Sun et al. [18] (rank 3), Chang et al. [19] (rank 10), and Kumar et al. [20](rank 11). In the same way, Ou[21] (rank 4) is the prominent publisher in the blue cluster.

2.5 Review of Previous Works

Reversible data hiding (RDH) is a cutting-edge technique that addresses a critical concern in data security and integrity. Unlike traditional data hiding methods, RDH allows for the complete recovery of the original cover medium (e.g., an image, audio file, or

Table 2.6: Documents citation linkages

Rank	Title of Article	Authors	Year	Journal	Citations	Links
1	Lossless data hiding for color images based on block truncation coding [16]	Chin-Chen Chang; Chih - Yang Lin; Yi-Hsuan Fan	2008	Pattern Recognition	94	21
2	Non-uniform Watermark Sharing Based on Optimal Iterative BTC for Image Tampering Recovery[17]	Chuan Qin; Ping Ji; Chin-Chen Chang; Jing Dong; Xingming Sun	2018	IEEE MultiMedia	73	4
3	High performance reversible data hiding for block truncation coding compressed images[18]	Wei-Yeh Sun; Zhe-ming Lu; Yu-Chun Wen; Faxin Yu; Rong-Jun Shen	2013	Signal, Image and Video Processing	68	23
4	High payload image steganography with minimum distortion based on absolute moment block truncation coding[21]	Duanhao Ou; Wei Sun	2015	Multimedia Tools and Applications	62	26
5	Lossless data hiding for absolute moment block truncation coding using histogram modification[22]	Cheonshik Kim, Dongkyoo Shin, L. Leng, Ching-Nung Yang	2016	Journal of Real-Time Image Processing	62	8
6	Steganography for BTC compressed images using no distortion technique[23]	Jeanne Chen, Wien Hong, Tung-Shou Chen, Chih-Wei Shiu	2010	The Imaging Science Journal	60	22
7	A novel reversible data hiding scheme based on AMBTC compression technique[24]	Lin, Chia-Chen; Liu, Xiao-Long; Tai, Wei-Liang; Yuan, Shyan-Ming	2015	Multimedia Tools & Applications	52	19
8	Content-Based Image Retrieval Using Error Diffusion Block Truncation Coding Features[25]	Guo, Jing-Ming and Prasetyo, Heri and Chen, Jen-Ho	2015	IEEE Transactions on Circuits and Systems for Video Technology	52	2
9	A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain[26]	Nguyen, Son and Chang, Chin-Chen and Yang, Xiao-Qian	2016	AEU - International Journal of Electronics and Communications	48	2
10	High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding[19]	Chang, I-Cheng and Hu, Yu-Chen and Chen, Wu-Lin and Lo, Chun-Chi	2015	Signal Processing	46	14

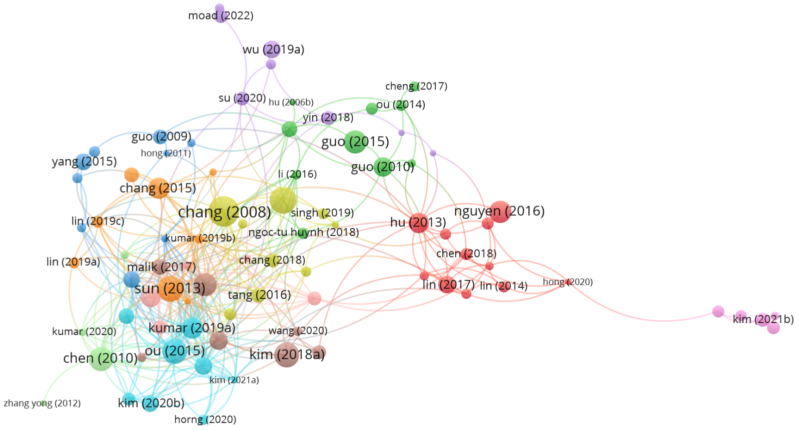


Figure 2.13: Document Citation network

video) after the embedded data has been extracted. This ability to restore the host medium to its pristine state makes RDH invaluable in applications where the integrity of the original content is paramount.

Reversible Data Hiding in Encrypted Images (RDHEI) is a novel topic that has emerged as a result of extensive study over the past ten years and more on the integration of RDH with encryption methods [27].Using the AES-128 approach for image encryption, Puech et al. [28] presented one of the pioneering creations in RDHEI. This approach was novel, but it suffered from an issue of low embedding capacity and was even not able to fully regenerate the cover image. Zhang [29] introduced an unexplored RDHEI technique in 2011 that encrypts the image blockwise. First, an XOR operator is applied, and then a random encryption key is generated. By utilizing this method, the regenerated cover medium's visual quality is enhanced and its embedding capacity is increased. However, only when the block size is larger than 32×32 pixels can the approach produce optimal results. Furthermore, Zhang [30] created an alternative RDHEI technique in which the least significant bits of the image are compressed to free up a large amount of room for secret data hiding. This method achieves a compromise between the requirement for a large data hiding capacity and the capability to recreate the original cover image. A series of improvements were then made with the goal of determining the ideal ratio between embedding capacity (EC) and the image quality

[31, 32].

Cao et al. [33] investigated redundancy in image patches in 2015 by encoding the residual errors to produce a significant data hiding space and using sparse coefficients to represent the original image. Despite these improvements, achieving an optimal balance required compromising either reversibility or embedding capacity. This paradigm shifted with the work of Puteaux et al. [34], who introduced entirely reversible RDHEI methods, opening new research avenues focused on enhancing embedding capacity (EC). Puyang et al. [35] expanded on this by using two MSBs for data embedding, unlike Puteaux et al. [34], but left potential for further increasing EC by not fully utilizing the lower MSBs.

In line with improving embedding capacity, various RDHEI techniques have been developed to achieve high embedding capacity while ensuring complete reversibility and cover media privacy [36, 37, 38, 39]. Among these, Shiu et al. [39] adopted a unique approach using Interpolative AMBTC to create more space in the image. This method uses an 8-bit bit plane instead of a 16-bit bit plane, thereby increasing hiding capacity. It also leverages the difference between the image blocks and the reconstructed blocks, compressing them with Huffman coding to regenerate the cover media, thus achieving lossless reconstruction of the original image while providing substantial data hiding capacity. Mittal et al. [11] discussed a novel RDHEI method utilizing both AMBTC and rhombus mean for accurate prediction and creating large embedding spaces. Similarly, this research work proposes a new RDHEI method based on the adaptive AMBTC technique for further increasing the embedding capacity. The proposed method employs the adaptive AMBTC [40] to minimize the difference between the reconstructed AMBTC image and the original image, thereby increasing the embedding space. Moreover, the proposed method is able to ensure complete reversibility and original image contents' privacy.

Chapter 3

PROPOSED WORK - ADAPTIVE AMBTC BASED RDHEI

This section discusses the proposed technique for embedding the secret data within the image itself along with AMBTC codes. The main aim of this proposed work is to enhance the data hiding capacity while maintaining the quality of stego-image. Initially, the suggested approach classifies the original image blocks into two categories: Saved and Hiding Blocks. During embedding, secret data can be embedded into hiding blocks only. Furthermore hiding blocks are divided into four other categories: Absolute Smooth, Slightly Smooth, Slightly Complex, and Absolute Complex as described by Kumar et al. [40].

3.1 Proposed Technique

This section discusses the proposed RDHEI method, which is an extension of Shiu et al. method [39]. The proposed method makes use of an adaptive AMBTC technique introduced by Kumar et al. [40] for reducing magnitude of the difference errors. For this, the image is initially is divided into blocks and then each block is classified either as Saved and Hiding Block, depending on its texture level. It is to be noted that the hiding blocks are then used for embedding the secret data by first dividing them into four other classes: Absolute Smooth, Slightly Smooth, Slightly Complex, and Absolute Complex as in [40]. The detailed working of the proposed method is provided as follows:

3.1.1 Block Classification and Marking

Initially, the original Image (I) is split into 4×4 size blocks. After splitting, the classification of blocks, into Saved or Hiding blocks, is performed. More specifically, a variance V_i is calculated for each block of I using Eq. 3.1.

$$V_i = \frac{1}{16}\sum_{k=1}^{16}(x_k - AVG)^2 \tag{3.1}$$

where i represents block number, x_k denotes k^{th} pixel value and AVG denotes the average value of i^{th} block that can be calculated using Eq. 3.4. If $V_i \geq Thr_V$, then i^{th}

block will be considered as saved block otherwise a hiding block, where Thr_V is a user-defined threshold. It is to be noted that hiding blocks are considered for embedding as these blocks are smoother and have high potential of being compressed and provide good embedding space. At the receiver's end during extraction phase, blocks needs to be identified. So, marking is required in both blocks. In a 4x4 block of 16 pixels, pixel x4 is used as a marking pixel.

Marking procedure for Hiding block is defined in eqn. 3.2:

$$x'_4 = floor(x_4/2) * 2 + 1; \tag{3.2}$$

Marking procedure for Saved block is defined in eqn.3.3:

$$x'_4 = floor(x_4/2) * 2 + 0; \tag{3.3}$$

At the receiver's end during extraction phase, blocks needs to be identified. So, marking is required in both blocks. In a 4x4 block of 16 pixels, pixel x4 is used as a marking pixel.

3.1.2 AMBTC Code Generation

After categorizing the image blocks into saved and hiding blocks, the secret data is concealed by creating embedding space inside the image. For this, the hiding blocks are used as these blocks have lesser variance. More specifically, the hiding blocks are encoded using adaptive AMBTC technique to create space for embedding. The adaptive AMBTC technique basically categorizes the hiding blocks into four sub-categories on the basis of their complexity levels. The complete step by step algorithm for the AMBTC code generation for the hiding blocks can be summarized as follows:

Input- $\mathscr{B}$: Hiding Block of size 4×4, $Thr1$: First threshold, $Thr2$: Second threshold.

Output- Adaptive AMBTC codes

Step 1: Apply AMBTC on hiding blocks Firstly each of the hiding block is encoded using original AMBTC technique by following steps 1.1, 1.2 and 1.3:

Step 1.1: Block Average Calculation

Calculate average (or mean) of each block using Eq. 3.4.

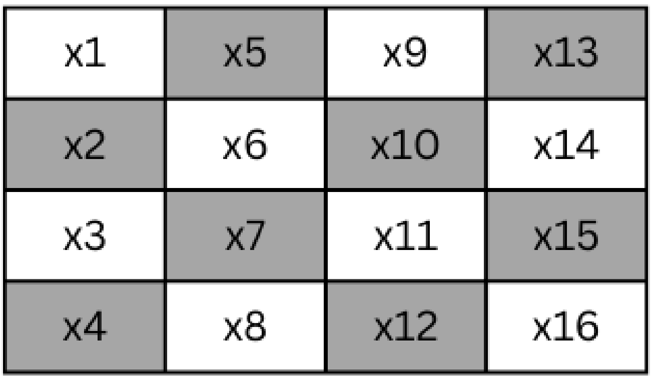
$$AVG = \frac{\sum_{k=1}^{16} x_k}{4 \times 4} \tag{3.4}$$

Step 1.2: Bit Plane Generation

Create a bitmap b for the block based on the following conditions:

- If $x_k \geq AVG$, then '0' will be placed at k^{th} location in b.
- Else '1' is placed.

Step 1.3: Quantization Level Calculation



x1	x5	x9	x13
x2	x6	x10	x14
x3	x7	x11	x15
x4	x8	x12	x16

Figure 3.1: Reduced bitmap, where gray pixels are dropped at the encoding stage and predicted at the decoding stage with the help of a given interpolation formula

Lower and Higher level Quantization values, to represent the block, are calculated using Eq. 3.5:

$$\mathrm{L} = \sum_{x_k < \mathrm{AVG}}^{4\times4} x_k/\mathrm{qH} = \sum_{x_\mathrm{k} \geq \mathrm{AVG}}^{\mathrm{M}\times\mathrm{M}} \mathrm{x_k}/(4\times4-\mathrm{q}) \tag{3.5}$$

where, q is the count of 0's in b.

Step 2: Calculate Quantization difference

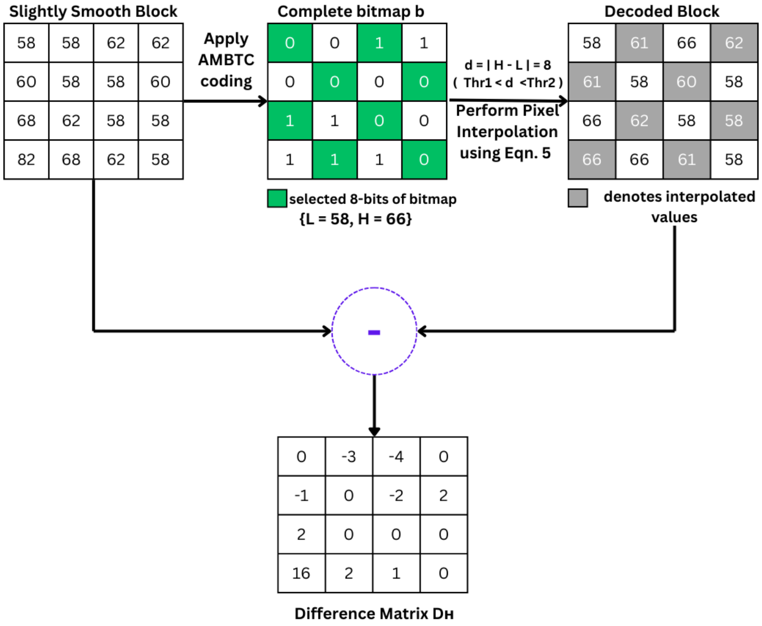
Quantization difference d is calculated in order to classify hiding blocks into different categories as: d = $|H-L|$

Step 3: Absolute Smooth Block(ASB)

If difference value $d \leq Thr1$, then the hiding block is an Absolute Smooth Block (ASB). In this case, AVG is used as the only quantization level to represent the block. Moreover, 2-bit classifier '00' is used for the block identification. Therefore, the AMBTC code for the ASB is $\{AVG\}$.

Step 4: Slightly Smooth Block(SSB)

If $Thr1 < d \leq Thr2$, then the hiding block is a Slightly Smooth block (SSB). In this case, there are two quantization levels L, H and reduced bitmap (b^r) of 8 bits as shown in 3.1, which are used for block representation. Here, pixels depicted in white color (as in Fig. 3.1) are only need to be recorded in the bitmap while grey color pixels can be interpolated using Eq. 3.6 at the time of decoding. Moreover, '01' is used for block identification.



Slightly Smooth Block

58	58	62	62
60	58	58	60
68	62	58	58
82	68	62	58

Complete bitmap b

0	0	1	1
0	0	0	0
1	1	0	0
1	1	1	0

Decoded Block

58	61	66	62
61	58	60	58
66	62	58	58
66	66	61	58

Difference Matrix DH

0	-3	-4	0
-1	0	-2	2
2	0	0	0
16	2	1	0

Figure 3.2: Illustration of encoding procedure of a slightly smooth block

$$x'_k = \begin{cases} \frac{x_{k-1}+x_{k+1}+x_{k+4}}{3} & ifk = 2 \\ \frac{x_{k-1}+x_{k+4}}{2} & ifk = 4 \\ \frac{x_{k-4}+x_{k+1}+x_{k+4}}{3} & ifk = 5 \\ \frac{x_{k-4}+x_{k-1}+x_{k+1}+x_{k+4}}{4} & \\ \frac{x_{k-4}+x_{k-1}+x_{k+4}}{3} & ifk = 7,10 \\ \frac{x_{k-4}+x_{k+1}}{2} & ifk = 12 \\ \frac{x_{k-1}+x_{k+1}+x_{k-4}}{3} & ifk = 13 \\ & ifk = 15 \end{cases} \tag{3.6}$$

Thus, the AMBTC code for the SSB will be $\{L, H, b^r\}$. The complete encoding process for SSB is illustrated in Fig.3.2 with the help of an example.

Step 5: Complex Block Classification

If $d \geq Thr2$, then the block $\mathscr{B}$ is either a Sightly Complex block (SCB) or Absolute Complex block (ACB). To exactly identify whether the block $\mathscr{B}$ is an SCB or ACB, following process is followed:

Step 5.1: Group Formation

Split the block $\mathscr{B}$ into two groups: the first group (IZ), which includes all '0' pixels and the second group (IO), which includes all '1' pixels of the bitmap b.

Step 5.2: Count the number of pixels in every group

Determine how many pixels are there in each of the groups.

Step 5.3: Any group having more than 9 pixels

The block is considered a SCB if the value of $(count(IZ)$ OR $count(IO)) > 9$ and following steps are performed otherwise the block $\mathscr{B}$ is an ACB and '11' is used as the block classifier for identification of the ACB.

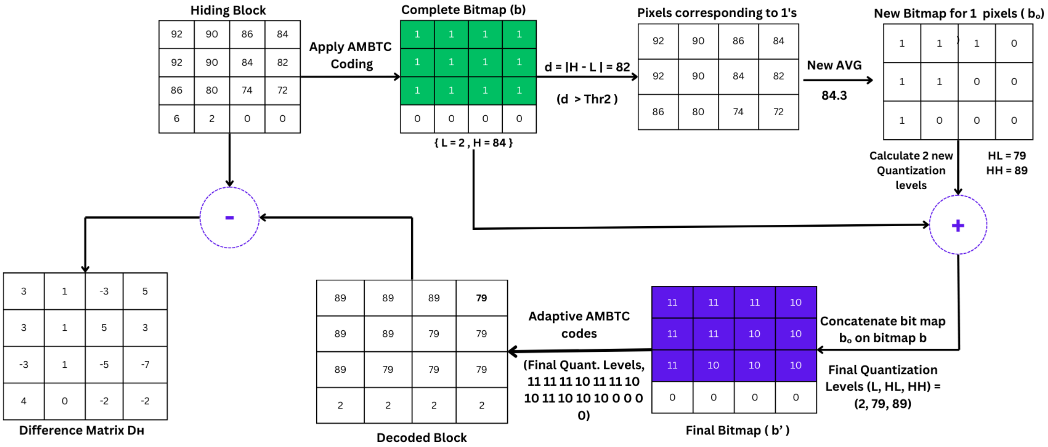


Figure 3.3: Illustration of encoding procedure of a slightly complex block with more ones

1. If $count(IZ) > 9$, apply step-1 for the first group (IZ) to obtain two new quantization levels, namely LL and LH and bitmap b_z.

2. Impose(or concatenate) bitmap b_z over the original bitmap b to get a new resultant bitmap $b^{'}$. Thus, the first group bitmap contains pixels having values of '00' or '01' and the second group contains pixels having the value '1' only.

3. Thus, the block is represented by a new bitmap $b^{'}$, and three quantization levels, LL, LH, and H; and '10' is used as the block classifier for identification.

4. If $count(IO) > 9$, apply step-1 for the second group (IO) to obtain two new quantization levels, namely HL and HH and bitmap b_o.

5. Impose(or concatenate) bitmap b_o over the original bitmap b to get a new resultant bitmap $b^{'}$. Thus, the second group bitmap contains pixels having values of '10' or '11' and the first group contains pixels having the value '0' only.

6. Thus, the block is represented by a new bitmap $b^{'}$, and three quantization levels, L, HL, and HH; and '10' is used as the block classifier for identification.

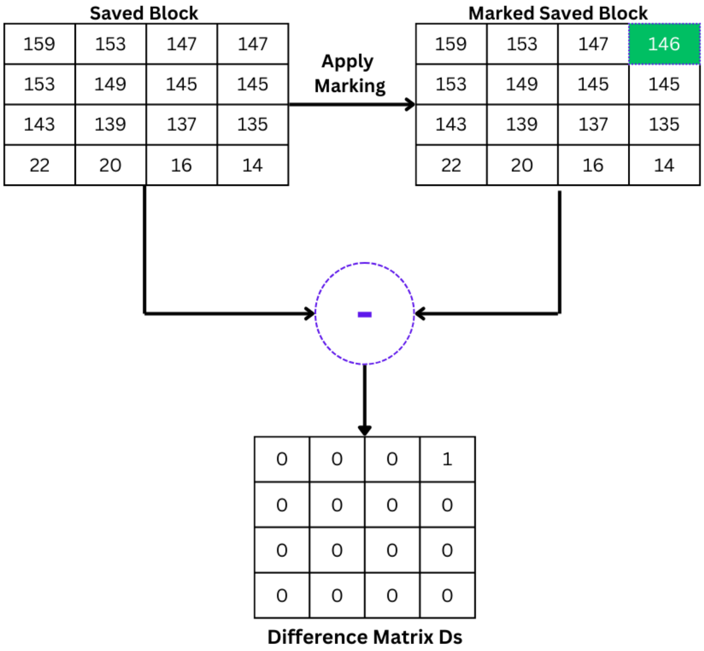
The whole encoding process of Slightly Complex Block with more ones is illustrated in the Fig. 3.3, with an example.

Step 5.4: Both groups have 9 pixels equally

The block is considered as an ACB if the value of $(count(IZ)$ AND $count(IO)) = 9$. In this case, data embedding is not possible in the block. So, the block will be treated as a saved block indirectly.

3.1.3 Data Embedding Procedure

In this sub-section, we outline the complete data embedding algorithm of the proposed method in step by step manner as follows:



Saved Block

159	153	147	147
153	149	145	145
143	139	137	135
22	20	16	14

Marked Saved Block

159	153	147	146
153	149	145	145
143	139	137	135
22	20	16	14

Difference Matrix Ds

0	0	0	1
0	0	0	0
0	0	0	0
0	0	0	0

Figure 3.4: Difference calculation and marking for saved block

Step 1 : Divide the original image into 4×4 size blocks and apply the ‘Block Classification and Marking’ procedure defined in Section II.A. It is applied to mark and classify each of the image blocks as either a ‘Saved block’ or ‘hiding block’.

Step 2 : Apply Adaptive AMBTC technique (as defined in Section II.B) on Hiding Blocks to get adaptive AMBTC codes.

Step 3 : Decode each of the hiding block from the adaptive AMBTC codes by replacing bits of the bitmap with their corresponding quantization levels as in [40].

Step 4 : Construct a difference matrix for each of the block using the following proicedure:

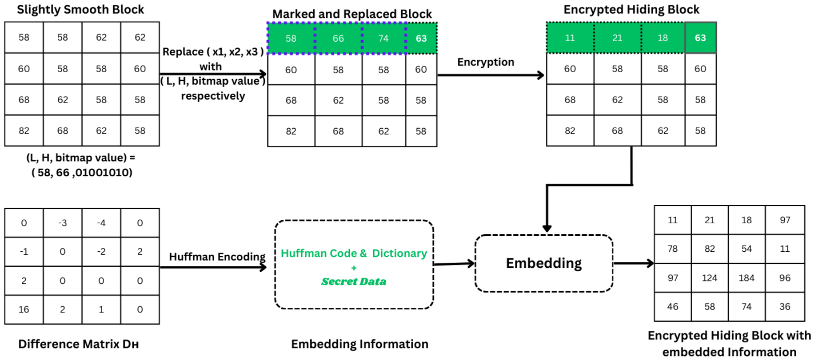
Step 4.1 : If the block is a Saved block then calculate a difference matrix D_S by deducting the pixel values of the marked saved block from the corresponding pixel values of the saved block, as illustrated in Fig.3.4.

Step 4.2 : If the block is a Hiding block then calculate a difference matrix D_H by subtracting the original block pixel values from the decoded block’s pixel values.

Step 5 : Employ the Huffman coding on the difference matrices D_H and D_S to compress them. This compression process will result into the Huffman codes assigned to each unique difference value and the corresponding Huffman dictionary that maps the codes back to the original values.

Step 6 : If the block is a hiding block, then do the following:

- If the block is an ASB, then replace x_1 with AVG, which serves as the only quantization level in this case.
- If the block is a SSB, then replace (x_1,x_2,x_3) with (L, H, b^r), respectively.


Slightly Smooth Block
Replace (x1, x2, x3) with (L, H, bitmap value) respectively
Marked and Replaced Block
Encryption
Encrypted Hiding Block
(L, H, bitmap value) = (58, 66 ,01001010)
Huffman Encoding
Huffman Code & Dictionary + Secret Data
Embedding
Difference Matrix DH
Embedding Information
Encrypted Hiding Block with embedded Information

Slightly Smooth Block

58	58	62	62
60	58	58	60
68	62	58	58
82	68	62	58

Marked and Replaced Block

58	66	74	63
60	58	58	60
68	62	58	58
82	68	62	58

Encrypted Hiding Block

11	21	18	63
60	58	58	60
68	62	58	58
82	68	62	58

Difference Matrix DH

0	-3	-4	0
-1	0	-2	2
2	0	0	0
16	2	1	0

Encrypted Hiding Block with embedded Information

11	21	18	97
78	82	54	11
97	124	184	96
46	58	74	36

Figure 3.5: Illustration of data embedding in hiding block

- If the block is a SCB, then replace (x_1,x_2,x_3,x_5,x_6,x_7,x_8) with (LL, LH, H, $b^{'}$) or (L, HL, HH, $b^{'}$), respectively. In this case, the bitmap ($b^{'}$) size can be in the range of [25, 32] bits, therefore, four pixels are used for storing the bitmap only.

It is worth noting that in all the above cases, LSBs of x_4 are reserved for marking saved or hiding blocks along with the 2-bit block classifier in case of the hiding blocks only.

Step 7 : Encrypt the substituted pixels of each of the blocks except the marking/classifier bits of x_4 using a given encryption key and algorithm to anonymize the contents of blocks. This process is shown in Fig. 3.5.

On the other hand in the case of the Saved block, the encryption key is used for the encryption of the Marked saved block, excluding the least significant bit (LSB) of x4. It will generate an encrypted saved block.

Step 8 : Now, store the side information such as Huffman Side information (Code along with dictionary) and the secret data onto the remaining pixels of hiding blocks as illustrated in Fig. 3.5.

Step 9 : Merge the Hiding Block and Saved Block to create the final marked and encrypted image.

3.1.4 Data Extraction and Image Restoration Procedure

At the receiver's end, in order to extract the hidden data and restore the image, following steps can be followed by first checking the LSB of the x_4 pixels for identifying the saved and hiding blocks.

1. If the block is a saved block, then no data was embedded into the block. So, no need for data extraction.

2. Otherwise, the block is a hiding block. In this case, the next two LSB of x_4 (i.e., classifier bits) give the detail about the exact sub-category of the hiding block.

- If the classifier bits are '00', then the block is an ASB. So, extract the value of x_1 to get the AVG value .

- If the classifier bits are '01', then the block is SSB So, extract the value of (x_1,x_2,x_3) for (L, H, bitmap), respectively.

- If the classifier bits are ‘10’, then the block is the SCB. So, extract the value of (x_1, x_2, x_3) for Quantization levels (LL, LH, H) or (L, HL, HH), respectively. Next, extract the value of next 4 pixels (x_5, x_6, x_7, x_8) to get the bitmap $(b^{'})$.

  In all the above cases, the values of the pixels are first decrypted by following the reverse of encryption stage and then the block is decoded as in [40]. Next, the side information from the remaining pixels is extracted to restore the originality of the image, followed by secret data extraction as in [39].

Chapter 4

RESULTS & ANALYSIS

In this section, we present and analyze the experimental results of the proposed methods, comparing them with state-of-the-art techniques. For the experiments, four grayscale test images, namely ‘Lena’, ‘Boat’, ‘Baboon’, and ‘Barbara’, from the SIPI database [41] are used. Each image has a resolution of 512 × 512 pixels.

The performance is evaluated based on the embedding rate (ER), which refers to the ratio of the number of secret data bits embedded into the cover image to the size of the cover image. For the proposed method, the the number of secret data bits embedded is calculated by subtracting the classifier bits, AMBTC code bits, bit plane bits, and Huffman code bits from the total hidden bits on a block-wise basis.

Here we present, compare and analyze the experimental results of the proposed method in two part. At first, we analyze the performance of the proposed method across different threshold values to determine the optimal parameters. Specifically, we focus on the variance threshold (Thr_V), used for classifying blocks into saved and hiding blocks, and the complexity thresholds ($Thr1$ and $Thr2$), which further categorize hiding blocks into four classes: ‘Absolute Complex block’, ‘Slightly Complex block’, ‘Slightly Smooth block’, and ‘Absolute Smooth block’.

The experimental results for various values of Thr_V, $Thr1$, and $Thr2$ are illustrated in Fig. 4.1, where the format for cutoffs is ($Thr1$, $Thr2$, Thr_V). As shown in Fig.

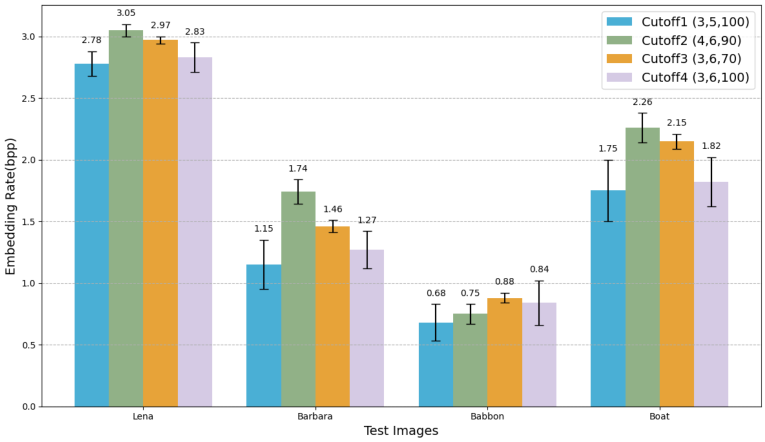


Figure 4.1: Embedding rate(bpp) of the proposed method on different thresholds

4.1, the 'Lena' image achieves the maximum ER of $3.05 bpp$ at complexity thresholds $Thr1 = 4$, $Thr2 = 6$, and variance threshold $Thr_V = 90$ while the 'Baboon' image achieves the maximum ER of $0.88 bpp$ at complexity thresholds $Thr1 = 3$, $Thr2 = 6$, and variance threshold $Thr_V = 70$. This shows that best values of the parameters can only be found by doing exhaustive search for optimal performance.

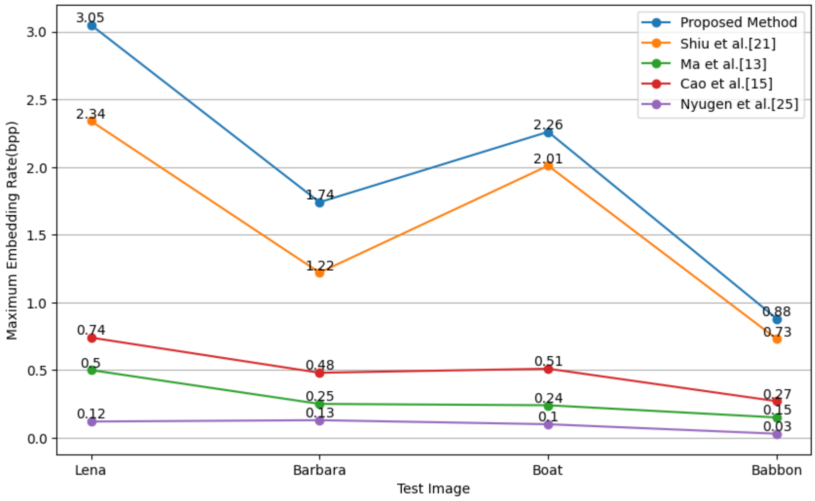


Figure 4.2: Comparison of embedding rate (bpp) of the proposed method with the existing methods

At last, we compare our proposed method with four other well-established methods namely, Shiu et al. [39], Cao et al. [33], Ma et al. [31] and Nguyen et al. [42]. The comparison is shown in Fig. 4.2, where it is clear that our method significantly outperforms all the aforementioned existing works [39, 33, 31, 42] in terms of ER for all the test images. The credit of this performance boost can be attributed to the efficient encoding achieved by the adaptive AMBTC for the hiding blocks, which has resulted in larger embedding space. Moreover, the proposed method is able to provide complete reversibility of the cover image while ensuring error free extraction of the secret data and similar level anonymizaion of the cover image contents as provided by Shiu et al. [39].

Chapter 5

CONCLUSION, FUTURE SCOPE AND SOCIAL IMPACT

5.1 Conclusion

In this paper, a new RDHEI method based on adaptive AMBTC has been introduced. More specifically, the proposed method makes use of adaptive AMBTC to reduce the reconstruction/decoding loss which in turn enhances the embedding capacity and help in getting the original image losslessly. For this. the proposed method first classifies the blocks into two types either saved or hiding blocks. Then hiding blocks are further divided into different categories based on the more detailed complexity analysis of the block. This fine-grained categorization of the image blocks helps in creating the larger space for embedding by enabling highly compressible difference error streams. Experimentally, the proposed method significantly improves the ER while ensuring complete reversibility and privacy of the cover media. In future work, we plan to further reduce the difference error overhead by customizing the conventional compression methods so that a higher ER can be obtained.

5.2 Future Scope

The proposed data hiding method, with its innovative combination of interpolative AMBTC, adaptive quantization, and dynamic block categorization, opens up several promising avenues for future research and development:

- **Advanced Image Formats**: The current work focuses on standard image formats. Future research could extend the technique to support high-dynamic range (HDR) images, medical images, or other specialized formats, each with its unique challenges and requirements.
- **Video Steganography**: The principles of this method could be adapted to develop reversible data hiding schemes for video data. This could have significant implications for secure communication, copyright protection, and content authentication in video streaming applications.
- **Real-Time Applications:** While the current method demonstrates high performance, further optimization could enable real-time data hiding and extraction in

video surveillance systems, augmented reality applications, and other scenarios where immediate information embedding is crucial.

- **Enhanced Security:** Future research could investigate the integration of additional security measures, such as encryption or watermarking, to further enhance the confidentiality and integrity of the embedded data.
- **Robustness to Attacks:** The proposed method could be tested and refined to withstand various image processing attacks, such as compression, filtering, and cropping, ensuring the reliability of data extraction even under adverse conditions.

5.3 Social Impact

The potential social impact of this research is significant, particularly in the realms of privacy, security, and data integrity:

- **Privacy Protection:** In an era of increasing concern over digital privacy, this method could provide individuals and organizations with a robust tool to protect sensitive information, ensuring confidentiality in communication and data storage.
- **Secure Communication:** This technology could be used to create secure communication channels for journalists, activists, or individuals living under oppressive regimes, where traditional communication methods may be monitored or censored.
- **Authentication and Copyright Protection:** The reversible nature of this method makes it suitable for applications like image authentication and copyright protection. The original image can be fully recovered after data extraction, ensuring the integrity of the content while still allowing for hidden metadata embedding.
- **Medical and Scientific Applications:** In fields like telemedicine and scientific research, this technique could facilitate the secure transmission of sensitive patient data or research findings while maintaining the integrity of the original images or videos.

By advancing the state of the art in reversible data hiding, this research has the potential to empower individuals, enhance security, and protect privacy in various aspects of digital life.

References

[1] R. Kumar and S. Chand, "A new image steganography technique based on similarity in secret message," in *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference).* IET, 2013, pp. 376–379.

[2] S.-H. Lim, S.-H. Shin, R. Kumar, and K.-H. Jung, "Data hiding in documents," in *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC).* IEEE, 2019, pp. 1–4.

[3] A. Malik, R. Kumar, and S. Singh, "A new image steganography technique based on pixel intensity and similarity in secret message," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).* IEEE, 2018, pp. 828–831.

[4] R. Kumar, A. Malik, S. Singh, B. Kumar, and S. Chand, "Reversible data hiding scheme for lzw codes using even-odd embedding strategy," in *2016 International Conference on Computing, Communication and Automation (ICCCA).* IEEE, 2016, pp. 1399–1403.

[5] R. Kumar and A. Malik, "Multimedia information hiding method for ambtc compressed images using lsb substitution technique," *Multimedia Tools and Applications*, vol. 82, no. 6, pp. 8623–8642, 2023.

[6] R. Kumar, R. Caldelli, K. Wong, A. Malik, and K.-H. Jung, "High-fidelity reversible data hiding using novel comprehensive rhombus predictor," *Multimedia Tools and Applications*, pp. 1–23, 2024.

[7] A. Kaushal, S. Kumar, and R. Kumar, "A review on deepfake generation and detection: bibliometric analysis," *Multimedia Tools and Applications*, pp. 1–41, 2024.

[8] S. Gandhi and R. Kumar, "A high-capacity reversible data hiding with contrast enhancement and brightness preservation for medical images," *Multimedia Tools and Applications*, pp. 1–26, 2024.

[9] Y. Huang, X. Cao, H.-T. Wu, and Y.-m. Cheung, "Reversible data hiding in jpeg images for privacy protection," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).* IEEE, 2021, pp. 2715–2719.

[10] N. Kansal, N. Tawar, R. Kumar *et al.*, "Study and comparative analysis of data hiding methods for animated gifs," in *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC).* IEEE, 2023, pp. 599–604.

[11] S. Mittal, S. Goyal, S. Aggarwal, and R. Kumar, "Interpolative ambtc based reversible data hiding in encrypted images using rhombus mean," in *2023 International Conference on Device Intelligence, Computing and Communication Technologies,(DICCT).* IEEE, 2023, pp. 451–456.

[12] R. Kumar, S. Chand, and S. Singh, "An optimal high capacity reversible data hiding scheme using move to front coding for lzw codes," *Multimedia Tools and Applications*, vol. 78, pp. 22 977–23 001, 2019.

[13] R. Kumar and K.-H. Jung, "A systematic survey on block truncation coding based data hiding techniques," *Multimedia Tools and Applications*, vol. 78, no. 22, pp. 32 239–32 259, 2019.

[14] D. Sharma, R. Kumar, and K.-H. Jung, "A bibliometric analysis of convergence of artificial intelligence and blockchain for edge of things," *Journal of Grid Computing*, vol. 21, no. 4, p. 79, 2023.

[15] N. Girdhar, D. Sharma, R. Kumar, M. Sahu, and C.-C. Lin, "Emerging trends in biomedical trait-based human identification: A bibliometric analysis," *SLAS Technology*, p. 100136, 2024.

[16] C.-C. Chang, C.-Y. Lin, and Y.-H. Fan, "Lossless data hiding for color images based on block truncation coding," *Pattern Recogn.*, vol. 41, no. 7, p. 2347–2357, jul 2008. [Online]. Available: https://doi.org/10.1016/j.patcog.2007.12.009

[17] C. Qin, P. Ji, C.-C. Chang, J. Dong, and X. Sun, "Non-uniform watermark sharing based on optimal iterative btc for image tampering recovery," *IEEE MultiMedia*, vol. 25, no. 3, pp. 36–48, 2018.

[18] W.-Y. Sun, Z. ming Lu, Y.-C. Wen, F. Yu, and R.-J. Shen, "High performance reversible data hiding for block truncation coding compressed images," *Signal, Image and Video Processing*, vol. 7, pp. 297 – 306, 2011. [Online]. Available: https://api.semanticscholar.org/CorpusID:207315753

[19] I.-C. Chang, Y.-C. Hu, W.-L. Chen, and C.-C. Lo, "High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding," *Signal Processing*, vol. 98, pp. 376–388, 03 2015.

[20] R. Kumar and K.-H. Jung, "Enhanced ambtc based data hiding method using hamming distance and pixel value differencing," *Journal of Information Security and Applications*, vol. 47, pp. 94–103, 05 2019.

[21] D. Ou and W. Sun, "High payload image steganography with minimum distortion based on absolute moment block truncation coding," *Multimedia*

Tools Appl., vol. 74, no. 21, p. 9117–9139, nov 2015. [Online]. Available: https://doi.org/10.1007/s11042-014-2059-2

[22] C. Kim, D. Shin, L. Leng, and C.-N. Yang, "Lossless data hiding for absolute moment block truncation coding using histogram modification," *Journal of Real-Time Image Processing*, vol. 14, pp. 101–114, 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:3320497

[23] J. Chen, W. Hong, T.-S. Chen, and C.-W. Shiu, "Steganography for btc compressed images using no distortion technique," *The Imaging Science Journal*, vol. 58, pp. 177 – 185, 2010. [Online]. Available: https://api.semanticscholar.org/CorpusID:120484796

[24] C.-C. Lin, X.-L. Liu, W.-L. Tai, and S.-M. Yuan, "A novel reversible data hiding scheme based on ambtc compression technique," *Multimedia Tools and Applications*, vol. 74, 06 2013.

[25] J.-M. Guo, H. Prasetyo, and J.-H. Chen, "Content-based image retrieval using error diffusion block truncation coding features," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 3, pp. 466–481, 2015.

[26] S. Nguyen, C.-C. Chang, and X.-Q. Yang, "A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain," *AEU - International Journal of Electronics and Communications*, vol. 70, 05 2016.

[27] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE signal processing letters*, vol. 19, no. 4, pp. 199–202, 2012.

[28] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 6819, 03 2008.

[29] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[30] ——, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[31] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on information forensics and security*, vol. 8, no. 3, pp. 553–562, 2013.

[32] K. Chen and C.-C. Chang, "High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based msb plane rearrangement," *Journal of Visual Communication and Image Representation*, vol. 58, pp. 334–344, 2019.

[33] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” *IEEE transactions on cybernetics*, vol. 46, no. 5, pp. 1132–1143, 2015.

[34] P. Puteaux and W. Puech, “An efficient msb prediction-based method for high-capacity reversible data hiding in encrypted images,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[35] Y. Puyang, Z. Yin, and Z. Qian, “Reversible data hiding in encrypted images with two-msb prediction,” in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2018, pp. 1–7.

[36] Ankur, R. Kumar, and A. K. Sharma, “Bit-plane based reversible data hiding in encrypted images using multi-level blocking with quad-tree,” *IEEE Transactions on Multimedia*, vol. 26, pp. 4722–4735, 2024.

[37] ——, “High capacity reversible data hiding with contiguous space in encrypted images,” *Computers and Electrical Engineering*, vol. 112, p. 109017, 2023.

[38] ——, “Adaptive two-stage reversible data hiding in encrypted images using prediction error expansion,” in *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE, 2023, pp. 427–432.

[39] P.-F. Shiu, W.-L. Tai, J.-K. Jan, C.-H. Chang, and C.-C. Lin, “An interpolative ambtc-based high-payload rdh scheme for encrypted images,” *Signal Processing: Image Communication*, vol. 74, 02 2019.

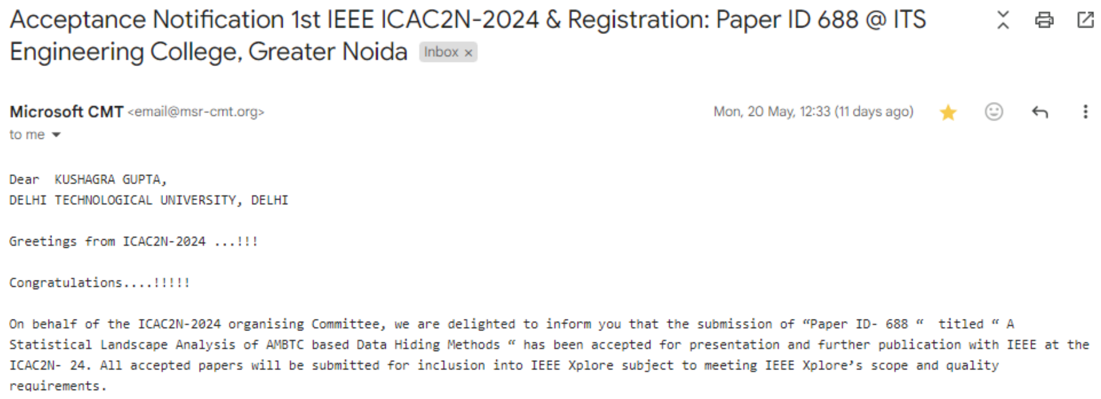
[40] R. Kumar and K.-H. Jung, “A new data hiding method using adaptive quantization dynamic bit plane based ambtc,” 05 2019.

[41] A. G. Weber, “The usc-sipi image database: Version 5,” *http://sipi. usc. edu/database/*, 2006.

[42] T.-S. Nguyen, C.-C. Chang, and W.-C. Chang, “High capacity reversible data hiding scheme for encrypted images,” *Signal Processing: Image Communication*, vol. 44, pp. 84–91, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0923596516300327

Proof of Publishing

Paper 1 Acceptance Proof & Submission Proof :



Acceptance Notification 1st IEEE ICAC2N-2024 & Registration: Paper ID 688 @ ITS Engineering College, Greater Noida

Microsoft CMT <email@msr-cmt.org>
to me

Mon, 20 May, 12:33 (11 days ago)

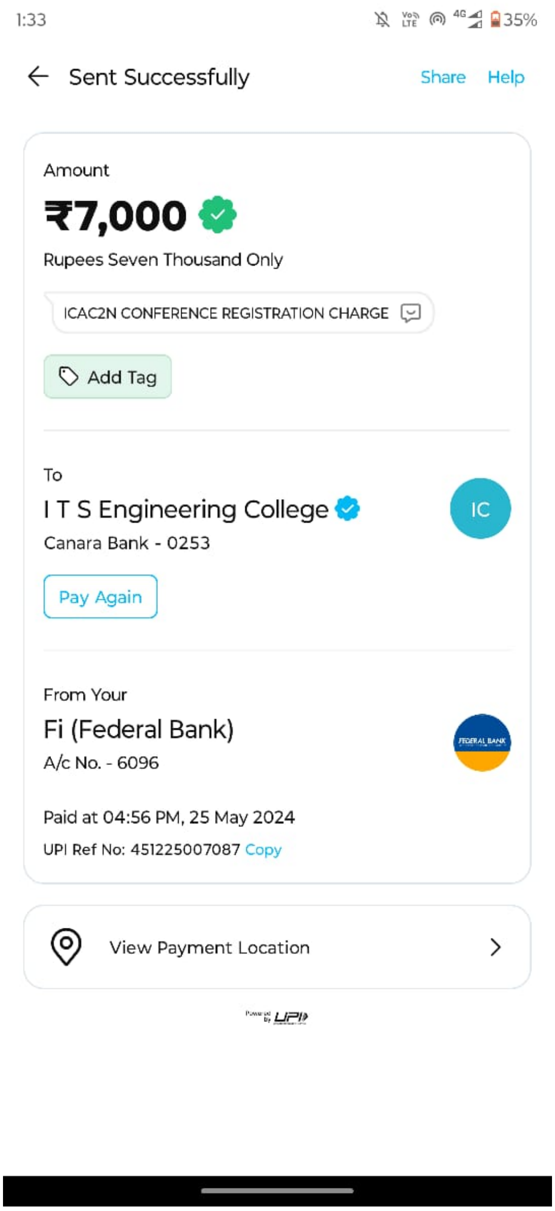
Dear KUSHAGRA GUPTA,
DELHI TECHNOLOGICAL UNIVERSITY, DELHI

Greetings from ICAC2N-2024 ...!!!

Congratulations....!!!!!

On behalf of the ICAC2N-2024 organising Committee, we are delighted to inform you that the submission of “Paper ID- 688 “ titled “ A Statistical Landscape Analysis of AMBTC based Data Hiding Methods “ has been accepted for presentation and further publication with IEEE at the ICAC2N- 24. All accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore’s scope and quality requirements.

Registration Fee receipt



Sent Successfully

Amount

₹7,000

Rupees Seven Thousand Only

ICAC2N CONFERENCE REGISTRATION CHARGE

To

I T S Engineering College

Canara Bank - 0253

From Your

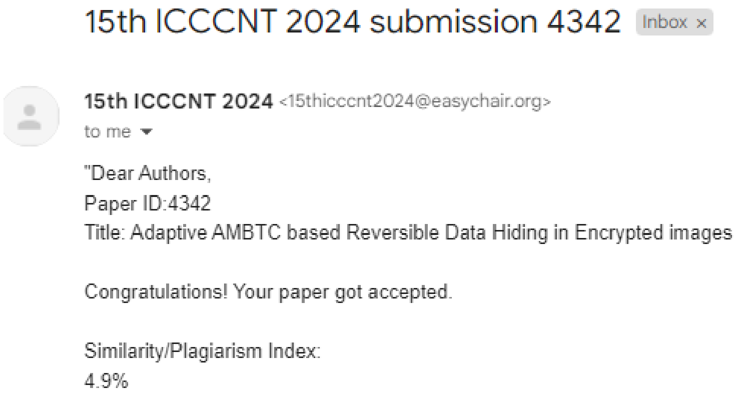
Fi (Federal Bank)

A/c No. - 6096

Paid at 04:56 PM, 25 May 2024

UPI Ref No: 451225007087 Copy

Paper 2 Acceptance & Submission Proof :



15th ICCCNT 2024 submission 4342

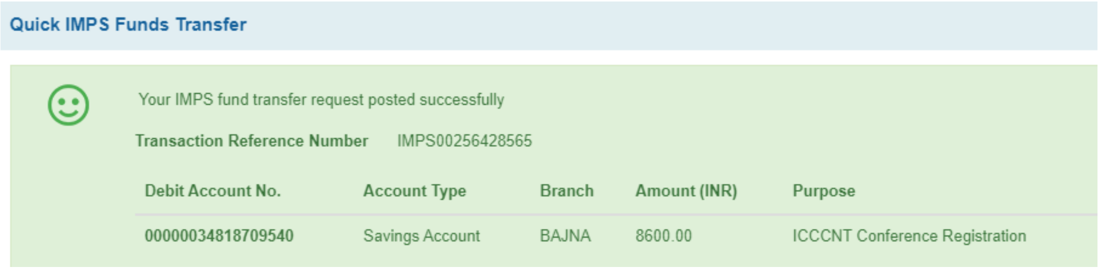
15th ICCCNT 2024 <15thicccnt2024@easychair.org>

"Dear Authors,
Paper ID:4342
Title: Adaptive AMBTC based Reversible Data Hiding in Encrypted images

Congratulations! Your paper got accepted.

Similarity/Plagiarism Index:
4.9%

Registration Fee receipt



Quick IMPS Funds Transfer

Your IMPS fund transfer request posted successfully

Transaction Reference Number IMPS00256428565

Debit Account No.	Account Type	Branch	Amount (INR)	Purpose
00000034818709540	Savings Account	BAJNA	8600.00	ICCCNT Conference Registration