

Image Encryption in Frequency Domain Using Hybrid Chaotic Maps, Hashing and Lifting Wavelet Transform



By

Fizza Batool

00000364135

Supervisor

Cdre Dr. Nadeem Kureshi

A dissertation submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cyber Security (MS CYS)

In

Department of Cyber Security,
Pakistan Navy Engineering College (PNEC),
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(April 2024)

Image Encryption in Frequency Domain Using Hybrid Chaotic Maps, Hashing and Lifting Wavelet Transform



By

Fizza Batool

Fall-2021-MS-CYS PNEC

Supervisor

Cdre Dr. Nadeem Kureshi

A dissertation submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cyber Security (MS CYS)

In

Department of Cyber Security,
Pakistan Navy Engineering College (PNEC),
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(April 2024)

With profound gratitude, I dedicate this thesis to my esteemed parents, whose unwavering support has been the foundation of my academic journey. To my exceptional teachers, whose guidance shaped my intellect and character. To my cherished spouse, whose unwavering belief in me has been a constant source of inspiration. Your unwavering presence throughout this endeavor has been invaluable. I am forever grateful for the love and support of all who have contributed to my personal and academic growth.

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at Department of Cyber Security at Pakistan Navy Engineering College (PNEC) or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at Pakistan Navy Engineering College (PNEC) or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Signature: Fizza

Fizza Batool

National University of Sciences and Technology

MASTER'S THESIS WORK


We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Regn No.) FIZZA BATOOL (00000364135) Titled: Image Encryption in Frequency Domain Using Hybrid Chaotic Maps, Hashing and Lifting Wavelet Transform be accepted in partial fulfillment of the requirements for the award of Master's degree.

EXAMINATION COMMITTEE MEMBERS


1. Name: DR MUHAMMAD USAMA

Signature: 

2. Name: DR AYAZ SHERAZI

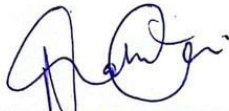
Signature: 

Supervisor's name: CDRE DR. NADEEM KURESHI

Signature: 

DR NADEEM KUR
Commodore
DEAN MIS
PNS JAUHAR

Date: 22-April-2024




Head of Department
Cdr Pakistan Navy
OPGP Cyber Security
PNS Jauhar

22-April-2024
Date

COUNTERSIGNED

Date: 22-April-2024



Date: _____
Dean / Principal

UZMA KHALID
Cdr Pakistan Navy
HOD Computer Science
PNS Jauhar


Approval

It is certified that the contents and form of the thesis entitled “**Image Encryption in Frequency domain using Hybrid Chaotic Maps, Hashing, and Lifting Wavelet Transform**” submitted by Fizza Batool have been found satisfactory for the requirement of the degree.


Advisor: Cdre Dr. Nadeem Kureshi

Signature: 
DR NADEEM KURESHI
Date: 22-April-2024
Commandore
DEAN MIS
PNS JAUHAR

Committee Member 1: Dr. Muhammad Usama

Signature: 
Date: 22-April-2024

Committee Member 2: Dr. Ayaz Sherazi

Signature: 
Date: 22-April-2024

CERTIFICATE FOR PLAGIARISM

1. It is certified that PhD / M.Phil / MS Thesis Titled "Image Encryption in Frequency Domain Using Hybrid Chaotic Maps, Hashing and Lifting Wavelet Transform" by FIZZA BATOOL (2021-NUST-MS Cyber Security (CyS Fall 2021)) has been examined by us. We undertake the follows:

- a. Thesis has significant new work / knowledge as compared already published or is under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph, or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results, or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled / analyzed.
- d. There is no falsification by manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.



DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JALWAR

Name & Signature of Supervisor

Acknowledgments

I would like to express my sincere gratitude to my supervisor Dr. Fawad Ahmed, and external advisor Dr. Jawad Ahmad of Edinburgh Napier University, UK, whose expertise, and unwavering assistance have been invaluable in helping me navigate the challenging terrain of my master's program. Their guidance has enhanced my academic endeavors, shedding light on avenues of understanding and discernment. I'm equally indebted to Lt. Cdr. Aaliya Ali and Cdre. Dr. Nadeem Kureshi, HoD, and Dean of the Cyber Security Department for their contributions and for their pivotal roles in shaping my academic journey. Their guidance and leadership have sculpted an environment conducive to scholarly excellence, fostering my growth and development. In their collective guidance, I have found not only mentors but also pillars of strength, whose unwavering belief in my capabilities has propelled me towards academic achievement.

Fizza Batool

TABLE OF CONTENTS

Table Of Contents	viii
List of Tables	xii
List of Figures	xiii
List of Abbreviations	xiv
Abstract	xv
1 INTRODUCTION	1
1.1 Background	1
1.2 Motivation	2
1.3 Image Encryption	2
1.3.1 Illustration of Image Encryption and Decryption Method	2
1.3.2 Exigency of Image Encryption in Digital Era	2
1.3.3 Benefits & Drawbacks of Image Encryption	3
1.3.4 Motive behind Image Encryption	4
1.4 Chaos Theory and its application	4
1.5 Frequency Domain Image Encryption	4
1.6 Research Objective	5
1.7 Thesis Layout	5
2 LITERATURE REVIEW	6
2.1 Overview of Image Encryption	6
2.2 Significance of Image Encryption	6
2.3 Traditional Encryption Methods	6
2.4 Existing Encryption Schemes	7

2.5 Standard Metrics for Image Encryption	9
2.6 Chaotic Maps	9
2.6.1 Logistic Map	9
2.6.2 Chaotic Sine Map	10
2.6.3 Chaotic Cosine Map	10
2.6.4 Chaotic Tent Map	10
2.7 Resistivity to Differential Attacks	11
2.8 Performance Evaluation Metrics	11
2.8.1 Peak Signal to Noise Ratio (PSNR)	11
2.8.2 Number of Pixels Change Rate (NPCR)	12
2.8.3 Unified Average Changing Intensity (UACI)	12
2.8.4 Mean Square Error (MSE)	13
2.8.5 Analysis of Histogram	13
2.8.6 Chi-Square	13
2.8.7 Entropy	14
2.8.8 Correlation	14
2.8.9 Key Sensitivity	15
2.8.10 Homogeneity	15
2.8.11 Contrast	15
2.8.12 Energy	16
2.8.13 Maximum Deviation	16
2.9 Lifting Wavelet Transform (LWT)	16
2.9.1 Distinctive Features of LWT	18
2.9.2 Inverse Lifting Wavelet Transform (ILWT)	18
2.10 Secure Hash Algorithm (SHA)	19
2.11 Permutation	19
2.12 Substitution	20
2.12.1 Dynamic S-box Substitution	20

3 PROPOSED ENCRYPTION SCHEME	21
3.1 Objective	21
3.2 Constituents of Proposed Integrated Algorithm	21
3.3 Hybrid Chaotic Maps in Proposed Scheme	22
3.3.1 Logistic Sine Cosine Map	22
3.3.2 Sine-Tent Cosine Map	22
3.3.3 Tent Sine System	23
3.4 Wavelet Transforms in Proposed Scheme	24
3.5 Extraction of LL component from LWT	24
3.6 Secure Hash Algorithm in Proposed Scheme	25
3.7 Application of Permutation in Proposed Scheme	26
3.8 Application of Dynamic S-box Substitution in Proposed Scheme	26
3.9 Working of Proposed Encryption Algorithm	27
3.9.1 Flow Chart of Proposed Encryption Algorithm	29
3.9.2 Procedural Encryption of Cameraman & its Histograms	30
3.10 Decryption of the Proposed Scheme	31
4 RESULTS AND DISCUSSION	33
4.1 Performance of Proposed Encryption Scheme	33
4.1.1 Histogram Analysis of Tested Image	33
4.2 Security, Confidentiality & Preservation of Images	33
4.2.1 Correlation Coefficient	34
4.2.2 Information Entropy	34
4.2.3 NPCR & UACI	34
4.2.4 PSNR	35
4.2.5 MSE	35
4.2.6 Computational Speed	36

5 CONCLUSION & FUTURE RECOMMENDATIONS	37
5.1 Overall Scheme of Proposed Algorithm	37
5.2 Future Roadmap for Image Encryption	37
6 REFERENCES	39

LIST OF TABLES

1	Benefits & Drawbacks of Image Encryption	3
2	Correlation values of Cipher Image & its comparison with existing methods	34
3	Entropy values of Cipher Image & its comparison with existing methods	34
4	NPCR values of Cipher Image & its comparison with existing methods	34
5	UACI values of Cipher Image & its comparison with existing methods	35
6	PSNR values of Cipher Image & its comparison with existing methods	35
7	MSE values of Cipher Image & its comparison with existing methods	35

LIST OF FIGURES

1	Image Encryption & Decryption Method	2
2	Rapid Increase of Digital Communication	3
3	Motive behind Image Encryption	4
4	Lifting Wavelet Transform	17
5	Inverse Lifting Wavelet Transform	18
6	Strategy of Permutation	19
7	S-box transformation	20
8	Generation of Logistic Sine Cosine Map	22
9	Generation of Sine Tent Cosine Map	23
10	Generation of Tent Sine System	24
11	Lifting Wavelet Transform Decomposition	24
12	Changes caused by input variation in SHA-512 algorithm	25
13	Workflow of SHA-512 algorithm	25
14	Application of permutation in proposed scheme	26
15	Flowchart of Proposed Encryption Scheme	29
16	Original Cameraman Image & its histogram	30
17	Permuted Image of Cameraman & its histogram	30
18	Encrypted CA of Cameraman Image & its histogram	30
19	Substituted Cipher of Cameraman image & its histogram	31
20	Encrypted Image of Cameraman Image & its histogram	31
21	Histogram of Original (a) and Encrypted Image (b)	33

LIST OF ABBREVIATIONS

AES : Advanced encryption standards

RSA : Rivest Shamir Adleman

CFES: Compression Friendly Encryption Scheme

MSE : Mean Square Error

CIEAIBO-DNAC : Chaotic image encryption algorithms with an improved Bonobo optimizer
DNA coding

SHA : Secure hash algorithm

NPCR: Number of pixels change rate

CTBCS : Cosine Transform-Based Chaotic System

GLCM: Gray-Level Co-Occurrence Matrix

MAE: Mean Absolute Error

RMSE : Root Mean Square Error

ECC: Elliptic Curve Cryptography

DES: Data Encryption Standard

UACI : Unified Average Changing Intensity

DNA: Deoxyribonucleic Acid

STC: Sine-Tent-Cosine Map

DWT: Discrete wavelet transform

LWT: Lifting wavelet transform

ILWT: Inverse Lifting Wavelet Transform

LSC-IES: Local Scrambling and Chaos-based Image Encryption Scheme

PSNR : Peak signal-to-noise ratio

ABSTRACT

The brisk augmentation of digital communication and the ubiquitous use of visual transmission have become quite common all over the globe. As far as the transmission between different communication mediums is concerned, a channel is always required to bridge the gap between the input source & destination and the internet stands as the most common and cheapest channel for such transmissions. Just because of the wide accessibility and high vulnerability of the internet, it demands robust security techniques to secure the information which is to be transmitted. Through cryptographic approaches, Visual information can have its confidentiality and integrity preserved. Although many researchers have worked well in the field of text encryption techniques, when it comes to image encryption techniques, there are several algorithms that combine various techniques to encrypt images. All of them, nevertheless, have the drawback of having mediocre encryption, which lowers the quality of the encrypted image. Strong picture encryption techniques must be used in order for a good image encryption method to guarantee that after the decryption procedure, the original image can be obtained again. To increase the encryption quality of a picture, many suitable algorithms must be combined into a single cryptographic technique. This increases the complexity and difficulty of decrypting the encrypted image for an attacker. The main motive behind this research was to encrypt the images by implementing multiple befitting approaches which are previously proposed in a single attempt and to upgrade the encryption quality. This quality up gradation of image encryption schemes has been done in Frequency domain by using the platform of MATLAB for the encoding of original image on LL band by using the algorithms including: SHA-512, Lifting wavelet transform, Logistic Sine Cosine map for permuted image and Sine Tent Cosine map for proceeding the permutation using XOR and then the substituted image is extracted out by deploying Tent-Sine map on 16x16 dynamic S-boxes, including AES, Gray & Hussain S-boxes. The original image is then lastly encrypted by using the Inverse Lifting Wavelet Transform, keeping the original content under several wraps, and making it unattainable for unauthorized users to gain hands on original image data. Lastly, comparative analysis of the encrypted images is rendered by using the standard parameters to acquire and prove the efficiency and quality of proposed image encryption technique.

Chapter 1

INTRODUCTION

1.1 Background

The security of transferred data has become an essential requirement in the age of fast digitization and widespread data transmission, one that cannot be ignored. Techniques for encryption are essential when it comes to safe picture transfer. There are various previously implemented or proposed encryption techniques which are based on mathematical algorithms such as RSA, AES and many more. Those proposed encryption methods might have provided robust security, but those techniques exhibit vulnerabilities under certain circumstances, compromising the quality of the encrypted image. In contrast to those methods, the previously implemented chaos-based encryption techniques have emerged as an efficient alternative that employs the inherent intricacy and inevitability of chaotic systems to enhance data security of the image. The efficiency of encryption based on chaos theory actually counts on the meticulous selection and amalgamation of different algorithms and their parameters. Assuring that encrypted images are safe from a range of attacks, including cryptanalysis, differential attacks, and brute force attacks, is one of the trickiest aspects of image encryption [12]. Qayyum et al. using dynamic replacement techniques for pixel modification, stressed the integration of chaos-based methodologies for enhancing the security of picture encryption systems [5]. Numerous chaotic maps, including the Cosine, Sine, and Logistic maps, have been shown to be useful for generating encryption keys and accelerating the encryption process [3].

Encryption algorithms need to be resistant to attacks, have a large key space, and high key sensitivity in order to guarantee the security and integrity of encrypted images [12]. In [10], the importance of combining several algorithms to develop an effective encryption method is addressed, proving that an integrated algorithm comprising of effective techniques can lead to a more robust image encryption scheme. Various chaotic maps, permutation methods, and key generation schemes can remarkably impact the encryption strength and the overall efficiency of the system. Researchers highlight the necessity of reviewing picture encryption algorithms for their encryption performance, efficiency, and security in order to resolve flaws and improve overall security of encrypted images [12]. Hence, it mandates in depth exploration to research the positive and negative effects of amalgamating multiple algorithms to elevate the security and functionality of cryptographic encryption of images using chaos-based theory.

Other than that, substitution is another notable encryption technique. S-boxes are nonlinear components used in encryption algorithms to substitute input bit patterns with alternative output patterns using a specified substitution table [7]. Traditional S-box designs have limited non-linearity, affecting the encryption algorithm's overall cryptographic strength. Additionally, low non-linearity in S-boxes can expose the encryption scheme to linear and differential cryptanalysis attacks, risking the system's security [7].

1.2 Motivation

Considering the significant relevance of safeguarding digital photos in this perilous time frame, various researchers have worked, and some are still working to secure every aspect of integrity of digital data. The motivation behind this thesis is to rectify the shortfall in the already prevailing literature by inter-mingling multiple chaos-based algorithms because of its significance emphasized in [3]. By the compilation and optimization of different encryption techniques, the aim of this research is to propose a robust and coherent encryption system which will be highly capable for the protection of digital images from any sort of unauthorized access and cyber-attacks.

1.3 Image Encryption

In order to secure confidential image data from unauthorized users and preserve the integrity of sensitive information, image encryption techniques are used. By implementing image encryption, nobody can be able to gain the original image data except the ones who are well aware about encryption scheme, hence they decrypt the original image data accurately.

1.3.1 Illustration of Image Encryption & Decryption Method

Image encryption method can be illustrated as follows in Fig. 1.

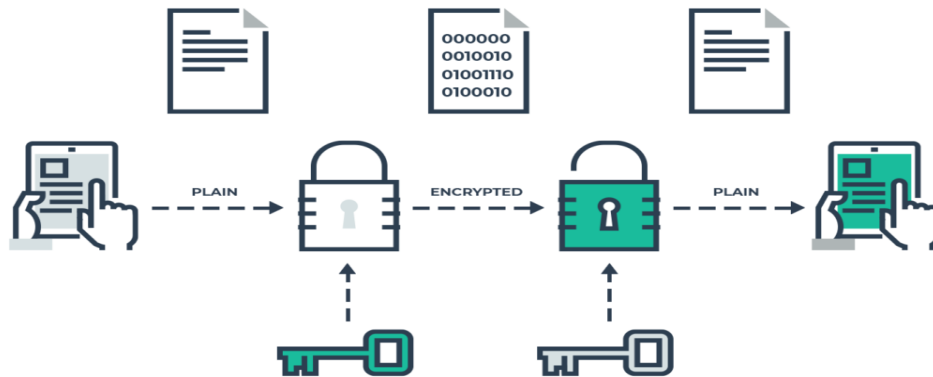


Figure 1 "Image Encryption & Decryption Method."

1.3.2 Exigency of Image Encryption in Digital Era

From the recent research [1], it can be concluded and illustrated by the below figure that in these recent years, the utilization of digital communication devices has rapidly increased, corresponding to the growth in the total population. Due to the widespread use of social media, sharing of multimedia data has become quite common. As far as online activities and transmission of social media are concerned, the internet serves as the only primary medium.

However, despite the various benefits it offers, it is a highly vulnerable network because of its wide accessibility, susceptibility to cyber threats and continuous evolution. Because of this, robust security methods are required beforehand for the transmission of our confidential image data and this calls for efficient encryption schemes.

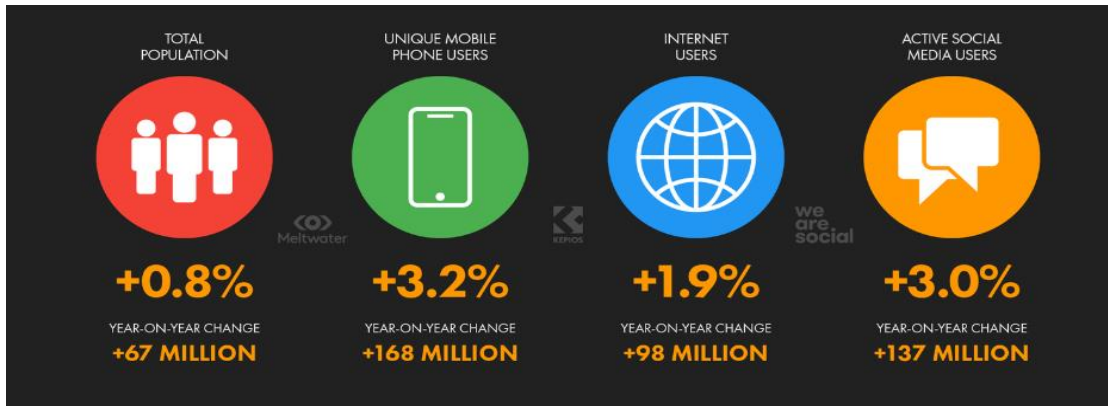


Figure 2 "Rapid increase of digital communication" [1]

1.3.3 Benefits & Drawbacks of Image Encryption

BENEFITS	DRAWBACKS
High Security	Prevents contextual services
Phishing Proof	Reduces automation capabilities
Prevents mass surveillance	Makes it harder to catch cybercriminals
Hacking Attempts are unfruitful	The meta data is not encrypted
Ensures compliance with legal requirements	Increased processing overhead

Table 1 "Benefits & Drawbacks of Image Encryption"

1.3.4 Motive Behind Image Encryption

The wide and continuous use of communication devices has ramped up the risk of more and more data breaches because of the vulnerability ports present during the transmission of data from source to destination or vice versa. To make sure that the transmitted data is only accurately visible to the desired destination point, the data needs to be encrypted so that it can be saved from any kind of intruder, attacker, or man in the middle (MITM). This can be depicted by the illustration of Figure ‘3’ as follows.

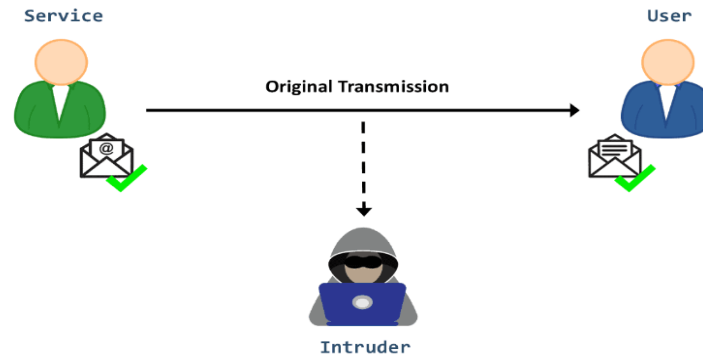


Figure 3 "Motive behind Image encryption."

1.4 Chaos Theory and Its Application

The behavior of multiplex dynamical systems, which are very sensitive to beginning conditions and situations, is studied mathematically in the field of chaos theory. This implies that significant variations in the beginning conditions of a chaos-based system can result in significant shifts in the system's long-term performance. There are multiple applications of this theory in various fields, including the weather, the stock market, and the behavioral changes of biological systems. Furthermore, chaos theory has also been employed to introduce updated and innovative methods for cryptography and secure communication.

1.5 Frequency Domain Image Encryption

The process of converting the images into frequency domain is used to implement frequency domain image encryption techniques. There are several merits of frequency domain encryption schemes over spatial domain encryption schemes. Frequency domain image encryption methods are highly efficient and effective against different sort of attacks because it is quite complex for the hackers to identify and exploit the patterns after encryption, it provides efficient technique for image compression, as the components in frequency domain are easy to compress than the components in the spatial domain. Therefore, the image encryption schemes in this domain are suitable and recommended to encrypt images that embody confidential and sensitive information.

1.6 Research Objective

The research objective of this thesis and whole research is to:

- Identify the research gap of previously implemented image encryption methods.
- Bridge the research gap by integrating the appropriate algorithms, logistic maps, chaos-based theory, lifting wavelet transform, inverse lifting wavelet transform, and dynamic S-box replacement.
- Quality of image encryption is improved.
- Assess the image encryption quality by using standard quality evaluation metrics and by comparing it with the previously proposed methods.

1.7 Thesis Layout

The layout of this thesis is classified into five different sections. The study of prior research and techniques for analyzing the difficulties in the field of image encryption are covered in Chapter 2. In order to identify the research gap in this field, the chapter examines the many studies that have already been done on picture security employing chaotic image encryption maps and transforms. In order to enhance the quality of the encrypted image, Chapter 3 outlines the thesis's methodology and suggests an integrated algorithm for image encryption. Additionally, the chapter uses the common metrics for evaluating quality to evaluate encryption quality. By contrasting the image encryption quality of the suggested scheme with that of previously used algorithms, Chapter 4 presents the findings and discussions. Lastly, Chapter 5 represents the concluded overview of the whole thesis and a road map for further advancements in this area in future.

Chapter 2

LITERATURE REVIEW

2.1 Overview of Image Encryption

Image encryption differs from text encryption because of the intrinsic properties of images, which include high redundancies, vast storage capacity, and strong pixel correlations. To overcome the difficulties associated with image encryption in real-time processing, new and sophisticated encryption methods are needed [2]. Image encryption uses a variety of techniques, including substitution, permutation, chaotic maps, S-boxes, and many more, to distort and diffuse the image data. These methods change the pixel values of the original image in a way that makes it impossible for an unauthorized person to undo without the required decryption key [4].

2.2 Significance of Image Encryption

Sensitive information found in digital photos needs to be protected both during transmission and storage [3]. To protect this data from several kinds of assaults, such as interception, modification, fabrication, and unauthorized access, image encryption is essential. By encrypting images, users can prevent adversaries or attackers from viewing or tampering with the visual content, ensuring the security of the transmitted or stored images [2]. The reality that medical photographs are regularly created and disseminated online has been highlighted by the recent COVID-19, underscoring the important need for security against unauthorized usage [12].

2.3 Traditional Encryption Methods

In earlier times, security of images was achieved by algorithms that were designed to primarily use text-based encryption techniques. There were multiple methods which were introduced earlier for robust security, but the encryption quality was not as effective and up to the mark with the real time processing systems. Traditional encryption algorithms come in two varieties: block cyphers and stream cyphers. Block cyphers handle data in fixed-size blocks, whereas stream cyphers encrypt data bit by bit. These encryption methods were originally developed for text-based applications, where the accurate recovery of each bit was essential for decrypting the original transmitted message accurately [2]. Many of the more traditional encryption methods from the past depended just on pixel permutation; yet these systems are vulnerable to different types of cryptographic attacks [6]

2.4 Existing Encryption Schemes

Multiple researchers have followed different strategies and schemes to secure the image data, proving the necessity and significance of appropriate, robust and effective image encryption schemes.

As researched by the authors in [2], AES is found to be more effective than CFES due to its weaknesses, such as lower values of entropy and horizontal correlation in images after encryption. The quality assessment of previously suggested image encryption techniques is examined. To evaluate the image quality, they employed factors including diffusion characteristics, information entropy, compression friendliness, encryption quality measurement, correlation coefficient analysis, key space analysis, and the effect of noise and JPEG compression on the AES and CFES encryption methods [2].

In [3], the authors' suggested encryption method makes use of a chaotic system based on the cosine transform (CTBCS). Although the LSC-IES (Local Scrambling and Chaos-based Image Encryption Scheme) minimizes significant correlations between neighboring pixels to some extent and uses high-efficiency scrambling of pixels to introduce changes in the cipher-image, more progress in this field could have increased the scheme's resistance to specific types of attacks [3].

As in [4], the authors have utilized a unique chaotic substitution technique by incorporating chaos in addition to substitution, using various S-boxes to enhance encryption strength but as per the results of the evaluation quality metrics, its encryption quality is not up to the mark because of low values of entropy and homogeneity.

Furthermore, in [5], a method of encryption based on chaos theory and dynamic substitution is proposed and this scheme involves the use of 2D Henon and Ikeda chaotic maps with a S-box to secure the image data but its security against adversarial scenarios and attacks is not as much efficient as it should be.

In [6], the encryption method for highly auto-correlated data is discussed. The encryption technique proposed in to enhance the security of digital images [6] uses chaotic maps and substitution boxes. However, the main problem is that the algorithm's resistance to sophisticated cryptanalysis techniques and security flaws beyond entropy attacks has not been thoroughly examined [6].

Moreover, in [7], a novel integrated algorithm is proposed by using lifting wavelet transform, Wide range beta chaotic map and Latin square. Along with the pros of proposed encryption algorithm in [7], the combination of different techniques integrated in this scheme has ramped up the execution time of the program, slowing down the execution time as compared to other methods.

In [8], for safe transmission, a novel 1D chaotic system is suggested. It is also evident that the suggested algorithm operates more quickly than the earlier schemes, but it can still be enhanced by including the 1D replacement process in addition.

The suggested algorithm in [9] encrypts data using chaotic maps, a pre-shared symmetric key, and an initialization vector (IV) to produce two 2D matrices that distort and diffuse the original image.

Although the algorithm in [9] works well enough but the value of PSNR should be minimized more to ensure the high-level robustness and secure transmission of images by integrating the proposed algorithm with any befitting algorithm. Other than that, a lightweight encryption solution for biometric images is proposed in [10]. While the algorithm in [10] focuses on gray-scale biometric picture encryption, the fundamental encryption methods and algorithms might be expanded or changed to include color image encryption with proper adjustments in the proposed algorithm.

The proposed approach in [11] integrates the technique of lifting wavelet transform and chaos-based maps but it comprises of the challenge of securely storing and managing the encryption/decryption keys. If the keys are lost or compromised, it could lead to difficulties in decrypting the image data, hence resulting in data loss or unauthorized access to sensitive information. Chaos-based picture encryption is a promising approach that requires further study and development to enhance security, efficiency, and usability as per the review laid down by authors in [12]. By tackling obstacles and seeking new opportunities we can protect sensitive information in the digital age.

The encryption method used in [13] is a compression-encryption/steganography scheme. This approach includes compressing photos, encrypting them, and then hiding the encrypted images under several cover images. However, it has two major drawbacks: First, fusing several photos of varying sizes into a single, huge image results in a compressed reconstructed image of lower quality. Secondly, while the OMP reconstruction algorithm employed in this scheme guarantees excellent image reconstruction quality, its execution time accounts for a significant portion of the overall method execution time, rendering this scheme slower than the others.

Image encryption techniques and schemes are not necessarily required only for accounts, finance, or administrative data, it is also required for the most sensitive yet the most overlooked department “healthcare”. Image encryption is required for healthcare applications [14] because of the confidential reports and pictorial data which needs to be handled with an extremely careful manner.

In [16], an improved Bonobo optimizer and DNA coding are used to create a chaotic picture encryption technique called CIEAIBO-DNAC. Although this method introduced substitution, diffusion and pixel scrambling procedure, but only four quality evaluation metrics are evaluated to figure out the quality of encryption without finding out the significant parameter values like; entropy, UACI, NPCR, homogeneity and many, hence the encryption quality wasn't properly evaluated. A hybrid encryption method that combines the Logistic-Cosine-Sine chaos map and Elliptic Curve Cryptography (ECC) is presented to secure images [17]. However, because the technique combines the two, it may be more difficult to integrate and implement.

After reviewing the methods proposed and implemented in fifteen different papers [2]-[17], it can be concluded that all of those methods and techniques encrypt the images well but there's a common issue of low encryption quality, complex decryption procedures, more consumption time for execution of algorithm and intricacies while implementing that scheme in real time applications.

2.5 Standard Metrics for Image Encryption Quality

Just like the multiple approaches and methods proposed by different researchers, they have also evaluated the quality of image data during the procedure of encryption and decryption of original image. The different standard parameters through which the former researchers have evaluated their encrypted image data quality in [2]-[17] are:

- MSE, RMSE, PSNR, Maximum Deviation, NPCR, UACI, Key Sensitivity
Correlation Coefficient, Entropy, Avalanche effect by MSE, GLCM
Homogeneity, Encryption Time, Contrast Analysis, Energy, Chi-square, MAE

2.6 Chaotic Maps

A mathematical model with dense periodic orbits, topological mixing, and sensitivity to chaotic initial conditions is called a chaotic map. In the context of cryptography, chaotic maps are utilized in chaos-based encryption schemes due to their properties of unpredictability and complexity [3]. Chaotic maps are employed in cryptography for generating pseudorandom sequences, key generation, and for the encryption of data.

2.6.1 Logistic Map

One of the most popular maps in chaos theory research is the logistic map, which is a straightforward dynamical equation with intricate chaotic behavior [8]. It can be mathematically defined in equation (1) as [8].

$$x_{n+1} = rx_n(1-x_n) \text{ -----(1)}$$

where “r” is the controller parameter for the degree of chaos and “x_n” is the value of the map at time “n.” The value of “r” determines whether the map behaves in an unstable or stable manner.

If $r < 1$ then, stable behavior of map

If r increases then, the map becomes rapidly chaotic

2.6.2 Chaotic Sine Map

The chaotic sine map and logistic map have similar characteristics to a certain degree in terms of the chaotic behavior [18]. The chaotic sine map has the following presiding equation as represented in [31].

$$y_{n+1} = \alpha \text{Sin} (\pi \cdot y_n) / 4, 0 < \alpha \leq 4; \text{-----}(2)$$

Similar to the tent map, the system parameter is denoted by α , and the state variable y_n is inside the interval [0, 1]. Common issues are also present in the Sine and Tent maps.

According to the bifurcation diagram in [18], the range of chaos in Sine maps is constrained. The possible applications of the Sine map are restricted by its non-uniform trajectory points and small chaotic range [18].

2.6.3 Chaotic Cosine Map

The chaotic cosine map has favorable chaotic distinctive characteristics, and it is a one-dimensional (1D) map, which implies that it connects two points that are in a one-dimensional space. Chaotic cosine map can be mathematically by using equation (3) as represented in [34].

$$x_{n+1} = G(F(x_n)) \text{-----}(3)$$

wherein G denotes the cosine function and F represents the starting point for the map. As a trigonometric function, G generates a wave.

2.6.4 Chaotic Tent Map

The chaotic tent map can be used to simulate a wide range of circumstances, including weather patterns, population increase, and stock market volatility and it is also utilized in cryptography and other applications that require unpredictability. The chaotic tent map can be expressed in equation (4) as represented in [32]:

$$y_{n+1} = \begin{cases} \tau \frac{y_n}{2} & y_i < \frac{1}{2} \\ \tau \frac{(1-y_n)}{2} & y_i \geq \frac{1}{2} \end{cases} \text{-----} (4)$$

where the state variable $y_n \in [0, 1]$ and the parameter τ 's range is $0 < \tau \leq 4$.

2.7 Resistivity to Differential Attacks

One of the most prevalent kinds of challenges is the differential attack. This attack compares changes in the input and encrypted output to find the desired key or plaintext message. It is possible to comprehend the influence on cypher photos by looking at the differences in the original images. The differential attack seeks to determine whether the original, plain pictures and the corresponding encrypted ones are equivalent. If a technique for picture encryption incorporates diffusion property, it offers a high degree of security for image transmission. The diffusion property states that even little changes to the plaintexts have the power to disseminate over the whole body of data in the cypher texts. The NPCR and UACI.t metrics can be used to assess an encryption algorithm’s resistance to differential assaults [22].

2.8 Performance Evaluation Metrics

An assessment of many metrics is essential to determine the efficacy or efficiency of the algorithms employed for image encryption. “Security” is one of the most important evaluation criteria out of all of them, evaluating an algorithm’s capacity to withstand attacks and maintain the confidentiality and integrity of the specific image data. The quality preservation of an image certifies that the encryption system does not impair the transparency of picture understanding by assessing how well the encrypted image maintains its visual integrity and allegiance. In addition, a variety of other variables can be taken into consideration when assessing the quality of picture encryption to guarantee full verification of image clarity following the decryption of the cypher image data.

2.8.1 Peak Signal-To-Noise Ratio (PSNR)

The PSNR parameter can be used to analyze encrypted images. By calculating the difference in pixel values between the original and ciphered images, it indicates the level of encryption [19]. Mathematically, equation (5) can be expressed as in [9];

$$PSNR= 20 \log_{10} \frac{MAX_p}{MSE} \text{-----}(5)$$

Where “MSE” stands for Mean Square Error and “MAX_p” is the maximum value a pixel could have (for instance, 255 in 8-bit pixels of the image). A higher PSNR number also results in an improvement in image quality [19]. So according to that, the lower the PSNR, the higher the encryption quality is [9]. Hence, PSNR and better encryption quality have an inversely proportional relationship as shown in equation (6).

$$Quality\ of\ encryption \propto \frac{1}{PSNR} \text{-----}(6)$$

2.8.2 Number of Pixels Change Rate (NPCR)

Any encryption method should have the desirable property that any changes made to the source picture should cause a noticeable difference in the cypher image. These measurements are employed to ascertain the impact of a single pixel alteration on the overall image. NPCR can be expressed mathematically as in equation (7) [3].

$$\text{NPCR}(C1, C2) = \sum_{i,j} \frac{A(i,j)}{G} \times 100\% \text{ -----(7)}$$

Where ‘G’ is the number of pixels in an image and ‘A’ records the difference between C1 ‘original image’ and C2 ‘cipher image’, the resultant matrix can be defined in equation (8) as expressed in [3];

$$A(i,j) = \begin{cases} 0, & \text{if } C1(i,j) = C2(i,j); \\ 1, & \text{if } C1(i,j) \neq C2(i,j). \end{cases} \text{ -----(8)}$$

NPCR value is desirable to guarantee strong diffusion properties in the encryption scheme. A common consideration for NPCR is around 99%, meaning that 99% of the pixels in the cipher text image change when a single pixel in the plaintext image is altered [2].

2.8.3 Unified Average Changing Intensity (UACI)

A further criterion for assessing encryption quality is UACI, or Unified Average Changing Intensity. UACI illustrates. Equation (9) provides a mathematical expression for it, which is defined in [3];

$$\text{UACI}(C1, C2) = \sum_{i,j} \frac{C1(i,j) - C2(i,j)}{R \times G} \times 100\% \text{ -----(9)}$$

The variables C1(i, j) and C2(i, j) represent the grayscale values of the pixels at grid (i, j) in C1 and C2, and the variables G and R denote the total number of pixels in an image, the maximum allowable pixel value, the “original image” and the “cypher image,” respectively.

The least ideal value of UACI as calculated by different authors in [2]-[30] should be 33.33. However, the more the value of UACI is, the more it is preferable.

2.8.4 Mean Square Error (MSE)

Mean Square Error (MSE) is used to measure the difference between the values estimated by a model or system and the values which are observed while processing it in real time. It is usually used in regression analysis to quantify the quality of a system or scheme. MSE can be mathematically defined in equation (10) as expressed in [20], [21]:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [C1(i, j) - C2(i, j)]^2 \text{ -----(10)}$$

The grayscale values of the pixels at grid (I, j) in the original image C2 and the cypher image C1 are represented by C1 (I, j) and C2 (I, j), respectively. The digital image width and height are indicated by M and N, respectively.

According to the proved research of author in [2], MSE should be greater than or equal to 30 decibels to achieve good quality of encryption.

Mathematically, $MSE \geq 30dB$

2.8.5 Analysis of Histogram

It is possible to plot an image's histogram to visually depict the distribution of pixel values in an image. Histogram analysis is used in picture encryption to determine whether the cypher image's histogram is uniform or not. If a cypher image has a uniformly distributed histogram, it indicates that the encryption technique is robust, protecting images from statistical attacks [9].

2.8.6 Chi-Square

The chi-square (χ^2) test is typically used to quantify the histogram analysis, and it may be formally stated as equation (11) as in [9]:

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - \epsilon)^2}{\epsilon} \text{ ----- (11)}$$

$$\epsilon = \frac{H \times W}{256}$$

The cipher image's height and breadth are represented by W and H, respectively, the histogram of the cipher image at index I is represented by f, and the projected value (mean) of the picture is marked by ϵ . It is also advised to maintain the value of χ^2 as low as feasible in order to achieve the encrypted image's uniformly distributed histogram. Therefore, it may be said that the optimal chi-square value for any uniform histogram is close to zero [9].

2.8.7 Entropy

In 1948, Claude Shannon developed the statistical test known as entropy, which quantifies randomness and unpredictability [23]. It is basically used for the quantification of the introduced uncertainty in communication systems.

One consideration for security when encrypting images is that a cypher image with a high entropy will muddle the original image or plaintext more effectively than a cypher image with a low entropy value [9]. Through this, it can be comprehended that Entropy has directly proportional relationship with image encryption quality as shown in (12);

$$\text{Quality of encryption} \propto \text{Entropy} \text{-----} (12)$$

For cryptographic schemes, high entropy values show that the encrypted data is effectively encrypted, and it does not depict any sort of pattern or regularities that could be identified by attackers without decrypting it.

Entropy can be mathematically represented by equation (13) as in [9];

$$H(m) = - \sum_{i=0}^{2^n-1} p(mi) \log_2[p(mi)] \text{-----} (13)$$

The symbol's probability, or the likelihood that a pixel in the image would have value "I," is represented by the symbol p(mi), where n is the number of bits utilized to represent it. The sign p(mi) denotes the normalized histogram counts for each intensity value in the picture. An entropy value for a cypher image is determined by an encryption technique; it should preferably be as near to 8 as is practical since images with lower entropies are more vulnerable to brute force attacks. Because it analyses the pixel information of the entire image rather than simply the randomly chosen portions, the Shannon entropy is referred to as a global entropy [9]. If the value of entropy follows this criterion, then it is considered as a positive sign for the quality of encryption scheme and security against entropy attacks and they are resistant to statistical analysis as well [6].

2.8.8 Correlation

One of the simplest techniques for determining how similar two photos are, this is correlation analysis [4]. It can be calculated by the mathematical formula depicted in equation (14) as in [4];

$$\text{Corr} = \sum_{i,j} \frac{(i-\mu_i)(j-\mu_j)p(i,j)}{\sigma_i\sigma_j} \text{-----}(14)$$

Where p(i,j) denotes the grey level co-occurrence matrices, σ is the standard deviation, μ is the variance, and i,j stand for the picture pixel positions.

The correlation value of the picture should be kept as low as possible to establish an inversely proportional relationship between them in equation (15), which will result in an increasingly random image that needs to be encrypted.

$$\text{Randomness in image} \propto \frac{1}{\text{Value of correlation}} \text{-----(15)}$$

2.8.9 Key Sensitivity

Key sensitivity refers to the significant deviation from the actual result or original image because of a very slight change in the initial conditions. An outstanding image-encryption strategy must have high value of key sensitivity, and its key space must be sufficiently extensive to safeguard against brute force attackers [25].

2.8.10 Homogeneity

Homogeneity corresponds to how close the element distribution is within the GLCM. Lower values of homogeneity are always required for an efficient encryption scheme. Mathematically, it is expressed by using equation (16) as represented in [5]:

$$\text{Homogeneity} = \sum_{(i,j)} \frac{p(i,j)}{1+|i-j|} \text{----- (16)}$$

where p (i, j) represents the gray-level co-occurrence matrices in GLCM.

2.8.11 Contrast

When analyzing picture encryption, contrast analysis is used to see how the encrypted or cypher image differs from the original, or plain text image. It is a quantitative technique that evaluates the difference in contrast between the “original and cypher image” and can be applied to evaluate how well an encryption scheme works.

To achieve the effectiveness of an encryption scheme, it is recommended by different researchers to keep it possibly high. The values of contrast while evaluation image encryption quality can be computed by using equation (17) as mathematically described in [5].

$$C = \sum_{i,j} |i - j|^2 \times p(i,j) \text{-----(17)}$$

2.8.12 ENERGY

When some of the GLCM values have larger magnitudes than others, energy has a high value; when the entries are nearly equal, energy has a low value.

Low energy is required for an encrypted image. Mathematically, image energy is calculated by equation (18) as described in [5]:

$$E = \sum_{i,j} p(i,j)^2 \text{ -----(18)}$$

2.8.13 Maximum Deviation

This encryption quality parameter quantifies how much the original or plain text image's pattern deviates from its original state, depicting a completely different cipher image and high encryption quality. So, it can be concluded that for good encryption algorithms, the value of maximum deviation should be kept as high as possible as represented in (19);

$$\text{Quality of encryption} \propto \text{Maximum Deviation} \text{-----(19)}$$

2.9 Lifting Wavelet Transform (LWT)

The wavelet is contemplated as a mathematical tool which is used for the analysis of signals for the extraction of information from them or data like images. Wavelet Transform is based on the theory of signal's breakdown into a sequence of tiny, local constituents, which are called wavelets. The distinctive feature of wavelet transform is how its decomposition occurs. When the data is decomposed, there is no sort of gapping or overlapping. Hence, wavelet transform is a mathematically reversible procedure. In addition, the lifting wavelet transform is a method for constructing wavelets and carrying out the discrete wavelet transform (DWT). This technique, also referred to as the second-generation wavelet transform, was first presented by Wim Swelders in [24]. The essential characteristic of it is that every derived building lies in the spatial domain. Complex mathematical calculations, which were necessary for the previous conventional approaches, are not needed for this. The lifting scheme can be divided into three subprocesses, as shown in the block diagram below, which is explained in [7]:

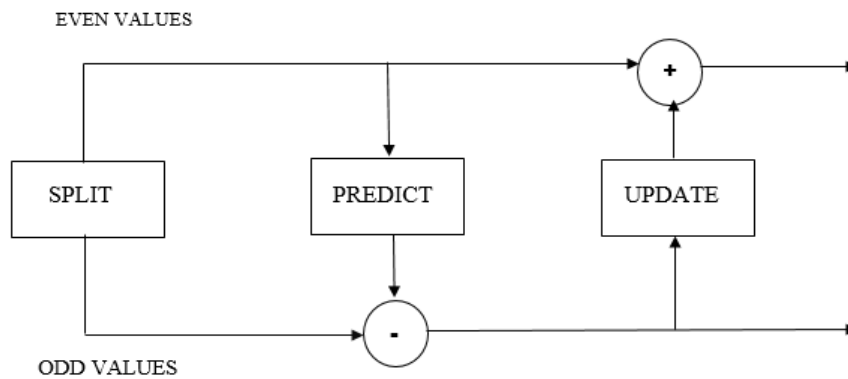


Figure 4 "Lifting Wavelet Scheme."

1. Split Phase:

In the split phase, data is split into even and odd sets to further carry out the procedure of lifting wavelet transform. It entails breaking down a signal into its wavelet and scaling coefficients by means of a sequence of lifting stages. To cut this step in short, the lifting scheme works through the application of a series of basic operations to the input signal, such as shifting, adding, and subtracting. These processes serve the purpose of dividing the signal into high-frequency (wavelet) and low-frequency (scaling) components.

2. Predict Phase:

The prediction step is essential for obtaining effective compression of data and noise reduction. It involves figuring out a particular sample's value according to its neighboring samples, resulting in a compressible residual signal.

3. Update Phase:

The update phase of the lifting wavelet transform (LWT) is a critical step that follows the predicted phase. During the update phase, each wavelet coefficient is adjusted according to the error of prediction, which corresponds to the difference between the signal that existed and the predicted approximation. The update formula is often a weighted sum of both the prediction error and the neighboring wavelet coefficients. This approach reduces the error of prediction, which leads to a more precise depiction of the signal.

2.9.1 Distinctive Features of LWT:

Compared to other conventional wavelets, LWT has the following unique properties:

1. It is capable of being computed more efficiently and requires fewer resources like memory space.
2. Non-linear wavelet transformations are trivial to execute and are commonly used to identify time and frequency.
3. In LWT, there are no quantization errors unlike that usual wavelet transform which is used to possess quantization errors.
4. There's linear phase in LWT and because of that, it does not contain any sort of phase distortion, and this is a crucial aspect for applications like: image processing and audio signal processing.

2.9.2 Inverse Lifting Wavelet Transform (ILWT)

The inverse lifting wavelet transform (ILWT) is a mathematical transform which is used to recreate or regenerate a signal with the help of its wavelet coefficients. In essence, it is the lifting wavelet transform (LWT) in reverse. Figure (3) expresses the Inverse Lifting Wavelet Transform (ILWT), as the authors demonstrated in [26].

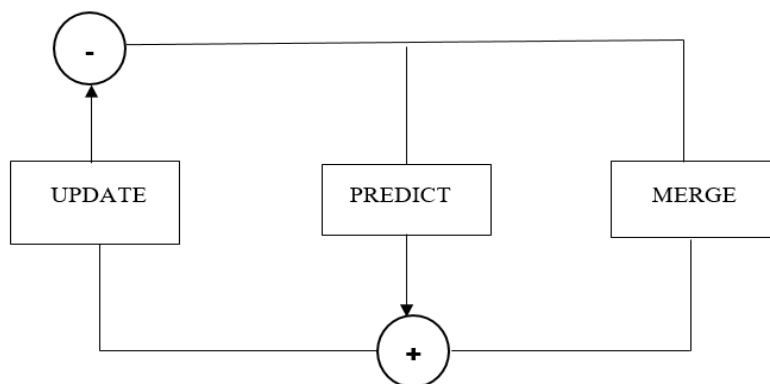


Figure 5 "Inverse Lifting Wavelet Transform" [26]

2.10 Secure Hash Algorithms (SHA)

The Secure Hash Algorithm (SHA) is a group or family of cryptographic hash functions. This is broadly used in multiple security systems and applications to generate fixed-size hash values from the input data. There are various hash functions of Secure Hash Algorithm. Though SHA-256 is a secure algorithm and is broadly used as well, it is computed with 32-bit words. However, in terms of comparison, SHA-512 purveys better security than SHA-256 as SHA-512 is computed with 64-bit words [27].

2.11 Permutation

Permutation is used to scatter the image pixels in image encryption. By using permutation, it makes it much complex and harder for the attacker or unauthorized user to decipher the image and gain the data of the original image. Figure '6' [30] depicts how the strategy of permutation is implemented.

The method presented by Alanezi et al. [29] made use of two chaotic maps: a logistic-sine map was employed to permute the original 'plain-text image', and a logistic-Chebyshev map was added to generate the resultant permuted image [29].

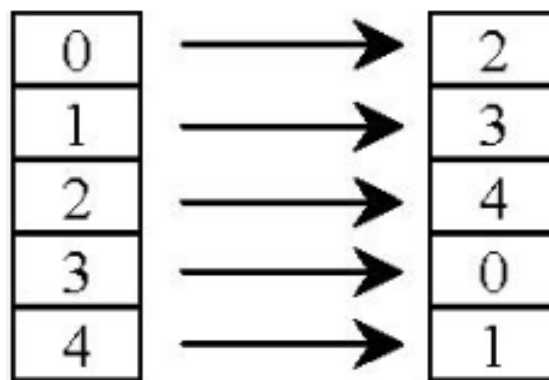


Figure 6 "Strategy of Permutation" [30]

2.12 Substitution

S-Boxes are the foundational components in multiple encryption algorithms, serving as a crucial element to enhance the security of our digital data. It substitutes the original or inputted data with the data of output. In terms of picture encryption, only one substitution box can encrypt the same fields (pixels) of an image into distinct symbols, increasing the level of protection of the procedure for encryption. However, for extremely auto-correlated data, an individual substitution box might not serve as a suitable cryptographic strategy. The S-box changes the values of pixels and introduces diffusion by diffusing a slight difference in the original-image to each pixel of the cipher image. Substitution can be explained by Figure ‘7’ as illustrated in [4].

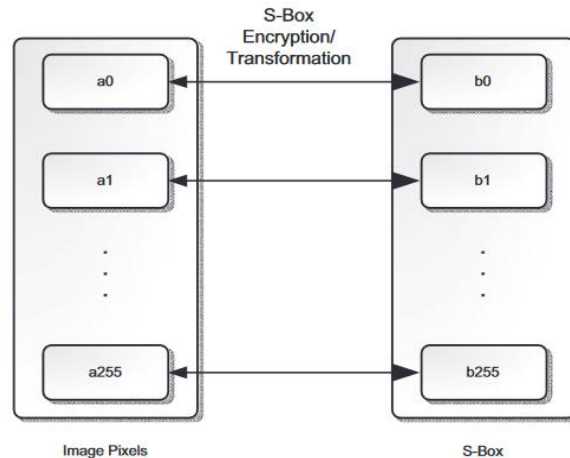


Figure 7 "S-box transformation"[4]

2.12.1 Dynamic S-Box Substitution

Although the substitution of image pixels creates significant variation in the cipher image, to ensure the confidentiality, integrity or security of image data requires efficient substitution methods like dynamic S-box substitution. The S-Box in *AES* deals with the distribution and confusion components of the encryption process, making it resistant to different cryptanalysis approaches [6]. Furthermore, *Hussain S-box* and *Gray S-box* [7] display exceptional security and efficiency. Their robustness is confirmed by different tests such as bit independence, non-linearity, and the majority logic requirements [7,8]. Hence, it can be concluded from [6-8] that Gray and Hussain S-boxes can be implemented by integrating it with the *AES* S-box for a more secure and robust encryption scheme, safeguarding against algebraic and interpolation attacks [10]. Grey S-Box presents rigorous avalanche standards, nonlinearity, and differential uniformity, which are considered ideal for good encryption schemes [10].

Chapter 3

PROPOSED ENCRYPTION SCHEME

3.1 Objective

The primary objective of this thesis is to amalgamate the effective and robust algorithms of image encryption. Through this amalgamation, an integrated form of algorithm is proposed which undergoes different sorts of techniques, mathematical transforms, substitution, and many more to develop a highly chaotic, complex, and deviated cipher image as compared to the original image, hence securing the image data in a much better way than the individual implementation of those algorithms. Running these schemes individually provides sufficiently good results as well but combining them guarantees exceptional outcomes. Due to the multiple schemes deployed in this encryption scheme, there will be more diffusion and confusion added to the original image to convert it into cipher or encrypted image, hence making it extremely difficult for the attackers and unauthorized users to identify the implemented method of encryption and decrypt the image easily and successfully. Hence, the transmission of the image can be made possible in a quite secure manner.

3.2 Constituents of Proposed Integrated Algorithm

To achieve a highly robust and efficient image encryption scheme, following algorithms and mathematical theories are integrated together because of their significance in the field of chaotic displacement of pixels and secure transmission of image data.

- Lifting Wavelet Transform
- SHA-512
- Logistic Sine Cosine Map
- Sine Tent Cosine Map
- Permutation
- XOR
- Tent Sine System
- 16 x 16 Dynamic S-box substitution
- Inverse Lifting Wavelet Transform

This amalgamation not only provides an encryption scheme; it also surveys an elevated quality of encryption with its notable results.

3.3 Hybrid Chaotic Maps in Proposed Scheme

Hybrid chaotic maps are generated after integrating two or more chaotic maps or systems. They have applications in multiple fields like cryptography, secure communications, random number generation, and nonlinear dynamics research. Hybrid chaotic maps provide improved chaotic behavior as compared to the implementation of individual chaotic maps and they can also be customized according to specific requirements or applications by selecting befitting combination of maps and parameters. By using various hybrid chaotic maps, chaotic range is also enhanced for the proposed image encryption scheme.

3.3.1 Logistic Sine Cosine Map

The suggested plan transmits the photos securely across several platforms by utilizing the logistic sine cosine chaos system, a more focused version of the Cosine transforms based chaos system (CTBCS). One way to think of CTBCS is as a chaos system that improves upon two simpler chaos systems. CTBCS can be described mathematically in equation (2) and expressed in [3].

$$x_{i+1} = \cos(\pi(4rx_i(1-x_i) + (1-r)\sin(\pi x_i) - 0.5)) \text{ -----(2)}$$

where r belongs to $[0,1]$

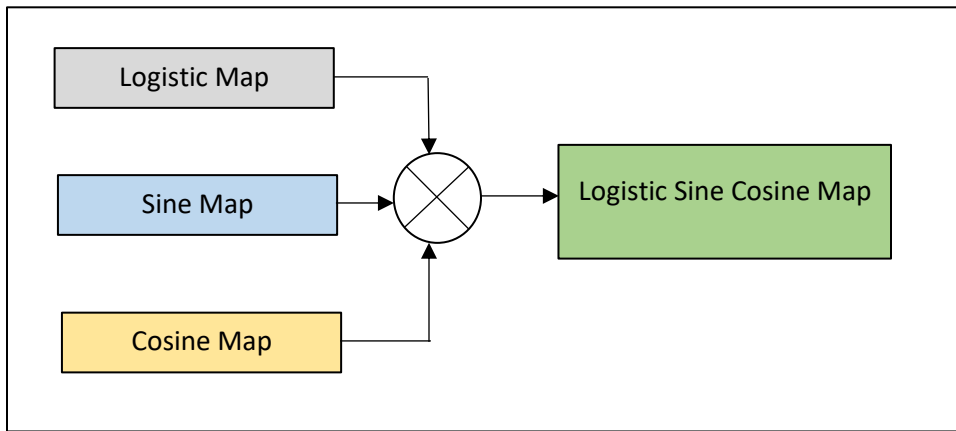


Figure 8 "Generation of Logistic Sine Cosine Map."

3.3.2 Sine-Tent Cosine Map

Another map which is used in this proposed scheme is Sine-Tent-Cosine (STC) Map, STC map is also one of the most famous chaotic maps which is used in image encryption. It is actually a fusion of sine and cosine functions which is then applied to the pixels of that particular image which has to be encrypted. STC map is recommended because of its chaotic behavior, ensuring the efficiency of encryption by depicting the image as random noise to the unauthorized users, facilitating a high level of security.

Furthermore, due to the extreme chaotic behavior of STC map, it offers defense against multiple cryptanalytics. It can be mathematically defined by equation (3) as depicted in [3]:

$$x_{i+1} = \begin{cases} \cos(\pi(r \sin(\pi x_i) + 2(1-r)x_i - 0.5)) & \text{for } x_i < 0.5; \\ \cos(\pi(r \sin(\pi x_i) + 2(1-r)(1-x_i) - 0.5)) & \text{for } x_i \geq 0.5, \end{cases} \text{-----(3)}$$

where the parameter $r \in [0, 1]$

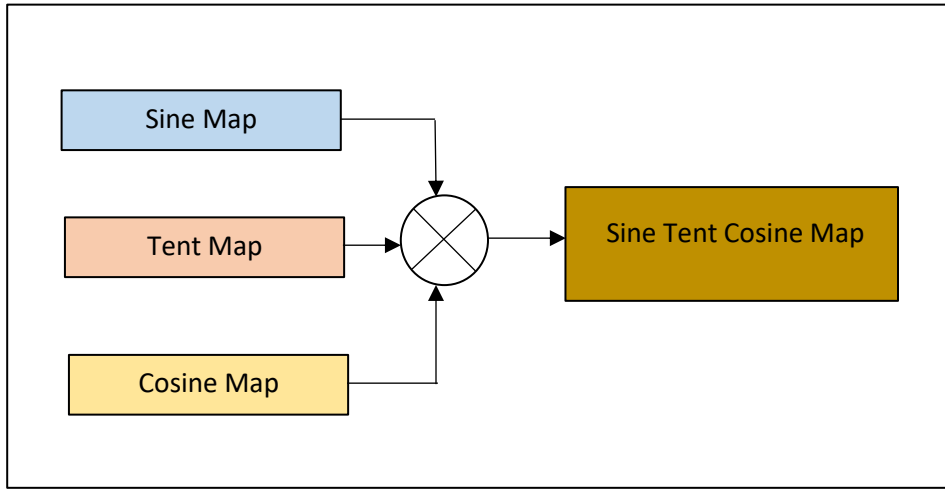


Figure 9 "Generation of Sine Tent Cosine Map."

3.3.3 Tent-Sine System

The authors presented a novel compound chaotic system in [28], which incorporates the essential elements of Tent and Sine maps, in response to the shortcomings observed in one-dimensional (1D) chaos-based systems. The combined chaos system that results from this is called the Tent-Sine (TS) chaos system. The mathematical representation of it is given in equation (4) as stated in [28];

$$x_{n+1} = \begin{cases} (4 * (\sin(2 * \pi * x_n * r)) + x_n) \text{MOD}1, & \text{if } 0.0 < x_n < 0.5 \\ (4 * (\sin(2 * \pi * x_n * r)) + (1 - x_n)) \text{MOD}1, & \text{if } 0.5 \leq x_n < 1.0 \end{cases} \text{-----(4)}$$

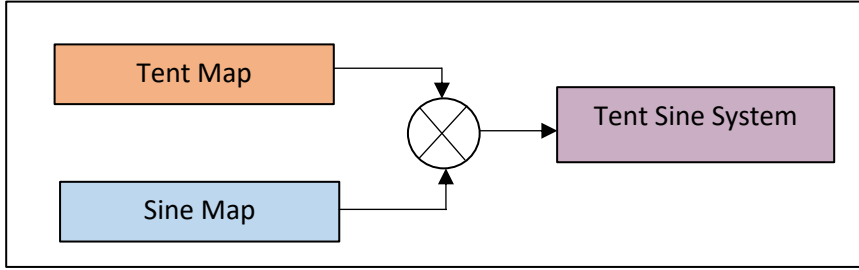


Figure 10 "Generation of Tent Sine System."

3.4 Wavelet Transforms in Proposed Scheme

The mathematical transforms can be integrated with encryption algorithms like; chaotic maps, or traditional cryptographic techniques as previously implemented in symmetric or asymmetric encryption to ensure secure image transmission. The mathematical transforms are specifically chosen on the basis of the desired level of security, level of complexity and other specific requirements. As per the requirements, the proposed scheme combines Lifting Wavelet Transform (LWT) & Inverse Lifting Wavelet Transform (ILWT) to encrypt the image into a cipher image.

3.5 Extraction of LL Component from LWT

The image is really divided into four frequency sub-bands following two dimensional decompositions: LL (low-low), LH (low-high), HL (high-low), and HH (high-high). Among all these bands, the LL component is the most sensitive. Since it has the lowest frequency components, it preserves most of the image's information, preventing data loss during encryption. It is the best possible approximation of the original image and is also referred to as the approximation sub-band [35].

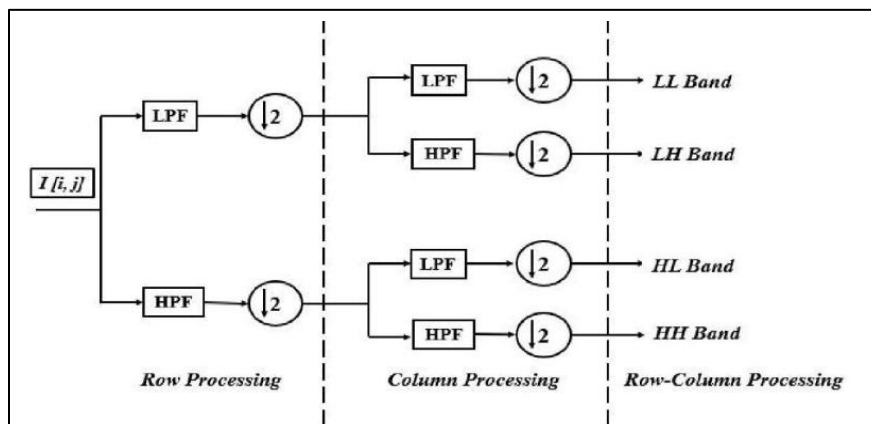
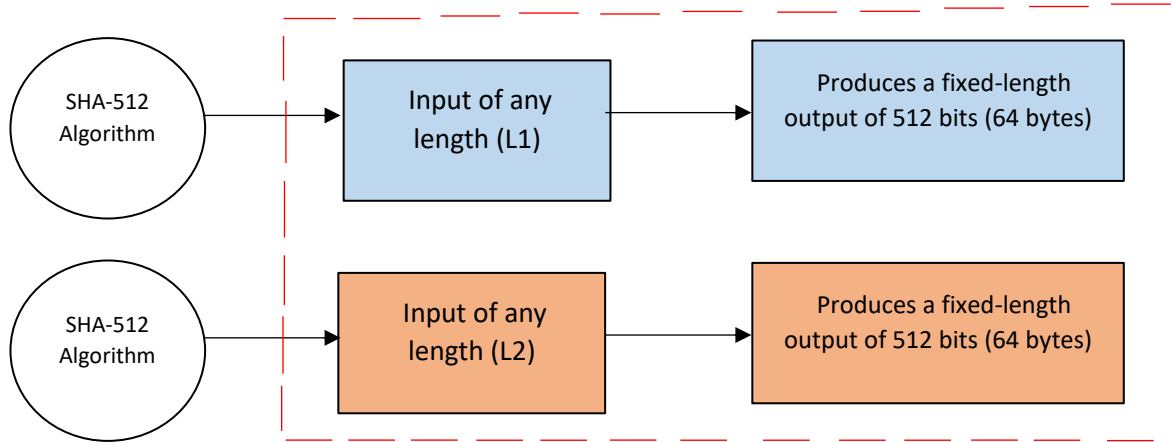


Figure 11 " Lifting Wavelet Transform Decomposition" [35]

3.6 Secure Hash Algorithm in Proposed Scheme

Although there are multiple hash functions that belong to the family of Secure Hash Algorithm (SHA), but SHA-512 is specifically chosen for the proposed scheme because it is a secure hash function, and it is widely used in a variety of applications. As Figure '12' illustrates, a relatively small change in the input value causes a substantial variation in the result in SHA-512. SHA-512 algorithm works by following the scheme as represented in Figure '13' in [33].



Slight difference in input values results in completely different output values.

Figure 12 "Changes caused by input variations in SHA-512 algorithm."

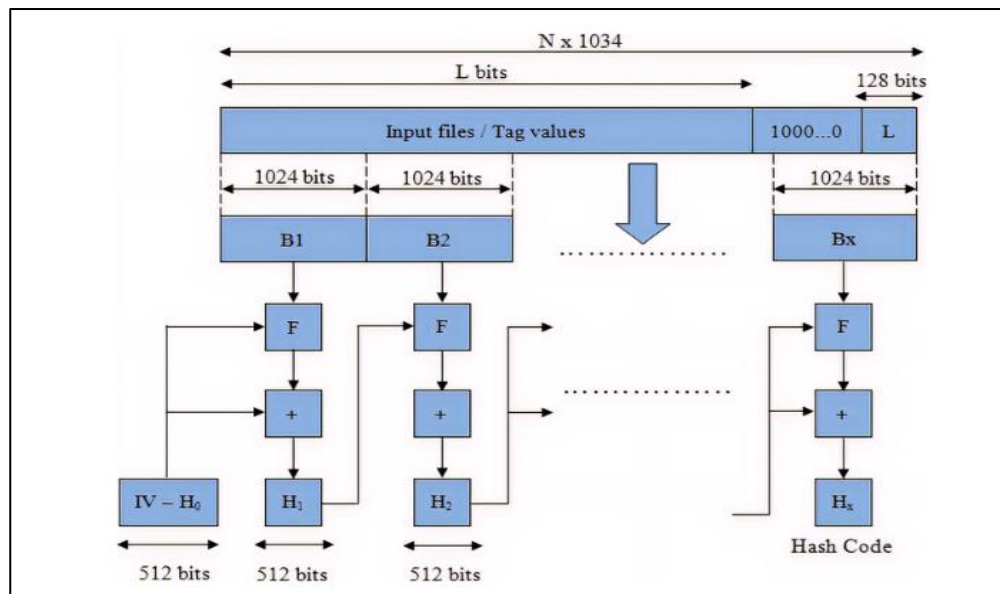


Figure 13 "Workflow of SHA-512 algorithm" [33]

3.7 Application of Permutation in Proposed Scheme

Figure “6” illustrates the approach that is used to create the permuted cypher image. After separating and extracting the LSB and MSB bits as shown in figure “16,” the chaotic sequence produced by the Logistic-Sine-Cosine map is used to carry out this image permutation process. Confusion is thereby added to the encrypted image. By randomly scrambling the pixel information throughout the image, this encryption technique improves the security of the encryption process. This application can be summarized by figure ‘14’ as follows.

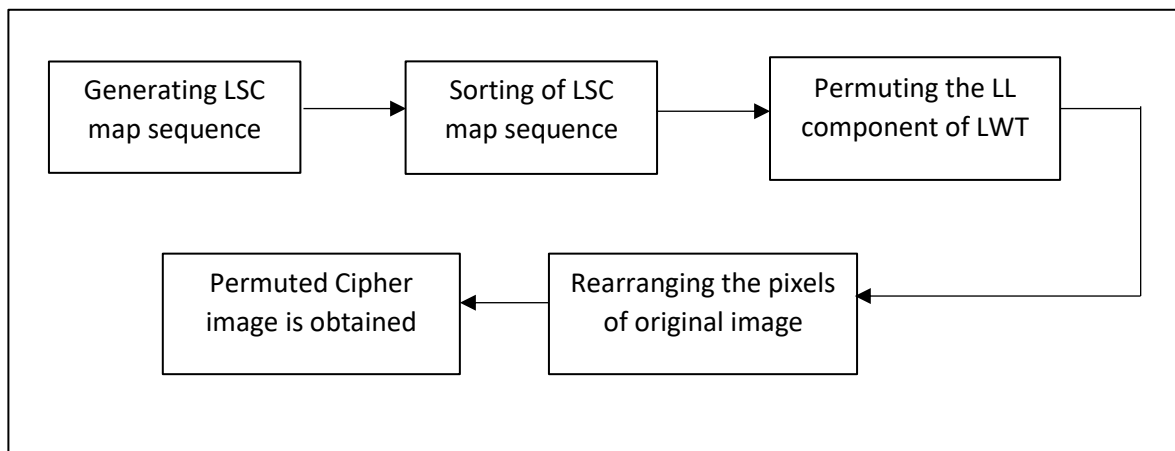


Figure 14 "Application of permutation in proposed scheme"

3.8 Application of Dynamic S-box Substitution in Proposed Scheme

This proposed approach introduces substitution using Figure ‘7’ transformative strategy. Three distinct S-boxes: the AES S-box, the Hussain S-box, and the Grey S-box were used in this system. Tent Sine map is used to create the chaotic sequence before continuing with the process. Next, by using modulus to determine the proper S-box selection, this chaotic sequence is transformed into a 0,1,2 sequence. The encrypted image’s pixels that remain after permutation are then subjected to dynamic S-Box substitution. Each pixel of the encrypted image is iterated to convert its value to binary, and then that binary value is split into MSB and LSB. Furthermore, inside the nested loop of encrypted image’s pixel, the appropriate S-Box is chosen based on the current index. The corresponding entry is made in accordance with the selected S-Box, and the S-Box value is used to replace the value of each pixel in the image.

3.9 Workflow of Proposed Encryption Algorithm

To put the suggested encryption technique into practice, take the following actions:

1. Read the input original image.
2. A lookup table is then computed for hexadecimal to binary conversion by this command.

```
hexToBinaryLookup = dec2bin(0:15, 4)
```

3. Each and every hexadecimal digit is then converted to binary and concatenated by.

```
binaryHash =  
reshape(hexToBinaryLookup(hex2dec(shaHash(:))+1,:),'',1,[])
```

4. The hash of the input image 'O' is then computed by using SHA-512 algorithm.

```
shaHash = DataHash(image, 'SHA-512')
```

5. Then the first 368 bits are extracted from the computed binary hash by.

```
HV = binaryHash (1:368)
```

6. The binary hash is then divided into MSB and LSB of 184 bits.
7. Along with the computation of hash, lifting wavelet transform (LWT) is also performed on the other hand on input image as depicted in Figure '4' using the Haar wavelet by setting the level of decomposition and other factors, hence obtaining LL band through LWT.
8. After further splitting into MSB and LSB, each with 92 bits, a chaotic sequence is then produced using the Logistic Sine Cosine (LSC) map, as indicated in equation (2).
9. The MSB of the computed hash is then used to obtain the initial condition (X_0) and parameter (r) for the LSC map.
10. The Logistic Sine Cosine map is then iterated by using the same equation as used in step 8 to generate a chaotic sequence.

11. The chaotic sequence is then sorted and truncated to form a permutation map.
12. Afterwards, the LL component of the LWT is permuted using the permutation map and LSC map, acquiring the permuted image 'P'.
13. Another chaotic sequence is generated using the Sine Tent Cosine (STC) map by applying equation (3) and utilizing LSB (92 bits) of the hash to obtain the initial condition (X_0) and parameter (r) for the STC map.
14. Modulus is then taken to acquire integers between 0 to 255.

$$\text{mod}(x, 256)$$

15. The obtained gray scale image is then arranged into 128x128 block size, generating a ZxZ block of STC component.
16. Each and every pixel of permuted image 'P' is then XORed with the ZxZ block of STC sequence, it can be computed as.

$$\text{bitxor}(P, \text{STC_ZxZ})$$

17. The obtained results are then further computed to perform dynamic S-box substitution using three different S-boxes i.e. AES, Hussain and Gray S-box.
18. Tent Sine System is then deployed, generating another chaotic sequence as TSS.
19. Afterwards, modulus is taken for the TSS sequence to generate integers: 0,1 and 2 as;

$$\text{mod}(\text{round}(\text{TSS_x} * 3), 3)$$

20. The XORed image is then substituted by denoting the implemented maps as 0,1,2 and then the conditional loop follows to choose the corresponding integer from TSS sequence, hence appropriate S-box is selected to represent the replacement image by substituting the pixel values.

21. Finally, as shown in Figure ‘5,’ the replacement image is subjected to the inverse lifting wavelet transform (ILWT) utilizing the Haar wavelet.

21. After going through the whole procedure, the final encrypted image is acquired.

3.9.1 Flow Chart of Proposed Encryption Algorithm

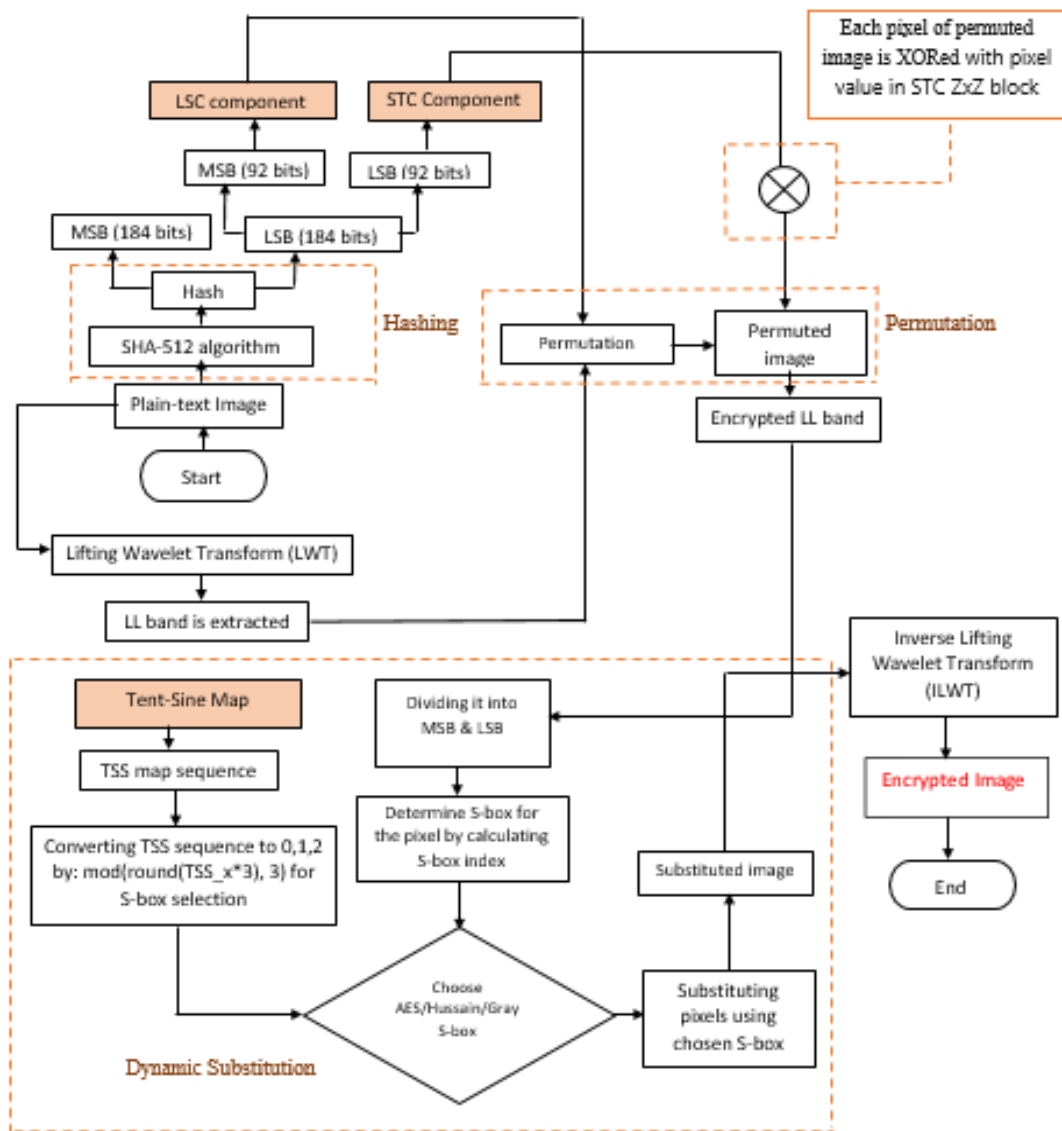


Figure 15 "Flowchart of Proposed Encryption Scheme"

3.9.2 Procedural Encryption of Cameraman & Its Histograms

- (a) Original Cameraman Image & its histogram is acquired to assure the correctness of decrypted image afterwards.

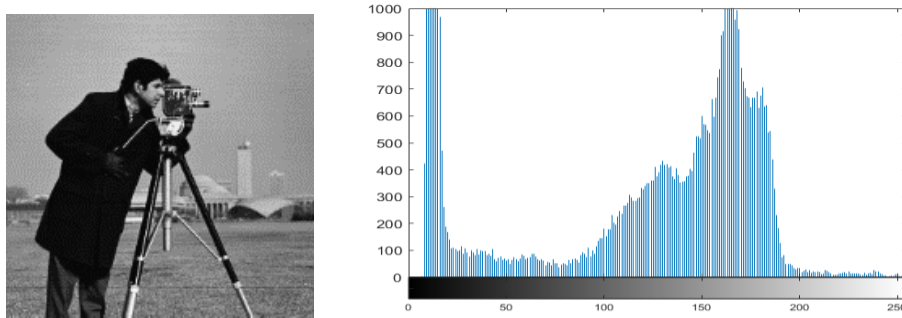


Figure 16 "Original Cameraman Image & its Histogram"

- (b) Permuted Image of Cameraman & its histogram is obtained after applying Logistic-Sine Cosine Map & scheme of permutation.

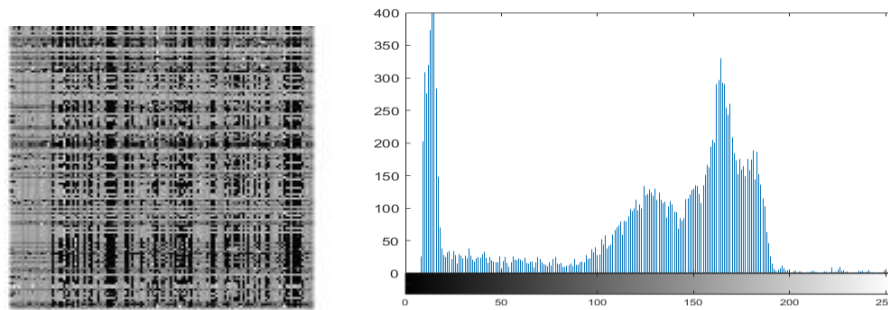


Figure 17 "Permuted Image of Cameraman & its Histogram"

- (c) Permuted image is re-encrypted with extracted CA (obtained from Lifting Wavelet Transform) & Sine-Tent Cosine Map using 'XOR'.

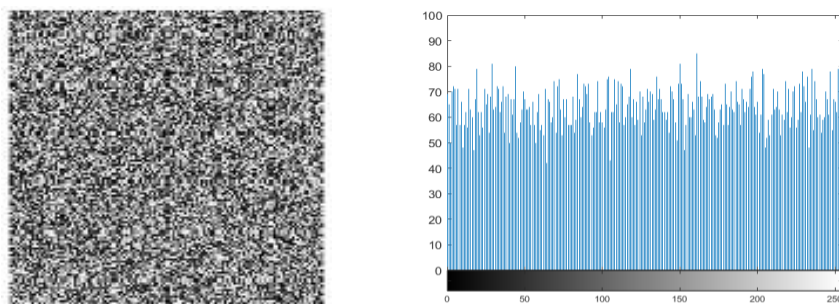


Figure 18 "Encrypted CA of Cameraman Image & its Histogram"

(d) Tent-Sine map is implemented on dynamic 16 x 16 S-boxes to acquire a substituted cipher image.

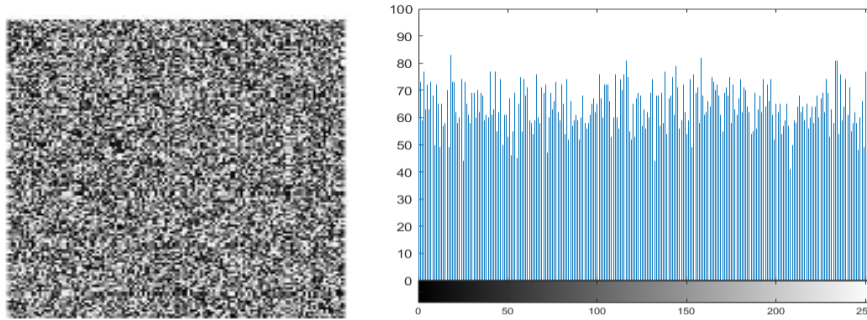


Figure 19 "Substituted Cipher of Cameraman Image & its Histogram"

(e) Inverse Lifting Wavelet Transform (ILWT) is applied on substituted image to generate the final encrypted image.

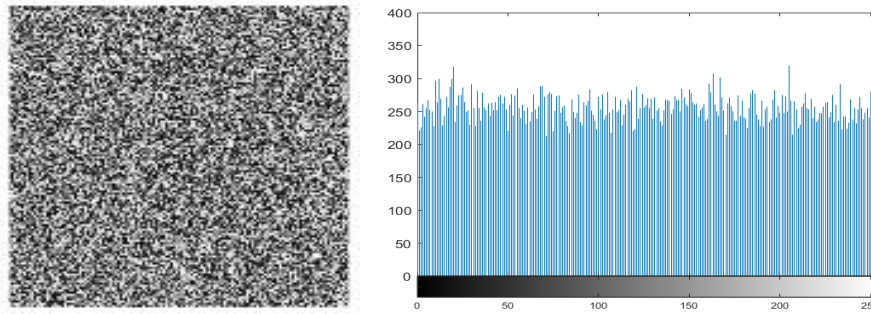


Figure 20 "Encrypted Cipher of Cameraman Image & its Histogram"

3.10 Decryption of the Proposed Scheme

The decryption algorithm acts as a precise countermeasure to the encryption process, rigorously reversing each step to recover the original image. The encrypted image is first subjected to Lifting Wavelet Transform to reverse the wavelet transform and reconstruct the frequency sub-bands, specifically the LL band that contains most of the image's information. On the received output, an inverse of the dynamic S-box substitution method is applied. This step is critically dependent on the correct selection sequence, which itself is a product of the Tent-Sine System map, intricately linked to the initial key. The chosen S-Boxes, AES, Grey, and Hussain S-Boxes are applied in reverse, guided by the key-derived sequence, restoring the pixel values to their intermediate state prior to the final encryption layer.

Following this, the encrypted image is methodically permuted in reverse. The original encryption's chaotic sequence, derived from the Logistic-Sine-Cosine and Sine-Tent-Cosine maps, serves as a cipher to the pixel disarray, dictating the unscrambling process. With the help of the original chaotic sequences generated by the LSC and STC components, reverse permutation is applied to the LL band to restore the pixels to their original locations. On the

received output, XOR operation is applied with the same pixel values from the ZxZ block derived from the STC sequence, is used during encryption to retrieve the permuted image prior to its last encryption step. In order to retrieve the sub-bands, ILWT is applied to the unscrambled LL band along with the other high-frequency sub-bands (LH, HL, HH) to reconstruct the original image. This step requires using the exact lifting scheme and level that were used during the encryption.

To finalize the decryption, the integrity of the reconstructed image can be tested against the original SHA-512 hash. This cryptographic checksum, unyielding in its precision, would confirm the integrity. Hence, the hash of the decrypted image is compared with the hash of the original image to ensure that decryption was successful, and the image integrity is maintained.

Chapter 4

RESULTS AND DISCUSSION

4.1 Visual Performance of Proposed Encryption Scheme

The tested cameraman image is evaluated on the basis of the evaluation metric of ‘histogram’ to verify the quality of image encryption.

4.1.1 Histogram Analysis of Tested Image

The histogram data shows that the proposed technique performs exceptionally well when comparing the histograms of the original and cypher photographs. This is because, after applying the final Inverse Lifting Wavelet Transform (ILWT) technique, the encrypted cameraman image’s histogram, as shown in Fig. 22(b), exhibits a uniform distribution along the “x” and “y” axes. This reflects the outstanding encryption quality of the suggested system. As discussed in chapter 2, the resilience of the encryption scheme protects images against statistical attacks if a cipher image has a uniformly distributed histogram [9].

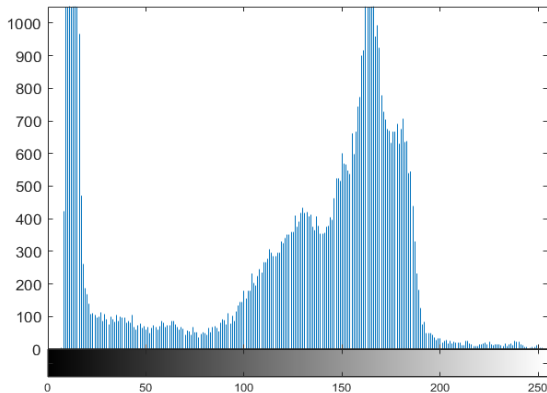


Figure 21 (a) “Histogram of Original Image”

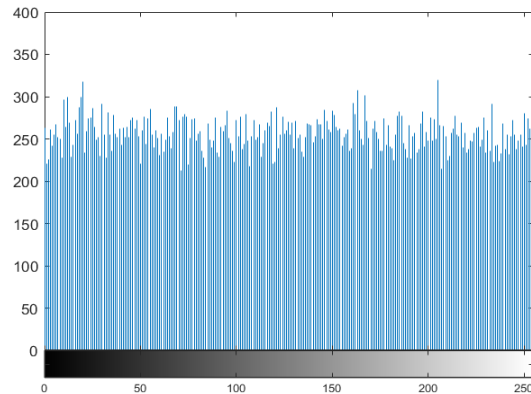


Figure 21(b) “Histogram of Encrypted Image”

4.2 Security, Confidentiality & Preservation of Images

To ensure the security, confidentiality, and retrieval of an image encryption algorithm against multiple sorts of attacks including brute force attack, statistical, or differential attacks, following parameters can be evaluated and then compared to the standard or ideal values.

4.2.1 Correlation Coefficient

By using equation (14), correlation values are calculated for cipher image as represented in Table ‘2’. As discussed in chapter 2, the value of correlation coefficient of cipher image should be reduced as much as possible, keeping it near to zero.

Table 2: Correlation values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[5]	[4]	[11]
Correlation coefficient	0.029	0.04	0.06	0.03

4.2.2 Information Entropy

By using equation (13), the value of information entropy is calculated and depicted in ‘Table 3’. This is calculated by considering the Shannon criterion [23] that the closer the value of entropy is to 8, the better the quality and confidentiality of image encryption algorithm is.

Table 3: Entropy values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[4]	[6]
Information entropy	7.972	7.653	7.903

4.2.3 NPCR & UACI

The values of NPCR & UACI are calculated by using equation (7) & (9) and shown in Table ‘4’ and ‘5’ respectively. As discussed in chapter 2, it is suggested by different researchers that the values of NPCR must be equal to or greater than 99% and UACI to be at least 33.33% or more.

Table 4: NPCR values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[4]	[6]
NPCR	99.6	99.3	99.6

Table 5: UACI values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[4]	[6]
UACI	30.417	31.4	33.44

4.2.4 PSNR

Peak signal to noise ratio (PSNR) is calculated by using equation (5) as shown in Table ‘6’. It has been verified by different researchers that the lower the value of PSN, the more it is preferred for good encryption scheme.

Table 6: PSNR values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[9]	[4]
PSNR	8.599	8.44	8.33

4.2.5 MSE

Similarly, the Mean Square Error (MSE) is calculated by equation (10) and its resultant value is depicted in ‘Table 7’. By the verification of existing research in chapter ‘2’, it can be concluded that the value of MSE should be greater than or equals to 30dB to verify the good quality of encryption.

Table 7: MSE values of Cipher Image & its comparison with existing methods

Security Parameter	Proposed Scheme	[2]	[16]
MSE	39.53	33.42	38

As per the computed results of Correlation coefficient in ‘Table 2’, Information entropy in ‘Table 3’, NPCR in ‘4’, UACI in ‘5’, PSNR in ‘Table 6’, and MSE in ‘7’, it is verified that the encryption quality is up to the mark, but it falls short of the UACI standard only.

4.2.6 Computational Speed

Despite the complexity of the proposed encryption algorithm, the encryption algorithm exhibits impressive computational speed, completing the encryption process in under 2 seconds on a system equipped with MATLAB 2023, Windows 11 OS, an 11th Gen Intel i7 processor, and 8 GB of RAM, underscoring the efficiency of the algorithm and the processing power of the hardware.

CHAPTER 5

CONCLUSION AND FUTURE RECOMMENDATIONS

5.1 Overall Scheme of Proposed Algorithm

To culminate, the proposed image encryption scheme bestows exemplified exceptional image encryption quality and efficiency as per its computed results. This scheme requires multiple hybrid chaotic maps to generate chaos based sequence, SHA-512 to generate hash functions for encrypted image, Inverse Lifting Wavelet Transform (ILWT) breaks down the original image into smaller bands, whereas Lifting Wavelet Transform (LWT) transforms the simple text image and gains the LL band, enabling compression sensing strategy in this scheme, permutation to rearrange pixel values of plaintext image, and substitution technique to replace the pixel values, adding extreme confusion and diffusion into the plaintext image for high level security of transmission of multimedia data.

To cut the long story short, all the multiple schemes which are integrated in this thesis hold significant importance in the field of image encryption and it is clearly depicted from the computed results of entropy, correlation, visual representation of histograms, NPCR & UACI, PSNR, and MSE of cipher image in contrast to the originally transmitted image sent by the sender. Hence, the proposed scheme in this thesis surpasses high encryption quality while transmitting multimedia data in real world.

Specifically, this image encryption approach is depleted in frequency domain and image encryption method is applied on LL band along with the different encryption techniques and maps to fasten the processing time, improve the compression sensing capability of algorithm, and increase the chaotic range for transmission of images. Hence, this method is ideal for a variety of applications because it effectively defends sensitive data against real-world threats like statistical, brute force, and differential attacks.

5.2 Future Roadmap for Image Encryption

Although multiple approaches and principles have been laid down in the field for image encryption algorithms to secure the transmission of confidential multimedia data but there is still a lot to be done. In the next ten years, there will be noticeable technological advancements in IT and this will definitely shift the landscape of digital realm to higher heights. Image encryption algorithms and schemes can be further modified by integrating the newly introduced techniques in parallel with the existing schemes.

Following methods can be assessed and implemented to mitigate attacks on multimedia data by making such schemes more effective and efficient to proceed in just pico (10^{-12} seconds), femto (10^{-15} seconds), attoseconds (10^{-18} seconds), zeptoseconds (10^{-21} seconds), or even in only yoctoseconds (10^{-24} seconds), making image encryption extremely cost effective because of less consumption of resources and time.

- Advanced machine learning algorithms can be integrated with chaos-based maps and neural networks to enhance the encryption techniques and optimize the key generation. The quality improvement of existing image encryption algorithms can also be done based on data driven methods to ensure long term security for image data.
- To maintain the integrity of multimedia data during image transmission, quantum attacks can also take place. To defend against such attacks, quantum computing should be implemented along with encryption algorithms and post-quantum methods should be implemented to introduce robust cryptographic approaches.
- Symbolic reasoning techniques can be integrated with neural network-based learning strategies to develop an image encryption algorithm that can enhance security measures for image data transmission.
- Zero-knowledge Proof (ZKP) techniques can be implemented after improving its scalability and performance issues to maintain the integrity of confidential data by keeping the approach cost effective and time efficient as well.
- To increase the precision of cryptographic encryption schemes, AI techniques ought to be combined with picture encryption algorithms. This amalgamation will lead to quick detection and mitigation of the pre and post risk factors during image transmission.
- Block-chain based image encryption algorithms should be further integrated with compatible Zero Knowledge Proofs (ZKP) techniques and homomorphic encryption schemes, making it harder for the attackers to decipher the cipher images.
- Lastly, Bio-encryption algorithms can also be introduced to store the confidential data of images in the form of biological molecules of living organisms like; DNA (preferably), RNA, Proteins, or carbohydrates.

Altogether, new developments, evaluations, and research in cryptographic picture encryption may produce state-of-the-art encryption techniques and data security system solutions.

REFERENCES

- [1] S. Kemp, "Digital 2023: Global Overview Report," *DataReportal*, Jan. 26, 2023. <https://datareportal.com/reports/digital-2023-global-overview-report>
- [2] J. Ahmad and F. Ahmed, 'Efficiency Analysis and Security Evaluation of Image Encryption Schemes,' *International Journal of Video & Image Processing and Network Security*, Vol. 12, No. 4. 2012, pp. 18-31. -
- [3] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, Apr. 2019, doi: <https://doi.org/10.1016/j.ins.2018.12.048>.
- [4] 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, no. 9, pp. 3106–3118, Sep. 2014, doi: <https://doi.org/10.1016/j.cnsns.2014.02.011>.
- [5] A. Qayyum *et al.*, "Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020, doi: <https://doi.org/10.1109/access.2020.3012912>.
- [6] J. Ahmad and Seong Ju Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," vol. 82, no. 4, pp. 1839–1850, Jul. 2015, doi: <https://doi.org/10.1007/s11071-015-2281-0>.
- [7] Z. Rim, E. Ridha, and Z. Mourad, "An improved partial image encryption scheme based on lifting wavelet transform, wide range Beta chaotic map and Latin square," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 15173–15191, Feb. 2021, doi: <https://doi.org/10.1007/s11042-020-10263-3>.
- [8] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, Apr. 2014, doi: <https://doi.org/10.1016/j.sigpro.2013.10.034>.
- [9] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, p. 1344, Sep. 2022, doi: <https://doi.org/10.3390/e24101344>.
- [10] Ahmad, J., & Hwang, S. (2015). "A Fast Encryption/Decryption Scheme for Biometric Images Using Multiple Chaotic Maps." *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 347-353, 2015
- [11] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A New Chaos-Based Image-Encryption and Compression Algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–11, 2012, doi: <https://doi.org/10.1155/2012/179693>.
- [12] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, p. 2585, Jan. 2023, doi: <https://doi.org/10.3390/math11112585>.

- [13] Z. Zhang, Y. Cao, Hadi Jahanshahi, and J. Mou, "Chaotic color multi-image compression-encryption/ LSB data type steganography scheme for NFT transaction security," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 10, pp. 101839–101839, Dec. 2023, doi: <https://doi.org/10.1016/j.jksuci.2023.101839>.
- [14] Priyanka and A. K. Singh, "A survey of image encryption for healthcare applications," *Evolutionary Intelligence*, Jun. 2022, doi: <https://doi.org/10.1007/s12065-021-00683-x>.
- [15] B. Zolfaghari and T. Koshiba, "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap," *Applied System Innovation*, vol. 5, no. 3, p. 57, Jun. 2022, doi: <https://doi.org/10.3390/asi5030057>.
- [16] A. S. Almasoud, Bayan Alabdullah, H. Alqahtani, S. S. Aljameel, S. S. Alotaibi, and A. Mohamed, "Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security," *Heliyon*, vol. 10, no. 3, pp. e25257–e25257, Feb. 2024, doi: <https://doi.org/10.1016/j.heliyon.2024.e25257>.
- [17] Bhat, J., Jasra, S., Saqib, M., & Moon, A. (2021). "Image Encryption Using Logistic-Cosine-Sine Chaos Map and Elliptic Curve Cryptography." *Journal of Theoretical and Applied Information Technology*, vol. 99, pp. 3970-3986, 2021.
- [18] Sajjad Shaukat Jamal, Amir Anees, M. Ahmad, Muhammad Fahad Khan, and I. Hussain, "Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System," *IEEE Access*, vol. 7, pp. 173273–173285, Jan. 2019, doi: <https://doi.org/10.1109/access.2019.2956385>.
- [19] M. El-Iskandarani, S. Darwish, and S. Abuguba, "A robust and secure scheme for image transmission over wireless channels," in *Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on*. IEEE, 2008, pp. 51–55
- [20] A. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of rc5 and rc6 block ciphers on digital images," in *Systems, Signals and Devices (SSD), 2011 8th International Multi-Conference on*. IEEE, 2011, pp.1–6.
- [21] A. Cheddad, J. Condell, K. Curran, and P. McKeivitt, "Securing information content using new encryption method and steganography," in *Digital Information Management, 2008. ICDIM 2008. Third International Conference on*. IEEE, 2008, pp. 563–568.
- [22] Y. Wu, J.P. Noonan, S. Aгаian, NPCR And UACI randomness tests for image encryption, *Cyber J. Multidisci. J. Sci. Technol. J. Select. Areas Telecommun.(JSAT)* (2011) 31–38.
- [23] Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* 1948, 27, 379–423. [CrossRef]
- [24] Daubechies I, Sweldens W (1998) Factoring wavelet transforms into lifting steps. *J Fourier Anal Appl*4(3):247–269

- [25] Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* 2004, 21, 749–761. [CrossRef]
- [26] Basheer, Taha & Basheer, Dujan & Ngadiran, Ruzelita & Ehkan, Phaklen. (2021). Digital Image Recovery Based on Lifting Wavelet Transform. *Journal of Physics: Conference Series*. 1962. 012021. 10.1088/1742-6596/1962/1/012021.
- [27] P G, Shynu & Rk, Nadesh & Menon, Varun & Parameswaran, Venu & Abbasi, Mahdi & Khosravi, Mohamadreza. (2020). A secure data deduplication system for integrated cloud-edge networks. *Journal of Cloud Computing Advances Systems and Applications*. 9. 1-12. 10.1186/s13677-020-00214-6.
- [28] Annas Wasim Malik, Amjad Hussain Zahid, David Samuel Bhatti, Yang Soo Kim, and K.-I. Kim, “Designing S-Box Using Tent-Sine Chaotic System While Combining the Traits of Tent and Sine Map,” *IEEE Access*, vol. 11, pp. 79265–79274, Jan. 2023, doi: <https://doi.org/10.1109/access.2023.3298111>.
- [29] Alanezi, A.; Abd-El-Atty, B.; Kolivand, H.; El-Latif, A.; Ahmed, A.; El-Rahiem, A.; Sankar, S.; S Khalifa, H. Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment. *Secur. Commun. Netw.* 2021, 2021, 6615512. [CrossRef]
- [30] “Permutation-Based Cryptography | A’s Online Journal,” *Permutation-Based Cryptography | A’s Online Journal*. <https://anthonilockheart.blogspot.com/2013/05/permutation-based-cryptography.html> (accessed Feb. 21, 2024).
- [31] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.
- [32] M. Alawida, A. Samsudin, and J. S. Teh, “Enhancing unimodal digital chaotic maps through hybridisation,” *Nonlinear Dyn.*, vol. 96, no. 1, pp. 601–613, Jul. 2019.
- [33] Shynu P G, John Singh K (2016) A comprehensive survey and analysis on access control schemes in cloud environment. *Cybern Inf Technol* 16:19–38. <https://doi.org/10.1515/cait-2016-0002>
- [34] M. Alawida, A. Samsudin, J. S. Teh and W. H. Alshoura, "Digital Cosine Chaotic Map for Cryptographic Applications," in *IEEE Access*, vol. 7, pp. 150609-150622, 2019, doi: 10.1109/ACCESS.2019.2947561.
- [35] Mahalingam, H. et al. (2023) ‘Dual-domain image encryption in unsecure medium—a secure communication perspective’, *Mathematics*, 11(2), p. 457. doi:10.3390/math11020457.