Hybrid Cryptosystem with Computational Ghost Imaging Based on Integer Wavelet Transform and Chaotic Maps

Khalid T. Alnidawi[1†], and Ali M. Sagheer[2]

[1]Department of Computer Science, College of Computer Science and IT, University of Anbar, Ramadi, Iraq

[2]Department of Computer Networks System, College of Computer Science and IT, University of Anbar, Ramadi, Iraq

***Abstract*—Computational ghost imaging encryption (CGIE) has gained increasing attention from researchers in the field of optical cryptography due to its unique phenomenon. However, traditional CGIE suffers from long imaging time, inherent system linearity, and an enormous number of random phase masks that must be transmitted as secret keys, which limits its application in practical communication. In this paper, a hybrid optical image encryption approach is proposed using CGIE based on integer wavelet transform and chaotic maps. In addition, Hadamard basis patterns are employed to reduce sampling times and improve reconstructed image quality. Simulation results demonstrate that the proposed system is robust against different types of attacks with high key sensitivity and low execution times of 0.03 s for encryption and 0.14 s for decryption. This approach will ensure broader adoption of this technology by facilitating its integration into cryptosystems.**

***Index Terms*—Chaotic maps, Cryptography, Ghost imaging, Optical image encryption, Wavelet transform.**

I. Introduction

The amazing phenomenon of computational ghost imaging (CGI) led us to focus on incorporating it more widely in image encryption systems (Liu, Wang and Zhao, 2022). Due to the special properties of CGI, such as non-local imaging by encoding the image into intensity correlation between the original image and the projected random patterns, make it a valuable technique in optical cryptography (Zhang, Wang and Zhang, 2022). CGI is a new technique that has been widely used since it appeared. This technique has a simple structure. The specialized light source continuously generates a changing laser speckle pattern and projects it onto an object, then uses a lens to direct the light that passes the object to a bucket detector to record the total intensity with no spatial information. The image is then constructed by using a simple linear operation between the bucket values and the total intensity recorded by the reference arm that calculates the total intensity of the speckle patterns alone (Zhang, et al., 2019). However, for encryption purposes, CGI encryption (CGIE) has serious limitations that the researchers are aiming to solve, such as the need for an enormous number of random patterns to encode and reconstruct the image. This will take a lot of time and consume high computational power. Another issue is the need for transmitting all the random patterns to the receiver side to reconstruct the image. To address these challenges, this work incorporates advanced techniques to improve the efficiency and security of CGIE. By leveraging the orthogonality and structured nature of the Hadamard matrix (HM) that generates unique and non-repetitive Hadamard basis patterns (HBPs) through its scrambling with chaotic maps, the need for transmitting large pattern sets is eliminated and the number of measurements required for image reconstruction is significantly reduced. Integer wavelet transform (IWT) ensures a lossless, integer-to-integer transformation, enabling faster encryption with XOR operations. I addition, the strong properties of the chaotic maps enhance both the security and efficiency of the system, ensuring improved resilience and optimized performance. The rest of this paper is organized as follows. The related works are described in Section 2. In Section 3, the theoretical background of the proposed system is introduced. In section 4, the proposed model framework is explained. Section 5 contains the quantitative measures used to evaluate the system. The simulation results and security analysis are performed in section 6, the conclusion is given in section 7.

II. Related Works

The CGI technique was first introduced by (Shapiro, 2008). In which the reference beam is computed offline using a computer instead of using a charged-coupled device. On the basis of this foundational work, (Clemente, et al., 2010) introduced a new approach in optical cryptography utilizing CGI for image encryption by using the random phase masks (RPMs) as a

ARO-The Scientific Journal of Koya University
Vol. XIII, No.1(2025), Article ID: ARO.12153. 12 pages
DOI: 10.14500/aro.12153
Received: 27 March 2025; Accepted: 22 May 2025
Regular research paper; Published: 05 June 2025
†Corresponding author's e-mail: kha23c1009@uoanbar.edu.iq

secret key. This approach paved the way for the researchers to enhance and develop CGI techniques for cryptography. However, the reconstruction quality is poor and the complexity of the system is high. To address these limitations, (Duran, 2011). introduced a new method by incorporating compressed sensing with CGI to reduce the complexity of the system while improving reconstruction quality. However, the system's linearity issue remains unresolved. To address this issue, (Chen and Chen, 2015) proposed an optical encryption technique by utilizing CGIE with labyrinth-like phase modulation patterns. The method employs a single phase-only mask (POMs), which optimizes storage and transmission efficiency of system keys while introducing highly randomness patterns. Similarly, in the same year, (Zhao, et al., 2015). incorporated CGIE with QR code improving image reconstruction quality and resisting cropping attack due to the high error tolerance in QR code. In a subsequent development, (Li, et al., 2016). developed a multiple image encryption scheme by using CGIE based on compressive ghost imaging leveraging the DCT domain and generating random patterns using a modified logistic map (LM) to reduce key transmission. Subsequently, (Yi, Leihong and Dawei, 2018). combined CGI with RSA algorithm to solve the problem with key distribution among the parties and add a high level of security to the system. In the same year, (Jiang, et al., 2017). Proposed a new approach using computational temporal ghost imaging to extend the concept to the time domain for encrypting temporal data in the time domain to improve the security and robustness against noise attack. Further enhancing security, (Zhu, et al., 2018). introduced a CGIE technique based on fingerprint phase mask to encrypt and decrypt the image using off-axis digital holography to add an additional layer of security besides the CGIE. Recently, (Guo, et al., 2024). proposed an optical image encryption and authentication scheme with CGI based on 4D chaotic system and DNA encoding using dual channels for encryption and authentication that alleviates the burden of key transmission need. In the same year, (Huang and Han, 2024). proposed CGIE technique using improved RSA algorithm and cake-cutting HM and discrete wavelet transform (DWT) to reduce the sampling times and eliminate RPMs transmission using a private channel. Building on previous advancements, (Miao, et al., 2025). proposed an image encryption and authentication scheme utilizing CGIE and lifting wavelet transform (LWT), employing the Knuth-Durstenfeld shuffling algorithm and chaotic maps. This approach ensures the enhancement of system's security and reduces the computational complexity of the wavelet transform due to the straightforward transformation of LWT.

However, most of these studies focused on performing CGIE on small-sized grayscale images to demonstrate the feasibility of CGIE. In this study, we have developed a low-complexity version that significantly reduces processing requirements. Our proposed system is designed to perform CGIE on a large-scale RGB image dataset with the aim of enabling the seamless adoption of this technology more widely within cryptographic frameworks. First, a two-level decomposition IWT is performed on the secret image. Second, a unique HM is generated and then scrambled using chaotic LM indices to eliminate POMs transmission needs. Then, HBPs are extracted from HM and projected on the LL sub-band to get the bucket signal. Firstly, a two-level decomposition IWT is performed on the secret image, generating four sub-bands: Low-Low (LL), High-Low (HL), Low-High (LH), and High-High (HH). LL serves as the approximation sub-band, preserving the most important structural details of the image, while the other sub-bands, known as detail sub-bands, capture edge and texture information. Finally, the other IWT sub-bands (HL, LH, HH) are shuffled with a piecewise linear chaotic map (PWLCM) then XORed with a second LM to achieve permutation-substitution. In addition, using another chaotic map to substitute the bucket signal to break the linearity of the system and improve the security. Simulation results show that our encryption system has a high level of security robustness against different attacks with perfect reconstruction quality compared to other methods.

III. Theoretical Background

A. CGIE

In the optical security field, instead of converting an image into a complex-valued matrix, CGI encrypts the image into correlated intensity values of the image and the HBPs, which makes CGI widely studied (Leihong, et al., 2018).

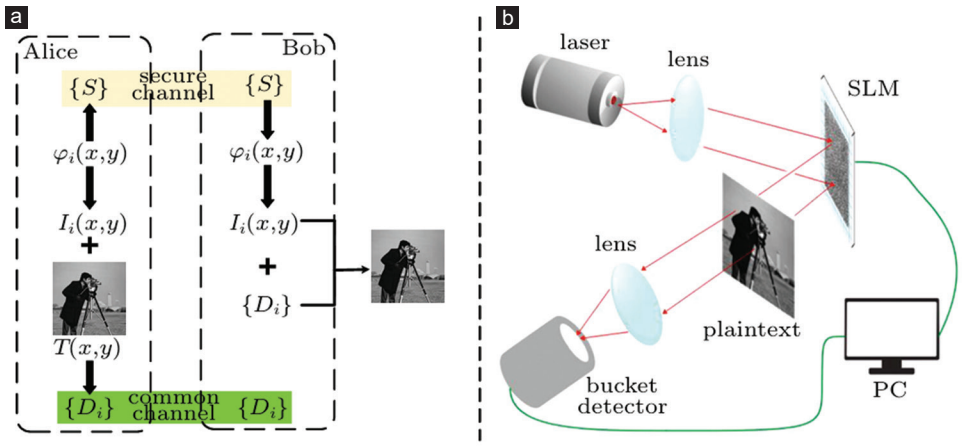

Fig. 1. (a). the block diagram of computational ghost imaging encryption encryption/decryption process, (b) The experimental setup of Computational Ghost Imaging (Kang, et al., 2021).

The structure of computational ghost imaging is very simple. As shown in Fig. 1a. Alice wants to encrypt the secret image $I(x, y)$ and transmit it to Bob using the public channel. Alice uses the CGI structure as shown in Fig. 1b. the specialized light source is passed through a lens to the spatial light modulator to regularly generate RPMs denotes $\emptyset(x, y)$ with values uniformly distributed between [0-2π] then project them onto an image $I(x, y)$ to record the total intensity with no spatial information. The resulting light intensity is directed by a lens to a bucket detector (B_i) using the equation as follows:

$$B_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \varnothing(x, y).I(x, y) \quad (1)$$

Then, Alice sends the (B_i) as a cipher image using the public channel and transmits all the RPMs using the secured channel to Bob to decrypt the image. On the receiving side, Bob uses a simple linear operation between the bucket values and the secret patterns to reconstruct the image (Tao, et al., 2020), by calculating the average sum of B_i denotes AVB, and the average sum of the RPMs denotes AVI, the image can be reconstructed by performing *image* = (*AVB* × *AVI*) – *AVI* × *AVB* to reconstruct the image $I(x, y)$. The equation is mathematically described as follows:

$$I(x, y) = \langle BI(x, y)\rangle - \langle B\rangle.\langle \emptyset(x, y)\rangle \quad (2)$$

Where ⟨•⟩ denotes the mean operation,
⟨*B*⟩ is the mean of the bucket values B_i,
⟨∅(*x*, *y*)⟩ is the mean of the RPMs,
BI(*x*, *y*) is the scalar product between B_i and ∅(*x*, *y*),
I(*x*, *y*) is the reconstructed image.

The CGIE can be implemented either with specialized hardware devices or through software simulation as we used in this paper.

B. HM and HBPs

Significant types of POMs are used in CGI, which is considered as a key to collect the measured intensities to encrypt and reconstruct the image in high quality. However, POMs with values between [0-2π] require a more complex representation (at least 8 bits per pixel), making the initialization more complex and the storage and transmission of these masks less efficient, which limits the adoption of CGI in practical applications (Liansheng, et al., 2019). In addition, because of the random nature of generating these masks, the redundancy is very high. To address these problems, an orthogonal HM with binary representation of values (+1, −1) is used to generate HBPs that serve as POMs (Zhang, et al., 2017). Because of the orthogonality of HM, the redundancy between these masks is decreased, which results in reconstructing the image with high quality by using fewer measurements (Wang and Zhao, 2016). In addition, HBPs are more efficient and require 8 times less storage than POMs for initialization due to their binary representation (1 bit per pixel). To encrypt an image with the size of (N, N) pixels, HM with order 2^k is constructed (Yu, 2019), where the condition ($N \times N = 2^k$) should be satisfied. The HM with 2nd-order is mathematically defined as:

$$H_{2^2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3)$$

Then, the HM with order 2^k can be calculated with the recursive formula is mathematically defined as:

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} \quad (4)$$

After obtaining the desired HM, 2^k HBPs can be extracted by rearranging each row into a 2D pattern with $N \times N$ pixels (Yu, et al., 2022). For example, as illustrated in Fig. 2. From our code, to encrypt and reconstruct an image with size (8, 8) pixels, 64 × 64 HM is generated to extract 64 HBPs with size (8, 8).

C. IWT

In cryptosystems, using traditional wavelet transform may result in distortion during the reconstruction, especially when using multilevel wavelet decomposition, resulting in quality degradation of the reconstructed image because the binary representation for the floating-point numbers is limited. Eventually, there will be energy loss during reconstruction. Even when representing the pixel values of the image in integer form, the coefficients obtained from the wavelet transform are not represented as an integer (Yunus, Firmansyah and Subiono, 2024). The significance of IWT provides an optimal solution. IWT is an integer-to-integer

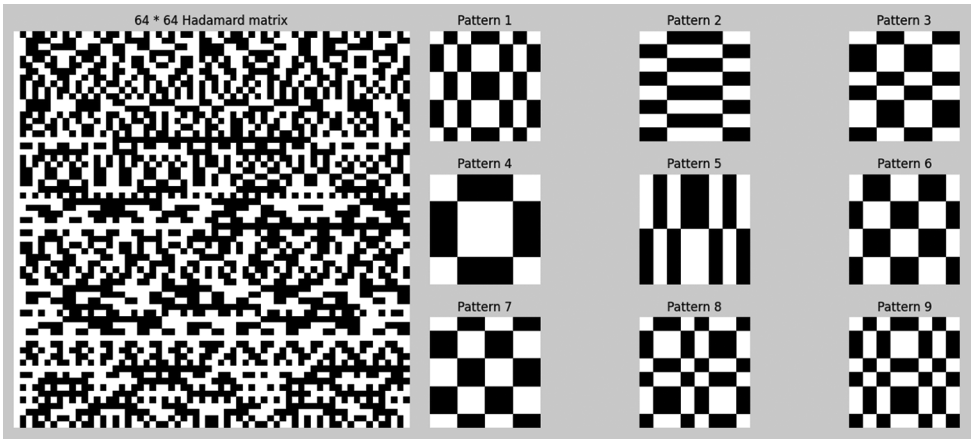

Fig. 2. Hadamard matrix and hadamard basis patterns generation and visualization from our code.

transformation, so there will be no degradation even after using multilevel decomposition.

IWT is implemented using a lifting scheme (LS) that replaces the convolution-based filter banks that used in the traditional wavelet transform, such as DWT with more computationally efficient and lossless transformation by performing simple operations (split, predict, update and merge), producing integer coefficients (Sweldens, 1996). In addition, IWT is preferable over DWT when performing XOR operation in cryptosystems because XOR only operates on integer values. DWT produces floating-point coefficients, requiring an additional step to convert them into integers, which increases computational time and may lead to precision loss, potentially reducing overall quality. By using IWT, this conversion is avoided, leading to more efficient processing and improved accuracy. In this paper, LS is performed on the Haar wavelet, and its implementation steps are detailed in the following section and illustrated in Fig. 3. On Haar wavelet, the implementation steps are outlined as follows:

Split the original image $A(i)$ into a disjoint two sequences based on odd and even indices as follows:

$$split(A(i)) = (even_i), (odd_i) \quad (5)$$

Then, the even sequence is used to predict the odd sequence that serves as high-pass filter to obtain detail signal $D(i)$ as follows:

$$D_{i+1} = odd_i - p[even_i] \quad (6)$$

Where $p[even_i]$ is the predicted value of odd_i based on $even_i$.

The idea is to find how much the original odd sequence differs from the even sequence.

Then, the detail signal $D(i)$ is used to update the even sequence that serves as low-pass filter to obtain the approximation signal $S(i)$ as follows:

$$S_{i+1} = even_i + u[odd_i] \quad (7)$$

For the inverse IWT, the $even_i$ can be obtained as follows:

$$even_i = S_{i+1} - u[D_{i+1}] \quad (8)$$

Then, odd_i can be recovered as follows:

$$odd_i = D_{i+1} - peven_i] \quad (9)$$

Finally, merge odd_i and $even_i$ to obtain A_i as follows:

$$A_i = merge\ (even_i, odd_i) \quad (10)$$

This scheme ensures lossless reconstruction with lowest calculation time and less memory taken by the system compared to the other wavelet schemes (Ananthi, et al., 2024).

D. Chaotic Maps

Chaotic maps are a field of study of mathematics where non-linear dynamic systems generate a set of random numbers that are absolutely disordered and appear irregular but are controlled by the initial seed conditions. It examines how minor variations in initial conditions can result in major different outcomes. This phenomenon is often called the "butterfly effect" (Shen, 2023).

The inherent nature of non-linear chaotic characteristics led to an increasing use of chaotic maps for image encryption, such as sensitivity to the initial conditions, pseudo-randomness, and non-periodicity (Zhang and Huo, 2019). These features motivated the researchers to propose a variety of chaotic maps with a particular focus on creating a strong random sequence for information encryption. There are two chaotic maps that we used in our system.

LM

The most popular one-dimensional chaotic LM was implemented in cryptography by (May, 1978) which led to its rise in popularity. The mathematical equation of the LM is as follows:

$$x_{n+1} = r * x_n * (1 - x_n) \quad (11)$$

The initial condition X_0 where ($X_0 \in [0, 1]$) and the control parameter r, where $0 < r \leq 4$ to control the chaotic phenomena. It has been proved by researchers that the LM exhibits the best chaotic dynamics behavior. When $r \geq 3.87$, the map becomes highly sensitive to initial conditions and exhibits strong randomness, producing non-repetitive and unpredictable sequences. For $r < 3.57$, the map enters a periodic window, and for $r > 3.57$ the system enters chaos, but there are three periodic windows within this chaotic regime as shown in Fig. 4.

The LM is an efficient, highly secured chaotic map with low computational complexity. Making it well-suited

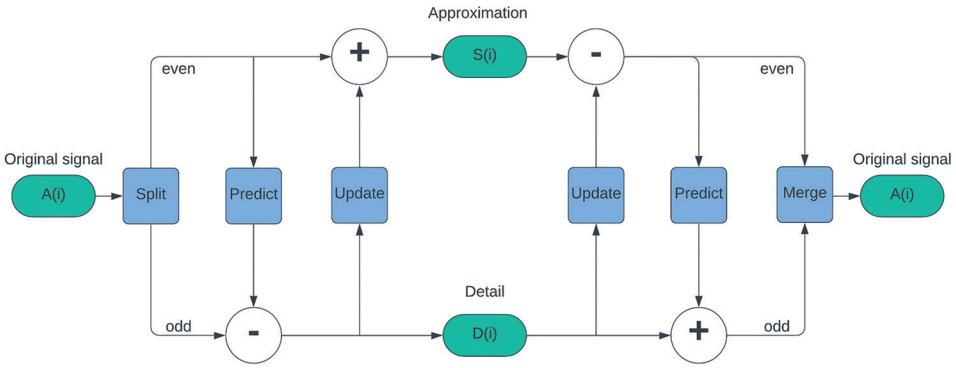

Fig. 3. The block diagram of lifting scheme.

for resource-constrained environments. The simplicity of this map ensures efficient processing without demanding significant computational resources (İnce, İnce and Hanbay, 2024).

PWLCM

PWLCM was first proposed by (Li, Chen and Mou, 2005). It is a map that is composed of multiple linear segments, allowing for a limited number of breakpoints (Wang and Chen, 2013). The mathematical equation of PWLCM is as follows:

$$G(x)=\begin{cases}\dfrac{x}{p}, & x\in[0,p]\\[2ex] \dfrac{1-x}{1-p}, & x\in[p,1]\end{cases} \tag{12}$$

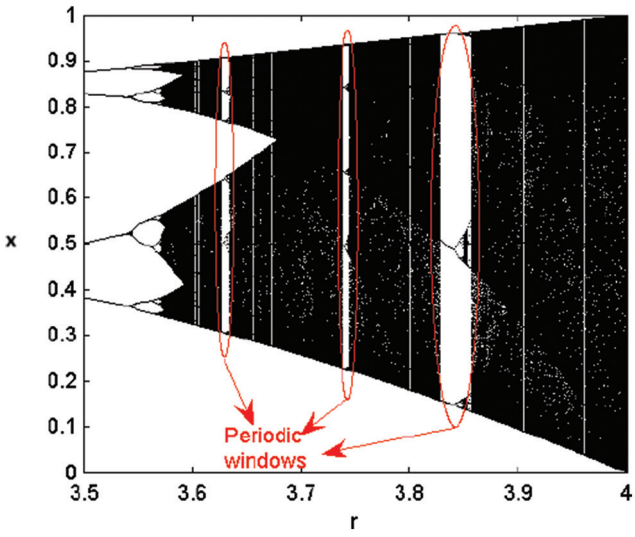

Fig. 4. The bifurcation diagram of the logistic map (Arroyo, et al., 2009).

Where p is the control parameter with values (0–1), X is the initial parameter with values (0–1).

PWLCM is linear but exhibits strong chaotic behavior with different initial conditions that make it sensitive to initial conditions, making it deterministic but unpredictable. In addition, it is simple in implementation and computationally lightweight, making it suitable for real-time applications (Chen, Tang and Yi, 2020).

IV. The Proposed Model

The proposed cryptosystem leverages the strength of advanced techniques to ensure robust and efficient encryption and decryption of large images. Optical CGI encryption technology based on wavelets and chaos theory is proposed. Below are the encryption and decryption processes as well as the algorithms used in the system.

A. Encryption Scheme

As shown in Fig. 5. The image channels are first separated, and then a two-level decomposition IWT is performed on the secret image to get the approximation sub-band (LL) and the detail sub-bands (HL, LH, HH). Second, HM with LL dimensions is generated. Subsequently, generate PWLCM sequence using LL dimensions. The indices of PWLCM sequence are used to shuffle HM. Then, taking each row of the shuffled HM and form it into a 2D array to extract HBPs and project them on the LL sub-band to get the bucket values. The bucket values are then substituted using XOR operation with the generated LM sequence. The other detail sub-bands are first substituted with a second LM then scrambled using a second PWLCM. The new two matrices are appended to form the final cipher image.

This process is repeated 3 times to encrypt image channels with different initial parameters to reach a high level of security.

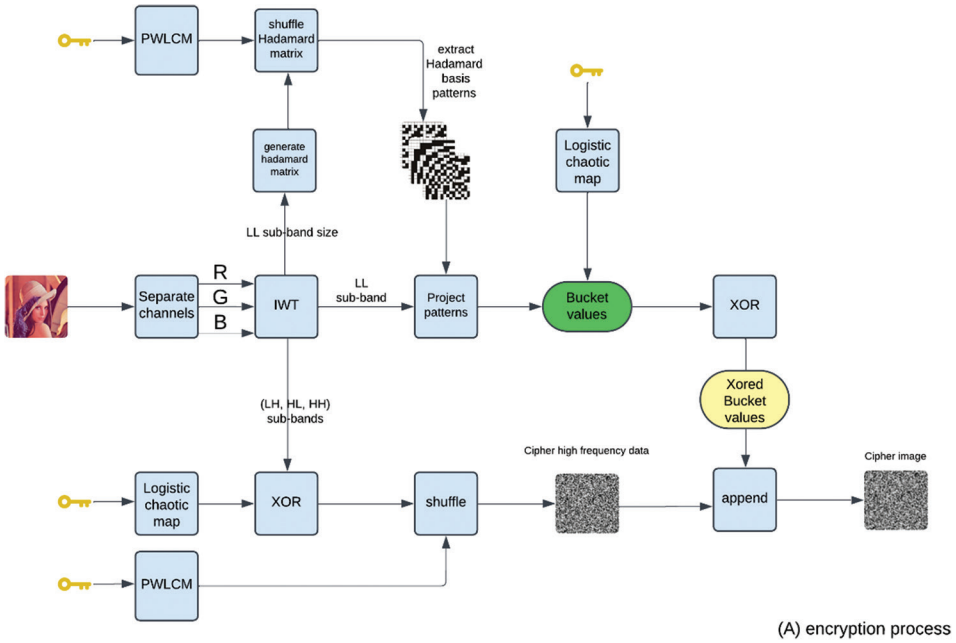

Fig. 5. The block diagram for the encryption process of the proposed system.

http://dx.doi.org/10.14500/aro.12153

Channel-wise processing is performed to avoid predictable patterns across channels and minimizing ciphertext correlation.
Algorithm 1: Encryption process

Input: original image (A), parameters of chaotic maps as a seed of the key such as(p_0=0.51, r_1= 3.991, r_2=3.992, x_{0r}=0.565, x_{0g}=0.566, x_{0b}=0.567).
Output: Cipher image(C).
Steps:
1. Read input image (A).
2. Separate (R, G, B) channels.
3. For each channel in (R, G, B):
   A. Perform $S = IWT(A)$.
   B. Separate Low frequency coefficients (LL) and the other coefficients (HL, LH, HH) as (OC).
   C. Generate HM as a measurement matrix (H).
   D. Generate chaotic map (C1) using PWLCM with (p_0, x_0) initial parameters.
   E. Scramble H using C1 indices to generate H_{new}.
   F. Extract HBPs from H_{new} by taking each row and convert it to 2D matrix.
   G. Project HBPs on (LL) to get the bucket values (B_i) for each channel as follows: $B[i] = HBP[i] \times LL$.
   H. Generate chaotic map (C2) using logistic chaotic map with (r_1, x_0) initial parameters.
   I. Perform bitwise XOR on the (OC) using C2 as follows $sub(OC) = OC \wedge C2$.
   J. Generate chaotic map (C3) using PWLCM with (p_0, x_0) initial parameters.
   K. Shuffle the substituted OC with C3 to get $SH(OC)$.
   L. Generate chaotic map (C4) using logistic map with (r_2, x_0) initial parameters.
   M. Perform bitwise XOR on bucket values $S(B_i) = B_i \wedge C4$.
   N. Append $S(B_i)$ and $SH(OC)$ to get the cipher image (C).
4. Append cipher image (C) for (R, G, B) channels.
5. Transmit C to the receiving side.

B. Decryption Scheme

The process of retrieving the secret image begins by separating the cipher image into two parts, as illustrated in Fig. 6. The cipher image is separated into two parts. The top left part is XORed with the LM using the same shared parameters as a secret key to get the bucket values. Then, perform the CGIE scheme on the result to retrieve the LL sub-band. The detail sub-bands are retrieved using the same parameters of LM and PWLCM on the remaining information of the cipher image. Finally, appending the results and performing inverse IWT to get the secret image.
Algorithm 2: Decryption process

Input: cipher image (C), parameters of chaotic maps as a seed of the key such as (p_0=0.51, r_1= 3.991, r_2=3.992, x_{0r}=0.565, x_{0g}=0.566, x_{0b}=0.567).
Output: Original image(A).
Steps:
1. Read cipher image (C).
2. Separate $S(B_i)$ and $SH(OC)$. .
3. Separate (R, G, B) channels.
4. For each channel in (R, G, B):
   A. Generate chaotic map (C1) using logistic map with (r_2, x_0) initial parameters.
   B. Perform bitwise XOR to get the bucket values $B_i = S(B_i) \wedge C1$.
   C. Generate chaotic map (C2) using PWLCM with (p_0, x_0) initial parameters.
   D. Scramble H using C2 indices to generate H_{new}.
   E. Extract HBPs from H_{new} by taking each row and convert it to 2D matrix.
   F. Perform a simple linear operation on B_i using HBPs to get the low frequency coefficients (LL).
   G. Generate chaotic map (C3) using PWLCM with (p_0, x_0) initial parameters.
   H. Reshuffle $SH(OC)$ to get $sub(OC)$ as follows: $sub(OC) = SH(OC) \wedge C3$.
   I. Generate chaotic map (C4) using logistic chaotic map with (r_1, x_0) initial parameters.
   J. Perform bitwise XOR on the $sub(OC)$ to get the other coefficients *OC* as follows: $OC = sub(OC) \wedge C4$
   K. Append LL and OC to get the original signal (S).
   L. Perform $A = IIWT(S)$.
5. Merge (R, G, B) channels to get the original image (A).

V. Quantitative Measures

A. Correlation Coefficient

Correlation coefficient is a statistical measure with values between (−1 and 1), it is used to assess how strongly and in what direction the two variables are linearly related. In security, it used to measure the similarity between the contents of the images to determine how much the the encrypted image or the reconstructed image differs from the original image (Elashry, et al., 2009), 1 indicates a perfect correlation (identical images) in the same direction, zero indicates no correlation and no linear relationship between the original image and the encrypted or reconstructed image, and −1 indicates a perfect negative correlation (different images) in opposite directions.

The correlation coefficient for two different images can be calculated using the following equation:

$$C = \frac{(\sum_{i=1}^{n}((Xi - uXi) \times (Yi - uYi)}{\sqrt{\sum_{i=1}^{n}(Xi - uXi)^2} \times \sqrt{\sum_{i=1}^{n}(Yi - uYi)^2}} \quad (13)$$

Where C is the correlation coefficient value, the two images variables are (X, Y), μ is the mean of X and Y.

B. Mean Square Error (MSE)

In cryptography, MSE is a measurement used to evaluate the quality of the encryption algorithm by calculating the average squared difference between the original image and the reconstructed image to determine how much information is lost or altered during the encryption and reconstruction

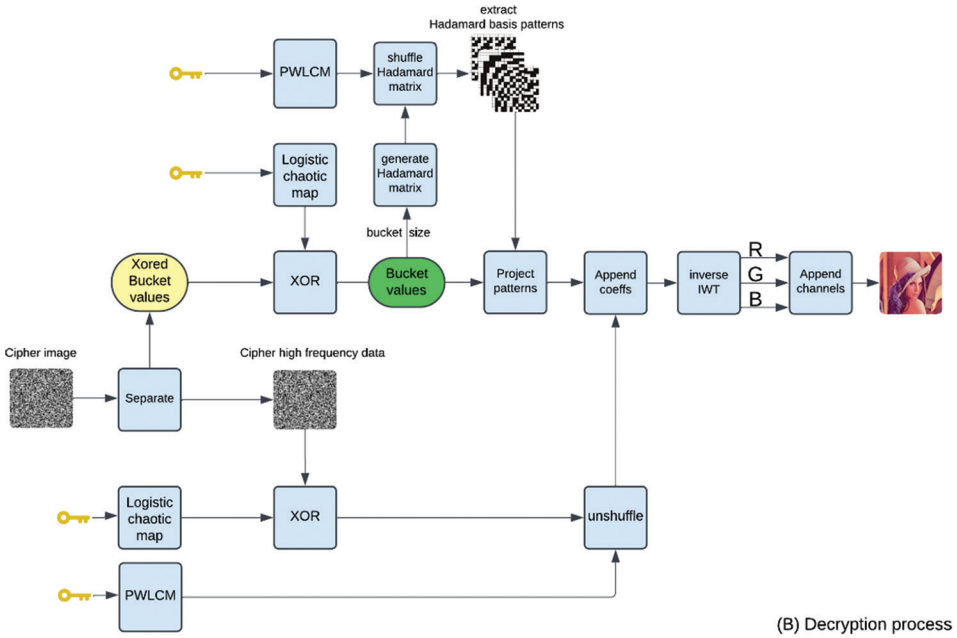

Fig. 6. The block diagram of the decryption process of the proposed system.

processes (Alghamdi, Munir and Ahmad, 2022). Lower MSE indicates better reconstruction.

The equation of MSE is as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(O_i - R_i)^2 \quad (14)$$

Where (o_i) is the original image, (R_i) is the reconstructed image, (n) is the number of pixels in an image.

C. Peak Signal-to-Noise Ratio (PSNR)

In cryptography, PSNR is a widely used measurement that is used to evaluate the quality of the reconstructed image compared with the original image by measuring the ratio between the maximum possible pixel value (peak signal) and the unwanted noise that appeared in the reconstructed image (MSE).

The equation of PSNR is as follows:

$$\text{PSNR} = 20.\log_{10}(\max_i) - 10.\log_{10}(MSE) \quad (15)$$

Where (Max_i) is the maximum possible pixel value of the image.

A higher PSNR value indicates better reconstruction and lower noise in the reconstructed image (Mali, Chakraborty and Roy, 2015).

D. Number of Changing Pixel Rate (NPCR)

NPCR is a measurement especially used in image encryption to evaluate the diffusion strength in the algorithm by measuring the percentage of changing pixels between two encrypted images by changing only 1 bit in the secret key (Chowdhary, et al., 2020). A higher NPCR value indicates better diffusion.

By creating a new empty matrix D(i, j) that has the same dimensions as the encrypted image. The result matrix is as follows:

$$D(i,\ j) = \begin{cases} 0 & C1(i,\ j) = C2(i,\ j) \\ 1 & C1(i,\ j) \neq C2(i,\ j) \end{cases} \quad (16)$$

Then, using the new matrix D(i, j) to calculate NPCR as follows:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}D(i,\ j)}{n \times m} \times 100\% \quad (17)$$

Where C1 is the first encrypted image, C2 is the second encrypted image, and (m, n) are the dimensions of the encrypted images.

The best NPCR value is typically >99.50%, meaning that almost all pixels in C1 differ from C2 (Saidi, et al., 2020).

E. Unified Averaged Changing Intensity (UACI)

UACI is a measurement especially used in image encryption to calculate the average intensities modified between two encrypted images by changing only 1 bit in the secret key. It gives insight about the strength of the algorithm (Khanzadi, Eshghi and Borujeni, 2014).

The UACI between two encrypted images can be calculated as follows:

$$UACI = \frac{1}{m \times n}\left[\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(C1(i,\ j) - C2(i,j))}{255}\right] \times 100\% \quad (18)$$

Where C1 is the first encrypted image, C2 is the second encrypted image, and (m, n) are the dimensions of the two encrypted images.

F. Entropy Analysis

In cryptography, entropy analysis is used to measure the randomness or unpredictability in the encrypted image. Higher entropy indicates a highly random distribution of

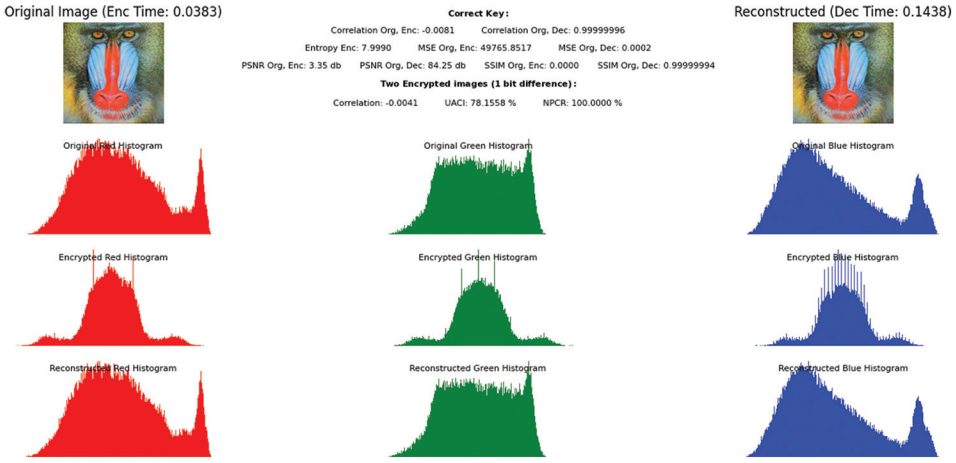

Fig. 7. Output visualization with correct keys.

image pixels. This indicates better complexity and high security in the encryption system. While lower entropy indicates that the pixel values of the encrypted image are less random and contain predictable patterns (Dick, 2014).

The equation for calculating Entropy is as follows:

$$H(x) = -\sum_{i=1}^{N} p(x_i) log_2 p(x_i) \quad (19)$$

Where H(x) is the summation of the entropy of all discrete random variables (x_i), $p(x_i)$ is the existence probability of the randomness in (x_i).

The negative sign before summation is to ensure that the entropy value is non-negative (Ye, Zhou and Gong, 2020).

G. Structural Similarity Index Measure (SSIM)

In cryptography, SSIM is used to measure how far the cipher image is deviated from the original image according to the structural properties. By measuring the luminance, contrast, and structural properties changes (Yuan, et al., 2019). SSIM values fall within the ranges of (−1, 1), where 1 indicates perfect similarity. 0 indicates no similarity. The formula of SSIM is as follows:

$$L(o, e) = \frac{2\mu_a\mu_c + C1}{\mu_a^2 + \mu_c^2 + C1} \quad (20)$$

$$C(o, e) = \frac{2\sigma_a\sigma_c + C2}{\sigma_a^2 + \sigma_c^2 + C2} \quad (21)$$

$$S(o, e) = \frac{\sigma_{ac} + C3}{\sigma_a\sigma_c + C3} \quad (22)$$

Where O is the original image, C is the encrypted image, μ_a and μ_c are the means of the original and encrypted images, σ_a and σ_c are the standard deviation of the original and encrypted images, σ_{ac} is the covariance of the original and encrypted images, and c1, c2, and c3 are constants used to avoid the multiplication by zero where $C1 = (K1.R1)^2$, $C2 = (K2.R1)^2$ and $C3 = K2/2$.

K1 and K2 are small variables, and R1 is the dynamic range of pixel values.

TABLE I
IMAGE DATASET

Image name	Color	Type	Dimensions
Lena	Color	tiff	512×512
Baboon	Color	tiff	512×512
Peppers	Color	tiff	512×512
Jellybeans	Color	tiff	256×256
Female	Color	tiff	256×256
Airplane	Color	tiff	512×512
Couple	Color	tiff	256×256
Female 2	Color	tiff	256×256
House	Color	tiff	256×256
House 2	Color	tiff	512×512
Sailboat	Color	tiff	512×512
Tree	Color	tiff	256×256

Finally, the SSIM can be calculated as follows:

$$SSIM = L(a, c).C(a, c).S(a, c) \quad (22)$$

VI. EXPERIMENTAL RESULTS AND ANALYSIS

To verify the feasibility and security of our encryption system, numerical experiments were carried out on this method. The proposed image encryption technique was implemented with a visual studio code environment using Python. The computer CPU was an AMD Ryzen 7 4700U, 16 GB RAM, Win 11 64-bit. A sample of output visualization of our code, as shown in Fig. 7. Contains all the measures used and the histogram analysis for the original, encrypted, and reconstructed images. The selected image dataset from the USC-SIPI Image Database is shown in Table I.

A. Security Analysis

The above-mentioned measures are used to evaluate the security and reconstruction quality of our system. To evaluate the security strength of the system, the test results as shown in Table II demonstrate that the key sensitivity of the system is very high, with only 1-bit difference between encryption keys resulting in two different cipher images with <0.006 correlation. To further validate these results, Table III provides a 95%

confidence interval analysis after performing 10 independent runs with different initial parameters for each tested image. Fig. 8. shows the output visualization using the wrong key (only 1 bit difference). To evaluate the reconstruction quality of the system, the test results presented in Table IV demonstrate that the system achieves perfect image reconstruction, indicating that it operates in a lossless manner. In addition, the XOR implementation with chaotic maps is completely reversible when the exact same parameters are used by both parties, ensuring that the original data can be accurately retrieved. This reversibility guarantees the integrity of the cryptosystem.

B. Key Space Analysis

Here we take a (256, 256) image as an example. With our system, we used a chaotic PWLCM with initial parameters (x, p). These parameters are securely exchanged between

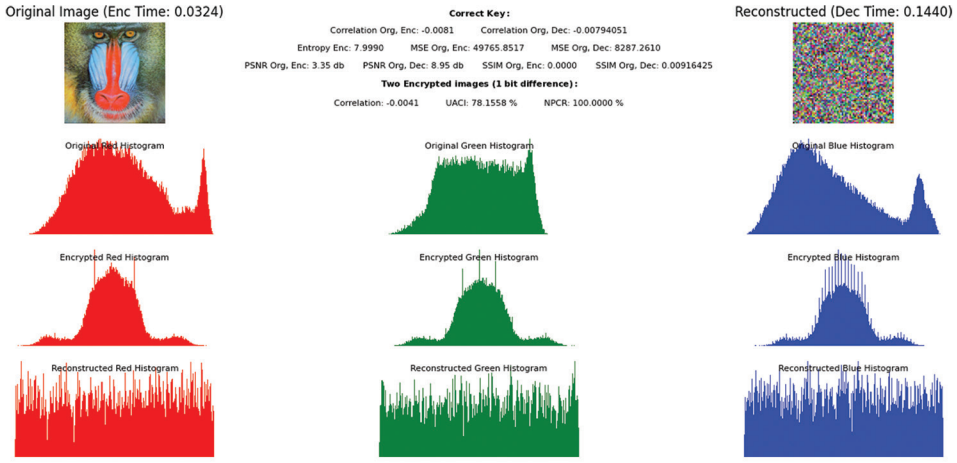

Fig. 8. Output visualization with wrong keys.

TABLE II
SECURITY TEST RESULTS

Images	Entropy Enc	CC Org, Enc	CC Enc1, Enc2	MSE Org, Enc	PSNR Org, Enc	SSIM Org, Enc	UACI Enc1, Enc2	NPCR Enc1, Enc2 (%)
Lena	7.9989	0.0013	0.0039	49175	5.43 DB	−0.000002	76.9823	100
Baboon	7.9990	−0.0081	−0.0041	49765	3.35 DB	0.000001	78.1558	100
Female	7.9988	0.0016	0.0063	35265	7.95 DB	0.000003	77.6543	100
Jellybeans	7.9983	0.0011	0.0014	39771	6.76 DB	−0.000001	78.2313	100
Peppers	7.9990	0.0008	−0.0001	41431	3.54 DB	0.000001	79.1012	100
Airplane	7.9997	0.0068	0.0001	35210	4.53 DB	−0.000001	59.4187	100
Couple	7.9989	0.0073	0.0011	35211	7.41 DB	0.000003	68.3211	100
Female2	7.9991	0.0006	0.0023	47561	3.31 DB	0.000001	78.6661	100
House	7.9984	0.0021	0.0084	31231	6.59 DB	−0.000002	73.5832	100
House2	7.9991	0.0009	−0.0011	38574	4.32 DB	0.000001	77.4390	100
Sailboat	7.9990	0.0003	0.0041	41854	5.21 DB	−0.000001	73.5832	100
Tree	7.9993	−0.0004	0.0012	47571	3.47 DB	0.000001	79.1211	100

TABLE III
RESULTS WITH A 95% CONFIDENCE INTERVAL FOR THE TESTED IMAGES WITH DIFFERENT INITIAL PARAMETERS

Images	Entropy Enc	CC Org, Enc	CC Enc1, Enc2	MSE Org, Enc	PSNR Org, Enc	SSIM Org, Enc	UACI Enc1, Enc2	NPCR Enc1, Enc2 (%)
Lena	±0.0005	±0.00075	±0.00131	±1384	±0.11	±0	±1.34	±0
Baboon	±0.0007	±0.00029	±0.00117	±1628	±0.09	±0	±1.11	±0
Female	±0.0011	±0.00092	±0.00311	±956	±0.33	±0	±2.04	±0
Jellybeans	±0.0006	±0.00106	±0.00152	±889	±0.13	±0	±2.87	±0
Peppers	±0.002	±0.00126	±0.00084	±1053	±0.21	±0	±3.25	±0
Airplane	±0.0009	±0.00191	±0.00114	±759	±0.12	±0	±2.01	±0
Couple	±0.0005	±0.00073	±0.00135	±931	±0.19	±0	±1.71	±0
Female2	±0.0009	±0.00095	±0.00127	±1355	±0.05	±0	±3.01	±0
House	±0.0005	±0.00115	±0.00232	±1249	±0.01	±0	±1.14	±0
House2	±0.002	±0.00109	±0.00301	±958	±0.29	±0	±1.31	±0
Sailboat	±0.001	±0.0007	±0.0023	±1633	±0.05	±0	±1.34	±0
Tree	±0.0009	±0.0011	±0.0008	±1282	0.19	±0	±1.29	±0

http://dx.doi.org/10.14500/aro.12153

communicating parties using public key cryptography, ensuring robust security against unauthorized access. Then, the chaotic sequence generated is used to scramble the HM rows to generate a unique HM. For an image with a size of (256, 256) pixels, the LL sub-band extracted after performing two-level decomposition IWT is (64, 64) pixels. Since HM size should be equal to the power of rows and columns for the LL sub-band, this will need to generate HM with size =(2^{64}, 2^{64}) = (4096, 4096). Suppose that the attacker attempts to directly manipulate the HM by rearranging its rows and trying to reach the correct sorting of the HM to obtain all the HBPs using brute-force cracking. The probability is (2^{4096}) to obtain only the LL sub-band. This will take an enormous amount of time due to the complexity and size of the matrix. The vast number of possible rearrangements makes it extremely time-consuming for an attacker to identify any hidden patterns through brute force methods. However, the attacker may seek alternative strategies to bypass direct guessing on HM by attempting to extract the initial parameters of PWLCM. Since each parameter is encoded with 64-bit precision, the probability of obtaining the parameters (x, p) is 2^{128}. In addition, this is only one layer of the system. The attacker still needs to break the substitution layer with a probability of 2^{128} for the parameter (x, u) of the chaotic LM to get only the LL sub-band of the secret image. The other coefficients are also encoded with two chaotic maps that need to be extracted with probability of 2^{128} for each map.

TABLE IV
RECONSTRUCTION QUALITY TEST RESULTS

Images	Correlation Org, Dec	MSE Org, Dec	PSNR Org, Dec	SSIM Org, Dec
Lena	0.99999997	0.0002	84.79 DB	0.99999995
Baboon	0.99999996	0.0002	84.25 DB	0.99999994
Female	0.99999995	0.0003	83.94 DB	0.99999994
Jellybeans	0.99999999	0.0001	85.15 DB	0.99999997
Peppers	0.99999992	0.0004	82.11 DB	0.99999991
Airplane	0.99999994	0.0002	83.21 DB	0.99999995
Couple	0.99999995	0.0002	84.76 DB	0.99999996
Female 2	0.99999992	0.0004	81.32 DB	0.99999993
House	0.99999996	0.0001	84.98 DB	0.99999996
House 2	0.99999998	0.0001	84.79 DB	0.99999998
Sailboat	0.99999994	0.0002	82.56 DB	0.99999995
Tree	0.99999996	0.0002	84.35 DB	0.99999995

MSE: Mean square error, PSNR: Peak signal-to-noise ratio, SSIM: Structural similarity index measure

C. System's Linearity Analysis

In CGIE, ensuring the system's security against unauthorized parties is important. Even if they manage to obtain partial information of the secret key, also called the Eavesdropping Ratio (ER). To test the linearity of the system, we conducted another experimental approach by removing the substitution layer to validate the impact of this layer within our system. As shown in (Fig. 9a), if the

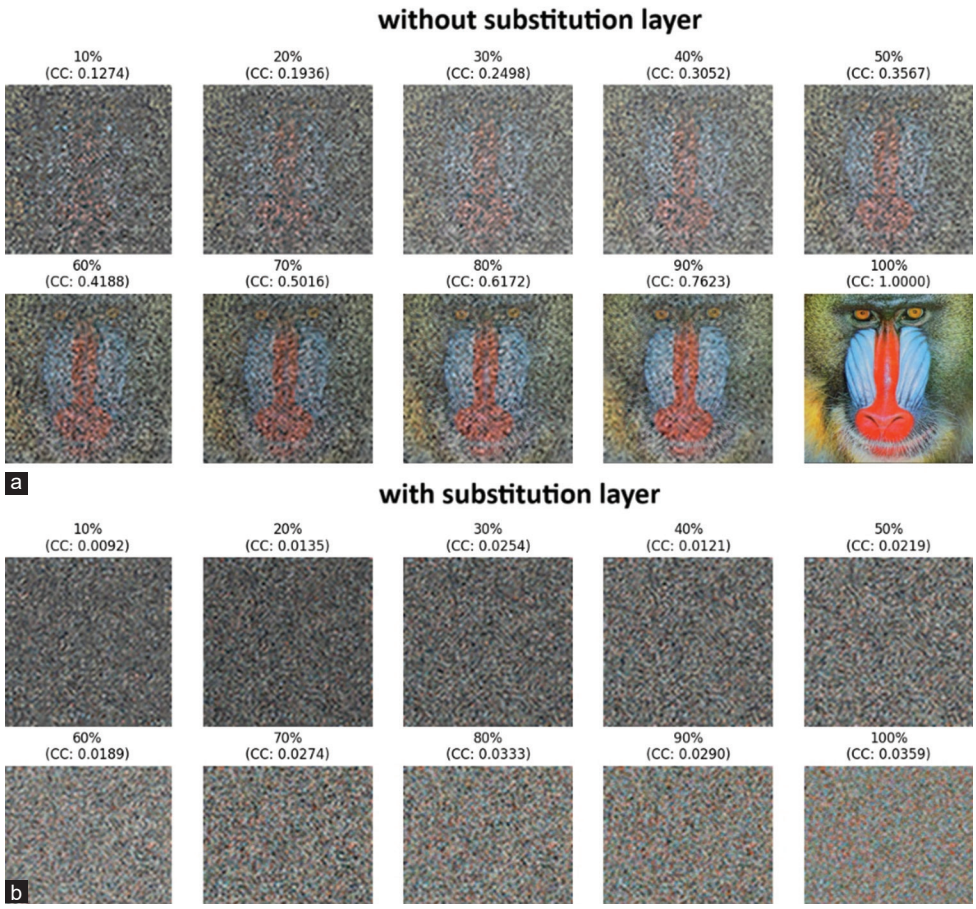

Fig. 9. Percentage of correct Hadamard basis patterns obtained by the eavesdropper. (a) Without the substitution layer, (b). With the implementation of the substitution layer.

attacker was able to get a percentage of HBPs randomly and wishes to decrypt only the LL sub-band. With ER = 30%, the secret image still appears distorted, with a correlation coefficient of 0.2498. The reconstructed image information remains incomplete. With ER = 50%, the image will become more recognizable with a correlation coefficient of 0.3567, and the hacker starts to recognize a small amount of image information, demonstrating improved approximation.

ER has further been promoted to 55%, 80% in (Chen and Chen, 2015; Zhao, et al., 2015) by Chen and Zhao, respectively. The problem still exists. Earlier, in the study by Huang and Han, a comparison was conducted between their method, which utilizes Cake-Cutting HM, and other transforms, such as DCT and HM. Notably, at ER = 60, the image information begins to be visible (Huang and Han, 2024). In contrast, as shown in (Fig. 9b), our proposed system ensures no information is obtained. Even with ER = 100%, the correlation coefficient is only 0.0359 due to the implementation of the second security layer (substitution layer).

VII. Conclusion and Future Recommendations

In this paper, we designed a new hybrid CGIE scheme to enhance encryption efficiency while significantly reducing computational complexity. By leveraging the orthogonality of Hadamard matrices, the limitation requiring the transmission of all the patterns is eliminated, and the number of measurements used for both encryption and reconstruction is minimized due to the non-repetitive HBPs. In addition, IWT preserves an integer-to-integer mapping, allowing lossless transformation and enabling more efficient encryption. Since XOR operations are inherently faster when applied to integer values, this approach significantly reduces computational overhead compared to methods that require floating-point conversions, making the encryption process both quicker and more efficient. Our approach strategically achieves a balance between security strength and low computational complexity while preserving the robust encryption strength of CGIE. The optimized framework not only improves computational feasibility but also enhances the adaptability of CGIE within cryptosystems, paving the way for broader adoption in encryption applications where efficiency and resilience are critical. However, the presented algorithm lies in the use of HM, which requires the input dimensions to be power of two (e.g., 64, 128, 256, etc.). Consequently, if the LL sub-band obtained from two-level IWT does not meet this criterion, the encryption process cannot be directly applied without resizing or padding.

Future recommendations include exploring a new alternative transform that supports arbitrary-sized dimensions, such as another orthogonal transform or custom-sized Hadamard-like matrices. In addition, replacing chaotic maps with a stochastic approach may enhance security while improving computational efficiency, offering a more secure and flexible framework.

REFERENCES

Alghamdi, Y., Munir, A., and Ahmad, J., 2022. A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy,* 24(10), p. 1344.

Ananthi, A., Subathra, M.S., Thomas George, S., and Sairamya, N.J., 2024. Entropy-based feature extraction for classification of EEG signal using lifting wavelet transform. *Przeglad Elektrotechniczny*, 9, pp. 146-150.

Arroyo, D., Alvarez, G., Li, S.J., Li, C.Q., and Fernandez, V., 2009. Cryptanalysis of a new chaotic cryptosystem based on ergodicity. *International Journal of Modern Physics B*, 23, pp. 651-659.

Chen, W., and Chen, X., 2015. Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption. *Europhysics Letters*, 109(1), p. 14001.

Chen, Y., Tang, C., and Yi, Z., 2020. A novel image encryption scheme based on PWLCM and standard map. *Complexity*, 23, p. 3026972.

Chowdhary, C.L., Virenbhai Patel, P., Kathrotia, K.J., Attique, M., Perumal, K., and Ijaz, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. *Sensors,* 20(18), p. 5162.

Clemente, P., Durán, V., Torres-Company, V., Tajahuerce, E., and Lancis, J., 2010. Optical encryption based on computational ghost imaging. *Optics Letters,* 35, pp. 2391-2393.

Dick, B., 2014. Inverting ion images without Abel inversion: Maximum entropy reconstruction of velocity maps. *Physical Chemistry Chemical Physics*, 16(2), pp. 570-580.

Duran, V., 2011. Optical encryption with compressive ghost imaging. In: *The European Conference on Lasers and Electro-Optics*. Optica, United States, p. CH3-4.

Elashry, I.F., Farag Allah, O.S., Abbas, A.M., El-Rabaie, S., and Abd El-Samie, F.E., 2009. Homomorphic image encryption. *Journal of Electronic Imaging*, 18(3), p. 033002.

Guo, Z., Chen, S.H., Zhou, L., and Gong, L.H., 2024. Optical image encryption and authentication scheme with computational ghost imaging. *Applied Mathematical Modelling*, 131, pp. 49-66.

Huang, H., and Han, Z., 2024. Computational ghost imaging encryption using RSA algorithm and discrete wavelet transform. *Results in Physics*, 56, p. 107282.

İnce, C., İnce, K., and Hanbay, D., 2024. Novel image pixel scrambling technique for efficient color image encryption in resource-constrained iot devices. *Multimedia Tools and Applications*, 83(29), pp. 72789-72817.

Jiang, S., Wang, Y., Long, T., Meng, X., Yang, X., Shu, R., and Sun, B., 2017. Information security scheme based on computational temporal ghost imaging. *Scientific Reports*, 7(1), p. 7676.

Yi, K., Leihong, Z., Dawei, Z., 2018. Optical encryption based on ghost imaging and public key cryptography. *Optics and Lasers in Engineering*, 111, pp. 58-64.

Kang, Y., Zhang, L., Ye, H., Zhang, D., and Zhuang, S., 2021. Ghost imaging-based optical cryptosystem for multiple images using integral property of the Fourier transform. *Chinese Physics B*, 30(12), p. 124207.

Khanzadi, H., Eshghi, M., and Borujeni, S.E., 2014. Image encryption using random bit sequence based on chaotic maps. *Arabian Journal for Science and Engineering*, 39(2), pp. 1039-1047.

Leihong, Z., Xiao, Y., Dawei, Z., and Jian, C., 2018. Research on multiple-image encryption scheme based on Fourier transform and ghost imaging algorithm. *Current Optics and Photonics*, 2(4), pp. 315-323.

Li, S., Chen, G., and Mou, X., 2005. On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos*, 15(10), pp. 3119-3151.

Li, X., Meng, X.F., Yang, X., Yin, Y., Wang, Y., Peng, X., He, W., Dong, G., and Chen, H., 2016. Multiple-image encryption based on compressive ghost imaging

and coordinate sampling. *IEEE Photonics Journal*, 8(4), pp. 1-1.

Liansheng, S., Cong, D., Minjie, X., Ailing, T., and Anand, A., 2019. Information encryption based on the customized data container under the framework of computational ghost imaging. *Optics Express*, 27(12), pp. 16493-16506.

Liu, J., Wang, L., and Zhao, S., 2022. Secret sharing scheme based on spread spectrum ghost imaging. *Applied Optics*, 61(24), pp. 7102-7107.

Mali, K., Chakraborty, S., and Roy, M., 2015. A study on statistical analysis and security evaluation parameters in image encryption. *International Journal of Scientific and Engineering Research,* 3, pp. 339-343.

May, R.M., 1978. *Exploiting Natural Populations in an Uncertain World*. Elsevier, North Holland.

Miao, M.K., Gong, L.H., Zhang, Y.J., and Zhou, N.R., 2025. Image encryption and authentication scheme based on computational ghost imaging and lifting wavelet transform. *Optics and Lasers in Engineering*, 184, p. 108560.

Saidi, R., Cherrid, N., Bentahar, T., Mayache, H., and Bentahar, A., 2020. Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted insar interferogram. *Ingenierie des Systemes d'Information*, 25(5), pp. 601-607.

Shapiro, J.H., 2008. Computational ghost imaging. *Physical Review Atomic*, 78(6), p. 061802.

Shen, B.W., 2023. *Attractor Coexistence, Butterfly Effects, and Chaos (ABC): A Review of Lorenz and Generalized Lorenz Models (published) Attractor Coexistence, Butterfly Effects, and Chaos (ABC): A Review of Lorenz's Models from 1960 to 2008*.

Sweldens, W., 1996. The lifting scheme: A custom-design construction of biorthogonal wavelets. *Applied and Computational Harmonic Analysis*, 3, pp. 186-200.

Tao, Y., Yang, X., Meng, X.F., Wang, Y., Yin, Y., and Dong, G., 2020. Plaintext-related multiple-image encryption based on computational ghost imaging. *Journal of Modern Optics*, 67(5), pp. 394-404.

Wang, L., and Zhao, S., 2016. Fast reconstructed and high-quality ghost imaging with fast Walsh-Hadamard transform. *Photonics Research*, 4(6), p. 240.

Wang, X., and Chen, D., 2013. A parallel encryption algorithm based on piecewise linear chaotic map. *Mathematical Problems in Engineering*, 2013, p. 537934.

Ye, H.S., Zhou, N.R., and Gong, L.H., 2020. Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. *Signal Processing*, 175, p. 107652.

Yu, W.K., 2019. Super sub-nyquist single-pixel imaging by means of cake-cutting hadamard basis sort. *Sensors (Switzerland)*, 19(19), p. 4122.

Yu, W.K., Cao, C., Yang, Y., Wei, N., Wang, S.F., and Zhu, C.X., 2022. Single-pixel imaging based on weight sort of the Hadamard basis. *Image and Video Processing*, 2203, p. 04659.

Yuan, X., Zhang, L., Chen, J., Wang, K., and Zhang, D., 2019. Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing. *Applied Physics B*, 125(9), p. 174.

Yunus, M., Firmansyah, M.I.D., and Subiono., 2024. A cryptography using lifting scheme integer wavelet transform over min-max-plus algebra. *Kybernetika*, 60(5), pp. 576-602.

Zhang, J., and Huo, D., 2019. Image encryption algorithm based on quantum chaotic map and DNA coding. *Multimedia Tools and Applications*, 78, pp. 15605-15621.

Zhang, L., Wang, Y., and Zhang, D., 2022. Research on multiple-image encryption mechanism based on Radon transform and ghost imaging. *Optics Communications*, 504, p. 127494.

Zhang, L., Yuan, X., Wang, K., and Zhang, D., 2019. Multiple-image encryption mechanism based on ghost imaging and public key cryptography. *IEEE Photonics Journal*, 11(4), pp. 1-14.

Zhang, Z., Wang, X., Zheng, G., and Zhong, J., 2017. Hadamard single-pixel imaging versus Fourier single-pixel imaging. *Optics Express*, 25(16), pp. 19619-19639.

Zhao, S., Wang, L., Liang, W., Cheng, W.W., and Gong, L., 2015. High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique. *Optics Communications*, 353, pp. 90-95.

Zhu, J., Yang, X., Meng, X., Wang, Y., Yin, Y., Sun, X., and Dong, G., 2018. Computational ghost imaging encryption based on fingerprint phase mask. *Optics Communications*, 420, pp. 34-39.