Hybrid Asymmetric Cryptography and Modified Cosine Wavelet Transform-Based Steganography Using Convolutional Autoencoder for Secure Data Sharing

R. Padma
Department of Computer Science, GITAM School of Technology, GITAM University, Bengaluru, India
pramacha@gitam.in (corresponding author)

Vamsidhar Yendapalli
Department of Computer Science, GITAM School of Technology, GITAM University, Bengaluru, India
vyendapa@gitam.edu

Received: 23 September 2025 | Revised: 20 November 2025 | Accepted: 7 December 2025

 DOI: https://doi.org/10.48084/etasr.15047

ABSTRACT

The need for secure data sharing has recently become a critical requirement in modern digital communication networks, especially for image-based information, due to the increasing threats of unauthorized access and privacy breaches. Although cryptography and steganography are widely used for protecting confidential information, it is still a great challenge to achieve high levels of confidentiality and integrity with low computational complexity and minimal error rates. To overcome this challenge, this study proposed the Cosine Wavelet Transformative Convolutional Autoencoded Cryptography Steganography (CWTCA CryptStego) technique, which combines cryptographic and steganographic processes in a Convolutional Autoencoder (CAE) structure. The proposed technique uses Schmidt-Samoa cryptography for secure encryption, Myriad Normalized Residual Filtering (MNRF) for noise removal, and a Modified Discrete Cosine Transform (MDCT) for efficient data embedding, while at the decoder, the stego image is reconstructed with reduced distortion and improved visual quality. Performance analysis using standard evaluation metrics demonstrates that the proposed CWTCA CryptStego technique achieves lower bit error rates, higher Peak signal-to-noise ratio (PSNR), and enhanced confidentiality and integrity, while reducing computation time compared with existing techniques.

Keywords-secure image sharing; myriad normalized residual filtering; convolutional autoencoder; Schmidt-Samoa cryptography algorithm; modified discrete cosine transform-based steganography

I. INTRODUCTION

With the rapid advancement of communication and information technologies, the volume of digital images shared online has increased exponentially, often containing sensitive user information. At the same time, the growing frequency of image sharing has amplified the risks of unauthorized access, data breaches, and privacy violations. As a result, protecting sensitive and confidential image data and ensuring the security of digital image transmission has become a critical concern for both individuals and organizations.

Techniques such as cryptography, steganography, and secure transmission protocols play a central role and are commonly used in safeguarding digital images. However, more recently, hybrid methods and Deep Learning (DL) models have emerged to simultaneously enhance secrecy, imperceptibility, robustness, and reconstruction quality. Table I lists previous studies that have employed either one or a combination of the abovementioned approaches, highlighting their main strengths and key limitations. These studies can be organized into four groups:

1) Steganography-Only Solutions

Steganography-based methods primarily rely on LSB substitution, transform-domain embedding, chaotic mapping, or optimization-based pixel selection. These techniques can achieve high levels of imperceptibility and embedding capacity; however, they generally lack encryption mechanisms. As a result, once the hidden data is detected, it becomes vulnerable to unauthorized extraction or manipulation.

2) Cryptography-Only Solutions

Cryptography-based image protection schemes employ symmetric or asymmetric encryption algorithms to ensure data confidentiality. While these methods provide strong protection

against unauthorized access, they do not conceal the existence of the encrypted content, which may attract adversarial attacks. Furthermore, several cryptographic schemes introduce high computational overhead, limiting their suitability for real-time or large-scale image-sharing applications.

TABLE I. SUMMARY OF RELATED WORKS

Ref.	Method	Core Techniques	Main Strengths	Key Limitations
[1]	Hybrid (CR, ST, DL)	HOG-LSB and ANC SHA-256	Strong layered security	High time complexity
[2]	Hybrid	Chaotic encryption, optimal pixel selection	Good embedding security	Not lightweight
[3]	Hybrid	Multi-stage CR, ST	Improved robustness	Limited confidentiality gain
[4]	Hybrid	AES and LSB	Simple and effective	Encoding efficiency limited
[5-6]	Hybrid	AES, secret sharing	Reduced MSE	BER not minimized
[7]	DL	SRDNN ST	Reduced processing time	Confidentiality improvement limited
[8]	Hybrid	LSB, AES, Blowfish	Multi-layer encryption	High complexity
[9]	ST	LFSR stochastic model	High capacity	No CR layer
[10]	CR	Signal-based encryption	Strong encryption	No hiding layer
[11, 12]	ST	LSB variants	Low error embedding	No DL support
[13-16]	ST, Secret Sharing	IWT / DHT secret sharing	Lower computation	Weak authentication and confidentiality
[17-19]	ST	Chaotic / CNN / LSB	Quality improvement	Security robustness limited
[20]	Hybrid (ST, CR)	Multimodal biometric system with CR-ST framework	Enhances biometric data security	Reconstructed image error rate not sufficiently minimized
[21]	CR, DL	DL and encryption	Improved security	No asymmetric CR
[22, 23]	ST	Optimization -based embedding	Better pixel selection	Security analysis limited
[24-26]	Hybrid	Graph / elliptic / multi-perspective	Reduced error	Not scalable
[27, 28]	DL, ST	Encoder-decoder	Good reconstruction	Higher complexity
[29]	CR, ST	Vigenère, ST	Simple confidentiality	Weak CR strength
[30]	CR	Lightweight protocols	Efficient for IoMT	No ST

CR: Cryptography, ST: Steganography, Histogram of Oriented Gradients - Least Significant Bit (HOG-LSB), Adversarial Neural Cryptography with Secure Hash Algorithm 256-bit (ANC-SHA-256), Advanced Encryption Standard (AES), Super-resolution Deep Neural Network (SRDNN), Linear Feedback Shift Register (LFSR), Integer Wavelet Transform (IWT) /Discrete Hartley Transform (DHT), Convolutional Neural Network (CNN), Bit Error Rate (BER), Mean Squared Error (MSE), Internet of Medical Things (IoMT)

3) Hybrid Cryptography-Steganography Solutions

Hybrid approaches integrate cryptographic encryption with steganographic embedding to provide dual-layer security. These methods typically offer improved confidentiality and robustness compared to standalone solutions. Nevertheless, many existing hybrid schemes rely on conventional transforms and traditional encryption algorithms, which often lead to increased computational complexity, higher bit error rates, or inefficient embedding processes.

4) DL-Based Solutions

Modern research work employs deep neural networks, encoder-decoder networks, and Convolutional Autoencoders (CAEs) to obtain adaptive embedding and reconstruction. These methods improve the visual quality and reconstruction quality; however, they often require high computational power and do not necessarily involve robust asymmetric cryptographic techniques.

Despite substantial progress, current secure image-sharing schemes still suffer from several limitations. Most of the schemes fail to simultaneously optimize confidentiality, integrity, imperceptibility, and computational efficiency. High bit error rates are commonly observed in noisy or complex image environments, while hybrid and DL-based approaches often incur increased computational complexity. Additionally, efficient embedding of large image data using asymmetric cryptography remains a challenging task.

To overcome these limitations, this paper proposes a Cosine Wavelet Transformative Convolutional Autoencoded Cryptography Steganography (CWTCA CryptStego) system, which combines asymmetric cryptography, transform domain steganography, and DL. Specifically, the proposed system employs Schmidt-Samoa asymmetric encryption, Myriad Normalized Residual Filtering (MNRF) for denoising, and Modified Discrete Cosine Transform (MDCT) embedding in a CAE architecture. The proposed system primarily focuses on simultaneously improving confidentiality, integrity, reconstruction quality, and computational complexity while reducing the BER and improving the Peak signal-to-noise ratio (PSNR).

II. PROPOSED METHODOLOGY

Figure 1 presents the overall architecture of the proposed CWTCA CryptStego method, which comprises several major processing stages that are executed prior to secure transmission.

A. Image Preprocessing with Myriad Normalized Residual Filtering (MNRF)

Image preprocessing is used to improve image quality and enhance subsequent feature extraction and embedding processes by suppressing noise, enhancing contrast, and improving visual clarity. To achieve these objectives, the proposed framework employs MNRF, which eliminates pixels with abnormal deviations, thus suppressing noise and improving contrast.

Let $TI = \{TI_1, TI_2, \ldots, TI_N\}$ represent the set of input text images obtained from the dataset. Each image consists of a set of pixels $\{p_1, p_2, p_3, \ldots . p_m\}$ which are arranged within a sliding 3×3 filtering window, as shown in Figure 2. The center pixel of the window is selected for evaluation, and the similarity between this pixel and its neighbors is assessed using the Normalized Residual Test (NRT), calculated as:

$$NRT = \frac{|p_i - \mu|}{\sigma} \quad (1)$$

where p_i denotes a pixel in the filtering window, μ represents the mean pixel intensity, and σ denotes the standard deviation of the pixel intensities within the window. The filtered output is obtained as:

$$filtered_{out} = arg\,max(NRT) \quad (2)$$

where $arg\ max$ identifies the pixel exhibiting the maximum deviation from the mean. Pixels with the highest deviation are classified as noisy and are subsequently removed or replaced, enhancing image quality.

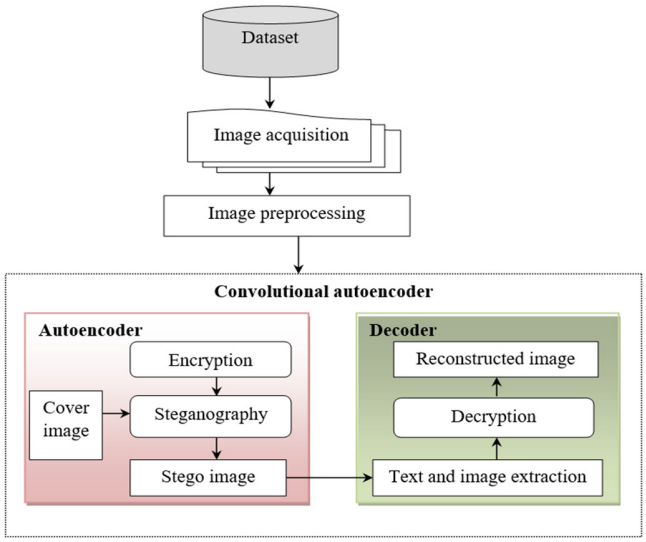

Fig. 1. Architecture of the proposed CWTCA CryptStego method.

p_1	p_2	p_3
p_4	p_c	p_6
p_7	p_8	p_9

Fig. 2. 3×3 filtering window used in the MNRF process.

The pseudocode algorithm of the MNRF-based image processing is given below:

```
Algorithm 1: MNRF for Image Preprocessing
Input: Set of input text images I
Output: Enhanced images with reduced noise
1. Collect a set of input text images
   from the dataset.
2. For each image, arrange pixels
   within a 3×3 filtering window.
3. Select the center pixel from the
   filtering window.
4. Compute the mean μ and deviation σ
   of pixels in the window.
5. Apply the Normalized Residual
   Statistical Test to measure the
   difference between each pixel and
   the mean.
6. Identify noisy pixels as those with
   maximum deviation from the mean.
7. Remove noisy pixels from the window.
8. Replace them with filtered output
   pixels to improve contrast.
Return the enhanced image.
```

B. Cryptographic Convolutional Autoencoder (CAE) with Modified Discrete Cosine Transform (MDCT)

After preprocessing, image sharing security is significantly enhanced through the integration of cryptography and steganography. The proposed framework employs a CAE, which combines the principles of convolutional networks with autoencoding architectures and consists of an encoder and a decoder. The encoder transforms the input image into a compact latent representation, while the decoder reconstructs the original data from this representation. Figure 3 illustrates the schematic structure of the CAE.

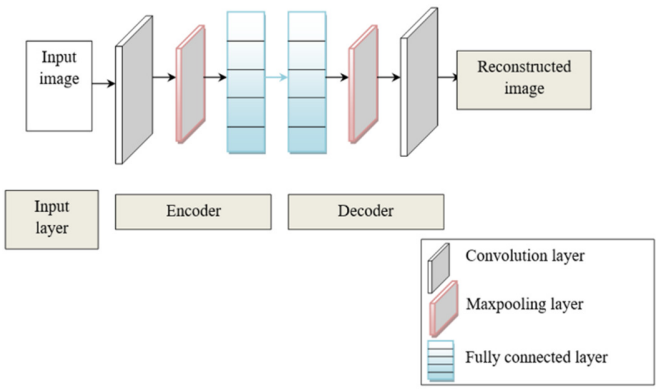

Fig. 3. Schematic structure of the CAE.

Let $MI = \{MI_1, MI_2, MI_3 \ldots MI_n\}$ denote the set of preprocessed images provided to the input layer. Each neuron computes a weighted sum of its inputs as:

$$Q = \sum_{i=1}^{n} (TI_i \cdot W_{ih}) + b_h \quad (3)$$

where Q indicates an activity of the neuron, W_{ih} represents a weight between the input and hidden layer, and b_h denotes the bias term. Then, the input image is transferred into the encoder network. The encoder consists of multiple sublayers, including convolutional layers, max pooling layers, and optionally fully

connected layers, which work together to hide the input images.

In the convolutional layers, image encryption is performed for securing digital images against unauthorized access. The proposed technique utilizes the Schmidt-Samoa cryptosystem asymmetric cryptographic technique, for generating the encrypted images. Asymmetric key cryptography, also known as public key cryptography, is a method of encryption that uses a pair of keys, such as a public key for encryption and a private key for decryption. This approach enhances security by ensuring that even if the public key is widely distributed, only the private key decrypts the information.

Key generation is a fundamental process in cryptography that involves creating keys for encryption and decryption. Let a and b be two large prime numbers. The public K and private M keys are generated as:

$$K = a^2 b \quad (4)$$

$$M = K^{-1} mod LCM\ (a-1, b-1) \quad (5)$$

The encryption process is performed using the receiver's public key:

$$CI = p^K mod K \quad (6)$$

where CI denotes a cipher image, and p denotes the pixel value in the input image.

After encryption, the encrypted images are forwarded to the fully connected layer of the encoder network, where the steganographic embedding process is performed. In this stage, steganography refers to the controlled embedding of encrypted secret information into a cover image in such a way that the presence of the hidden data remains imperceptible.

Figure 4 illustrates the MDCT-based steganography process applied to both the cipher and cover image. Figure 5 illustrates the block diagram of the cipher and cover image decomposition. In the first level of decomposition, the input image is divided into two sub-bands, low (L) and high (H). The low (L) sub-band is further decomposed into two sub-bands, low-low (LL) and low-high (LH). Similarly, the high (H) sub-band is further decomposed into two sub-bands, high-low (HL) and high-high (HH). This process is repeated across multiple decomposition levels, resulting in different sub-band representations.

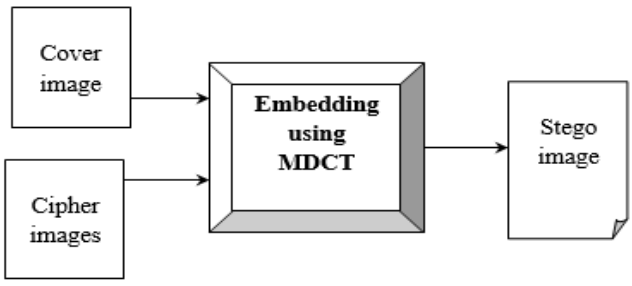

Fig. 4. MDCT-based image steganography process.

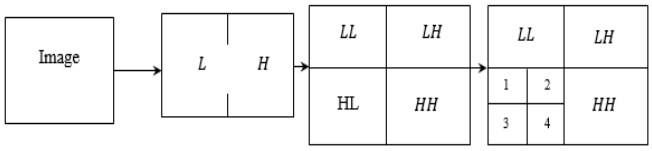

Fig. 5. Block diagram of the MDCT-based decomposition.

Let CI denote the cipher image and VI be the cover image. The modified cosine wavelet coefficients are computed as:

$$C_k = \sum_{j=1}^{2m-1} p_j cos\left[\frac{\pi}{m}(j + 0.5 + 0.5m)(k + 0.5)\right] \quad (7)$$

where C_k represents the wavelet coefficient, p_j denotes the input pixel value, m is half the number of input pixels (indicating dimensionality reduction from $2m$ to m), and k denotes the transform coefficient index.

The image embedding process hides the cipher image within the cover image to produce the stego image, which is not easily visible by the human eye. The embedding process is formulated as:

$$C_k(E) = C_k(VI) + \alpha \cdot C_k\ (CI) \quad (8)$$

where $C_k(E)$ denotes a modified MDCT coefficient after embedding the cipher image into the cover image, while α indicates the scaling factor that controls the amount of modification to the cover image coefficient.

After the embedding process, the resulting stego image SI is generated by applying the inverse modified cosine coefficients of the cover image to the cipher image data:

$$SI = IMDCT\ (C_k(E)) \quad (9)$$

The pseudocode algorithm of the encoding process of CWTCA CryptStego is given below:

```
Algorithm 2: Encoding Process of CWTCA
CryptStego
Input: Preprocessed text image I, Cover
image C
Output: Stego image SI
   1. Preprocessing Phase
      1.1. Collect preprocessed image I
      from the dataset.
      1.2. Apply MNRF to remove noise and
      enhance contrast.
   2. Encryption Phase
      2.1. Generate public-private key
      pair using the Schmidt-Samoa
      cryptographic algorithm.
      2.2. Encrypt the preprocessed image
      I with the receiver's public key to
      produce cipher image E.
   3. Autoencoder Encoding Phase
      3.1. Feed cipher image E into the
      encoder network of the CAE.
      3.2. Apply convolution and max
      pooling operations to reduce
      dimensionality and enhance feature
      representation.
```

```
   4. Steganography Embedding Phase
      4.1. Apply MDCT to decompose both
      cover image C and cipher image E
      into sub-band coefficients.
      4.2. Select wavelet coefficients
      from C and embed coefficients from E
      using the embedding rule:
C′=C+α·E
         Where α is the scaling factor.
4.3. Generate modified coefficients C′.
4.4. Apply the Inverse Modified Cosine
Wavelet Transform to reconstruct the stego
image SI.
Output
5.1. Return the stego image SI for secure
transmission.
```

C. Decoding Process

After transmission, the stego image is passed to the decoder module of the autoencoder to retrieve the original cipher image. First, the MDCT is applied to the stego image to extract the embedded coefficients:

$$C_k(E) = MDCT\ (SI) \tag{10}$$

To reverse the max-pooling operation performed during encoding, a MaxUnpooling operation is applied to upsample the feature maps and restore spatial resolution. The cipher image coefficients are then extracted by reversing the embedding process:

$$EC_k(CI) = \frac{C_k(E) - C_k(VI)}{\alpha} \tag{11}$$

where $EC_k(CI)$ denotes an extracted cipher coefficient. The cipher image is reconstructed using the inverse MDCT:

$$CI = IMDCT\ (EC_k(CI)) =$$

$$\frac{1}{m}\sum_{k=1}^{m-1} EC_k(CI)\ cos\ \left[\frac{\pi}{m}(j + 0.5 + 0.5m)(k + 0.5)\right] \tag{12}$$

Finally, the original text image is recovered by decrypting the cipher image using the private key:

$$TI = CI^M mod\ (K) \tag{13}$$

The pseudocode algorithm of the decoding process of the CWTCA CryptStego is given below:

```
Algorithm 3: Decoding Process of CWTCA
CryptStego
Input: Stego image SI
Output: Reconstructed original text image
   1. Apply the MDCT to extract cipher
      coefficients.
   2. Perform MaxUnpooling to reverse the
      MaxPooling step and upsample pixels.
   3. Extract the cipher image
      coefficients using the reverse
      embedding formula.
   4. Apply the inverse MDCT to
      reconstruct the cipher image.
   5. Use the private key to decrypt the
      cipher image and recover the
      original text image.
Return the reconstructed image.
```

D. Dataset

For the evaluation of the proposed CWTCA CryptStego model, the BOSSBASE 1.01 dataset [31] was employed. The dataset contains 10,000 grayscale images with pixel intensity values ranging from 0 to 255 and a spatial resolution of 256 × 256 pixels, which are used for secure data sharing experiments. For performance evaluation, the dataset was divided into 80% training images and 20% testing images to ensure an unbiased assessment. The dataset includes two types of images; namely natural images used as cover images and text images used as secret messages or secret images.

III. RESULTS AND DISCUSSION

A. Data Confidentiality Analysis

The data confidentiality rate refers to the percentage of textual image data successfully received by the intended recipient. It is mathematically expressed as the ratio of the number of sample textual images received to the total transmitted textual images, ensuring secure communication. The formula for calculating the data confidentiality rate DC is:

$$DC = \sum_{i=1}^{N} \frac{TI_{IR}}{TI_i} \cdot 100\% \tag{14}$$

where TI_i denotes a sample textual image involved in the secure data sharing process, and TI_{IR} denotes a sample textual image accessed only by the intended recipient.

For the evaluation of the proposed model, three additional methodologies were used for comparison: HOG-LSB with ANC SHA-256 [1], Bald Eagle Search Optimal Pixel Selection with Chaotic Encryption (BESOPS-CE) [2], and the hybrid data security system [4]. Figure 6 shows the data confidentiality performance of the evaluated methods for varying numbers of input images. Ten experimental observations were conducted for each method using different numbers of input images. The results indicate that the CWTCA CryptStego method consistently achieves a higher confidentiality rate than the other methods. For example, when 13 images were used, the CWTCA CryptStego method achieved a confidentiality rate of 92.3%, whereas the confidentiality rates of methods [1], [2], and [4] were 76.92%, 76.92%, and 90.72%, respectively. The overall comparative analysis shows that the confidentiality rate of the CWTCA CryptStego method improved by 13%, 20%, and 10% compared to methods [1], [2], and [4], respectively. This improvement is attributed to the use of the CAE.

B. Data Integrity Analysis

Data integrity DI refers to the percentage of textual image data that remains unaltered by any unauthorized users relative to the total input sample textual images:

$$DI = \sum_{i=1}^{N} \frac{TI_{NA}}{TI_i} \cdot 100 \tag{15}$$

where TI_i denotes a sample textual image data involved in the secure data sharing process, and TI_{NA} denotes a sample textual image not altered by malicious users.

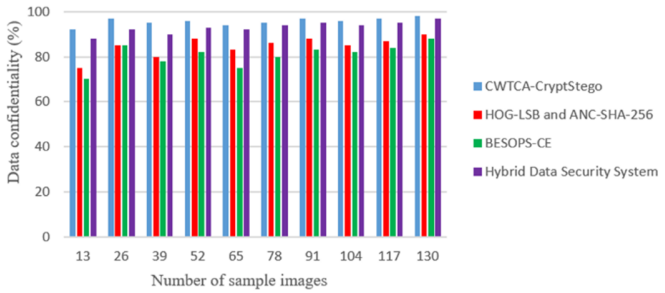

Fig. 6. Data confidentiality comparison of CWTCA CryptStego, HOG-LSB with ANC-SHA-256, BESOPS-CE, and hybrid data security system.

Figure 7 illustrates the data integrity performance of the evaluated methods. The results demonstrate that the CWTCA CryptStego method achieves higher data integrity than the existing methods across all test cases, and overall, 13% higher than the HOG-LSB with ANC SHA-256, 23% higher than the BESOPS-CE, and 10% higher than the hybrid data security system proposed in [4]. This improvement is mostly attributed to the use of the Schmidt-Samoa cryptographic algorithm.

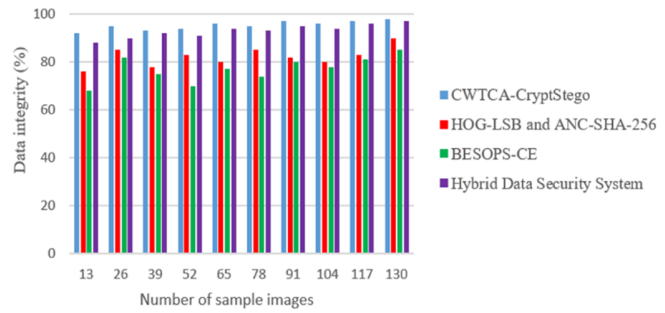

Fig. 7. Data integrity comparison of CWTCA CryptStego, HOG-LSB with ANC-SHA-256, BESOPS-CE, and the hybrid data security system.

C. Bit Error Rate (BER) Analysis

The BER is used to evaluate the efficiency and accuracy of the proposed method by comparing the original textual image data with the decoded textual image data. This metric provides a quantitative measure of transmission accuracy and is mathematically expressed as:

$$BER = \frac{1}{mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} TI_i(i,j) \oplus TI_i'(i,j)\right] \cdot 100 \quad (16)$$

where $TI_i(i,j)$ represents the original textual image data, $TI_i'(i,j)$ represents the decoded textual image data, and mn denotes the corresponding image dimensions.

Figure 8 presents the BER performance of the evaluated methods. The results show that the CWTCA CryptStego method consistently achieves a lower BER than the existing methods. For instance, when 13 images were used, the BER obtained by the CWTCA CryptStego method was 0.028, compared to 0.035, 0.038, and 0.032 for methods [1], [2], and [4], respectively. Overall, the BER when using the proposed method was lowered by 18% compared to HOG-LSB with ANC SHA-256, 29% compared to BESOPS-CE, and 7% compared to [4]. This improvement is primarily due to the application of MNRF.

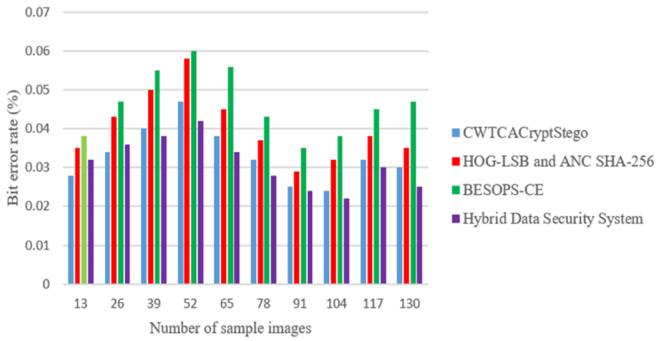

Fig. 8. BER performance of CWTCA CryptStego compared with HOG-LSB with ANC-SHA-256, BESOPS-CE, and the hybrid data security system.

D. Peak Signal-to-Noise Ratio (PSNR) Analysis

The PSNR metric is utilized to measure the efficiency of the proposed method. It is computed based on the MSE, representing the mean squared difference between the original textual image and the decoded textual image:

$$PSNR = 10log_{10}\frac{255^2}{MSE} \quad (17)$$

where:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[TI_i(i,j) - TI_i'(i,j)]^2 \quad (18)$$

Figure 9 illustrates the PSNR scores achieved by each of the approaches used. The results indicate that the proposed CWTCA CryptStego method achieves, in most cases, a higher PSNR, corresponding to a lower MSE between the original and decoded images, compared to the existing methods. Overall, the proposed CWTCA CryptStego had an increased PSNR by 15%, 19%, and 6% compared to the methods used in [1], [2], and [4], respectively, and it is attributed to the use of the CAE.

E. Computation Time Analysis

Computation time CT refers to the total time required by the algorithm to perform encoding and decoding for a given input image. It is mathematically expressed as:

$$CT = \sum_{i=1}^{n} TI_i * [TM_E + TM_D] \quad (19)$$

where TI_i denotes the number of textual images, TM_E denotes the time consumed for encoding, and TM_D denotes the time consumed for decoding during the overall embedding process.

Figure 10 presents the computation time required by each of the methodologies used. As expected, computation time increases with the number of images; however, the proposed CWTCA CryptStego method consistently requires less computation time than the existing techniques. Overall, the computation time of the proposed method is reduced by 11% compared to [1], 19% compared to [2], and 7% compared to [4]. This reduction is achieved through the application of the CAE and the MNRF.

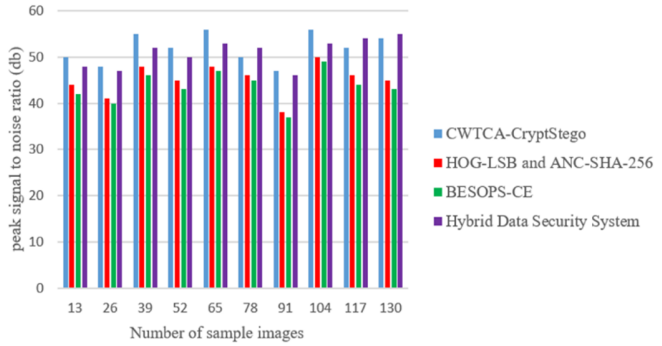

Fig. 9. PSNR analysis of CWTCACryptStego compared with HOG-LSB with ANC-SHA-256, BESOPS-CE, and the hybrid data security system.

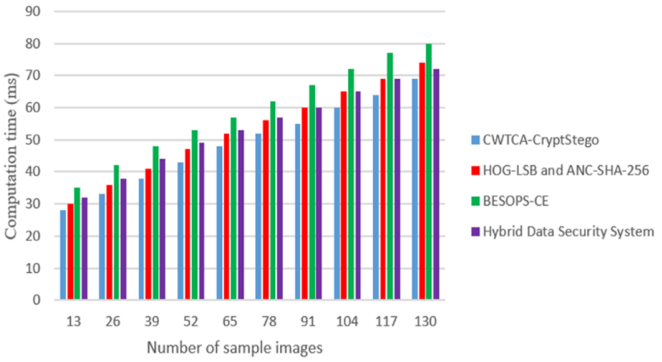

Fig. 10. Computation time analysis of CWTCA CryptStego compared with HOG-LSB with ANC-SHA-256, BESOPS-CE, and the hybrid data security system.

F. Analysis of Variance (ANOVA) Statistical Test

To statistically evaluate the performance differences between the proposed CWTCA CryptStego method and the other methods, a two-way Analysis of Variance (ANOVA) test was conducted. The test was used to assess the effects of the security scheme and the type of performance metric on the observed results, thereby determining whether the improvements were statistically significant.

The two-way ANOVA test without interaction was applied with the security scheme as one factor with four levels and the performance metric as the second factor with five levels, namely confidentiality rate, integrity rate, BER, PSNR, and computation time. The dependent variables were the corresponding performance values obtained from repeated experimental trials, with ten trials conducted for each combination of security scheme and performance metric.

Table II presents the ANOVA analysis results, revealing that the effect of the method on performance is statistically significant ($p<0.001$), indicating that the observed differences among methods are not due to random variation. Similarly, the effect of the performance metric is also statistically significant ($p<0.001$), confirming meaningful variability across evaluation criteria. These statistical results validate that the proposed CWTCA CryptStego method demonstrates significantly improved performance compared to the other techniques.

TABLE II. ANOVA STATISTICS

Source of Variation	Degrees of freedom	F-value	P-value
Method	3	18.47	<0.001
Performance Metric	4	26.12	<0.001

IV. CONCLUSION

In this paper, a hybrid data security system combining image steganography with a cryptography model, named Cosine Wavelet Transformative Convolutional Autoencoded Cryptography Steganography (CWTCA CryptStego) method, is proposed. This method is developed to achieve effective image security by integrating Convolutional Autoencoder (CAE)-based encoding and decoding operations for efficient image encryption and embedding. Through this process, both cipher and stego images are generated. The decoder network subsequently extracts and decrypts the embedded images, reconstructing the original images securely with minimal error.

To evaluate the performance of the proposed method, several quantitative metrics, including data confidentiality, data integrity, Bit Error Rate (BER), Peak signal-to-noise ratio (PSNR), and computation time, were employed. Experimental results demonstrate that the CWTCA CryptStego method outperforms techniques such as Histogram of Oriented Gradients - Least Significant Bit (HOG-LSB) with Adversarial Neural Cryptography with Secure Hash Algorithm 256-bit (ANC-SHA-256), Bald Eagle Search Optimal Pixel Selection with Chaotic Encryption (BESOPS-CE), and a hybrid data security system, achieving higher security levels while reducing transmission time and minimizing errors during image sharing.

Despite these advantages, the proposed method has some limitations. The data-hiding capacity is limited, particularly when applied to compressed or small-sized images, potentially leading to longer transmission times. Additionally, the combination of steganography with cryptography can increase data size, which may exceed available bandwidth, and may require specific cryptographic configurations to avoid high computational complexity. For future work, the focus will be on developing more robust, imperceptible, and intelligent security systems, leveraging advancements in Artificial Intelligence (AI) and addressing the growing demand for secure communication in emerging technologies, such as the Internet of Things (IoT).

REFERENCES

[1] M. A. Hameed, M. Hassaballah, R. Abdelazim, and A. K. Sahu, "A novel medical steganography technique based on Adversarial Neural Cryptography and digital signature using least significant bit replacement," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 379–397, 2024, https://doi.org/10.1016/j.ijcce.2024.08.002.

[2] A. A. Bahaddad, K. Ali Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," *Alexandria Engineering Journal*, vol. 75, pp. 41–54, July 2023, https://doi.org/10.1016/j.aej.2023.05.051.

[3] M. M. Msallam and F. Aldoghan, "Multistage Encryption for Text Using Steganography and Cryptography," *Journal of Techniques*, vol. 5, no. 1, pp. 38–43, Mar. 2023, https://doi.org/10.51173/jt.v5i1.1087.

[4] S. E. Ghrare, M. A. Abouras, and I. A. Akermi, "Development of Hybrid Data Security System using LSB Steganography and AES Cryptography," *African Journal of Advanced Pure and Applied Sciences (AJAPAS)*, vol. 3, no. 2, pp. 86–95, Jun. 2024.

[5] M. E. Danlami, L. L. Raymond, and T. Solomon, "Hybridization of Cryptography and Steganography to Achieve Secret Communication," *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 5, no. 8, pp. 428–437, Aug. 2024.

[6] M. M. Shwaysh, S. Alani, M. A. Saad, and T. A. Abdulhussein, "Image Encryption and Steganography Method Based on AES Algorithm and Secret Sharing Algorithm," *Ingénierie des systèmes d'information*, vol. 29, no. 2, pp. 705–714, Apr. 2024, https://doi.org/10.18280/isi.290232.

[7] S. Priya, S. P. Abirami, B. Arunkumar, and B. Mishachandar, "Super-resolution deep neural network (SRDNN) based multi-image steganography for highly secured lossless image transmission," *Scientific Reports*, vol. 14, no. 1, Mar. 2024, Art. no. 6104, https://doi.org/10.1038/s41598-024-54839-7.

[8] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, vol. 13, no. 21, Oct. 2023, Art. no. 11771, https://doi.org/10.3390/app132111771.

[9] M. EL-Hady, M. H. Abbas, F. A. Khanday, L. A. Said, and A. G. Radwan, "DISH: Digital image steganography using stochastic-computing with high-capacity," *Multimedia Tools and Applications*, vol. 83, no. 25, pp. 66033–66048, Jan. 2024, https://doi.org/10.1007/s11042-023-17998-9.

[10] A. İhsan and N. Doğan, "An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security," *Multimedia Tools and Applications*, vol. 83, no. 35, pp. 82589–82619, Mar. 2024, https://doi.org/10.1007/s11042-024-18722-x.

[11] S. Rahman *et al.*, "A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image," *Scientific Reports*, vol. 13, no. 1, Aug. 2023, Art. no. 14183, https://doi.org/10.1038/s41598-023-41303-1.

[12] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022, https://doi.org/10.1109/ACCESS.2022.3224745.

[13] Z. Saeidi, A. Yazdi, S. Mashhadi, M. Hadian, and A. Gutub, "High performance image steganography integrating IWT and Hamming code within secret sharing," *IET Image Processing*, vol. 18, no. 1, pp. 129–139, Jan. 2024, https://doi.org/10.1049/ipr2.12938.

[14] B. Parihar, M. Deshmukh, and A. S. Rawat, "Efficient Single Secret Image Sharing in Resource-Constrained Environment using Counting-Based Secret Sharing over Cloud," *Procedia Computer Science*, vol. 230, pp. 158–167, 2023, https://doi.org/10.1016/j.procs.2023.12.071.

[15] C. Yu, X. Zhang, C. Qin, and Z. Tang, "Reversible Data Hiding in Encrypted Images With Secret Sharing and Hybrid Coding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 11, pp. 6443–6458, Nov. 2023, https://doi.org/10.1109/TCSVT.2023.3270882.

[16] R. M. Holla and D. Suma, "Progressive Hartley image secret sharing for high-quality image recovery," *Cogent Engineering*, vol. 10, no. 2, Dec. 2023, Art. no. 2262805, https://doi.org/10.1080/23311916.2023.2262805.

[17] L. Huo, R. Chen, J. Wei, and L. Huang, "A High-Capacity and High-Security Image Steganography Network Based on Chaotic Mapping and Generative Adversarial Networks," *Applied Sciences*, vol. 14, no. 3, Feb. 2024, Art. no. 1225, https://doi.org/10.3390/app14031225.

[18] V. K. Sharma, P. Kumar, S. Singhal, B. P. Soni, and P. K. Shukla, "Secret image scrambling and DWT-based image steganography using smoothing operation and convolution neural networks," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 26, no. 3, pp. 695–705, 2023, https://doi.org/10.47974/JDMSC-1742.

[19] R. Panigrahi and N. Padhy, "An effective steganographic technique for hiding the image data using the LSB technique," *Cyber Security and Applications*, vol. 3, Dec. 2025, Art. no. 100069, https://doi.org/10.1016/j.csa.2024.100069.

[20] G. M. Salama *et al.*, "Efficient multimodal cancelable biometric system based on steganography and cryptography," *Iran Journal of Computer Science*, vol. 6, no. 2, pp. 109–121, June 2023, https://doi.org/10.1007/s42044-022-00115-8.

[21] M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, "Face Image Encryption Based on Feature with Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map," *Sensors*, vol. 23, no. 3, Jan. 2023, Art. no. 1415, https://doi.org/10.3390/s23031415.

[22] A. S. Ali, S. Alsamaraee, and A. A. Hussein, "Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity," *Journal of Computer Networks and Communications*, vol. 2024, no. 1, Jan. 2024, Art. no. 2516567, https://doi.org/10.1155/2024/2516567.

[23] S. Rezaei and A. Javadpour, "Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission," *Multimedia Tools and Applications*, vol. 83, no. 35, pp. 82247–82280, Mar. 2024, https://doi.org/10.1007/s11042-024-18776-x.

[24] A. Sabharwal, P. Yadav, and K. Kumar, "Graph Crypto-Stego System for Securing Graph Data Using Association Schemes," *Journal of Applied Mathematics*, vol. 2024, no. 1, Jan. 2024, Art. no. 2084342, https://doi.org/10.1155/2024/2084342.

[25] M. Kaur *et al.*, "EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT," *IEEE Access*, vol. 11, pp. 90739–90748, 2023, https://doi.org/10.1109/ACCESS.2023.3305271.

[26] S. Rahman *et al.*, "Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats," *Sustainability*, vol. 15, no. 5, Feb. 2023, Art. no. 4252, https://doi.org/10.3390/su15054252.

[27] A. Kumar, R. Rani, and S. Singh, "Encoder-Decoder Architecture for Image Steganography using Skip Connections.," *Procedia Computer Science*, vol. 218, pp. 1122–1131, 2023, https://doi.org/10.1016/j.procs.2023.01.091.

[28] Y. Y. Abdullahi, L. G. Farouk, A. S. Nur, and A. Sale, "Proposition of a Better Data Security Model for a Protective Information Exchange on the Internet with Advanced Steganographic and Cryptographic Algorithm," *Journal of Applied Sciences and Environmental Management*, vol. 28, no. 10, pp. 3013–3018, Oct. 2024, https://doi.org/10.4314/jasem.v28i10.8.

[29] V. Smith, M. Mendoza, and I. Ullah, "Data Security Techniques Using Vigenere Cipher And Steganography Methods In Inserting Text Messages In Images," *Journal of Information Systems and Technology Research*, vol. 3, no. 3, pp. 92–100, Sept. 2024, https://doi.org/10.55537/jistr.v3i3.867.

[30] H. Y. Naser, A. K. Mattar, M. A. Saare, M. A. Almaiah, and R. Shehab, "A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25746–25756, Aug. 2025, https://doi.org/10.48084/etasr.12204.

[31] BOSSBASE. (1.01),. [Online]. Available: https://dde.binghamton.edu/download/.