International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

Myriad Wavelet Transformed Certificateless Signcryptive Extreme Learning Steganography for Secure Medical Image Transmission

J. Shaik Dawood Ansari (Author)
Research Scholar, Department of CS,
Karpagam Academy of Higher Education
Coimbatore, India.
e-mail: jsdansari@gmail.com

Dr. P. Tamilselvan
Research Supervisor, Department of CS,
Karpagam Academy of Higher Education
Coimbatore, India.
e-mail: tamilselvancs@kahedu.edu.in.

Abstract— Medical imaging is a vital part of the healthcare sector which facilitates the communication of medical images like X-rays, MRIs, and CT scans from one place to another. Medical images are now being sent over public networks due to improvements in the healthcare industry, which creates potential security challenges like authentication, integrity, and confidentiality. The medical images size being transmitted has also become a major concern after the rapid growth of computer networks and information technology. Therefore, ensuring secure medical image transmission and efficient compression are crucial aspects of modern healthcare systems. To enhance the security of image transmission while reducing image size, an efficient technique known as Myriad Wavelet Transformed Certificateless Signcryption Extreme Learning Steganography (MWTCSELS) has been introduced. The MWTCSELS involves four distinct processes namely image preprocessing, image compression, signcryption, and embedding. The first step is to denoise the medical image, the Wilcox indexive myriad filtering technique is used. Then after the preprocessing is done by compressing the image and minimizing the storage space in the communication, the Burrows-Wheeler Hilbert linear curve transform is used. In the third step, the Schmidt-Samoa cryptographic Certificateless Signcryption method is employed to encrypt the input image securely. Lastly, the Mar Wavelet transformed Extreme Learning Machine is used to embed confidential data into the image using a Stego key. The resulting Stego images can be transferred to the receiver end. The original images are restored from the Stego images by the authorized receiver after performing the extraction process. Subsequently, the unsigncryption and decompression processes are carried out to restore the original medical image with enhanced security. An experimental evaluation is conducted using medical chest X-ray images, to measure its performance based on aspects like peak signal-to-noise ratio (PSNR), compression ratio, space complexity, confidentiality rate, and integrity rate. The obtained results demonstrate that MWTCSELS is more efficient in achieving higher peak signal-to-noise ratios and compression ratios while maintaining strong confidentiality and utilizing less storage space compared to existing approaches.

Keywords*-Secure medical image transmission, Wilcox indexive myriad filtering, Burrows-Wheeler Hilbert linear curve transform based compression, Schmidt-Samoa cryptographic Certificateless Signcryption, Mar Wavelet transformed Extreme learning machine*

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

I. INTRODUCTION

Enabling secure communication of digital images, especially over open wireless networks, poses significant research challenges. Among digital images, medical images are particularly well-known. Due to their inherent sensitivity, transmission of medical images over networks with the highest standards of security is a major challenging issue. Any alteration that occurs in the medical image during transmission could significantly impact the accuracy of patient diagnoses. Therefore, the primary objective is to transmit these images securely and without any modifications. Steganography algorithms are commonly employed to address this concern. These algorithms facilitate the concealment of confidential information within the pixel values of medical images. This practice not only enhances the security of the transmission but also ensures that the integrity of the medical image.

A Lightweight Certificateless Group Signcryption Technique (CGST) was designed in [1]. This technique relies on Fractional Chaotic Maps (FCM) to distribute sensitive user information across wireless channels. However, the higher confidentiality rate was not achieved. The authors of [2] designed an enhanced steganographic algorithm for medical images that can cover patients' sensitive information within the images. The algorithm designed offers more confidentiality, higher embedding capacity, and robustness. However, embedding did not take less time.

The authors of [3] designed a double image compression-encryption model to enhance the effectiveness and security of image compression-encryption algorithms. However, steganography aspect was not considered to increase the confidentiality. The authors of [4] designed a novel quantum multi-image compression and encryption algorithm. This algorithm minimizes computational complexity by integrating the discrete cosine transform. However, in terms of performance the higher compression ratios are not achieved. The integration of the modified Salp Swarm Algorithm (SSA) and Chaotic Coupled Map Lattices (CML) was introduced in [5]. The aim of this integration is to make the transmission more secure by encrypting and compressing medical images. However, the integrity level was not improved. The authors of [6] designed a new image encryption algorithm with the support of fractional-order chaotic system and compression sensing algorithm. However, the computational cost of this encryption algorithm was higher compared to the original encryption method. An optical-based algorithm was developed in [7] to improve the efficiency and security of transmitting medical images through insecure channels. The algorithm enhances authentication and data integrity, but it did not reduce the time consumption. A hybrid data compression algorithm was designed in [8] based on RSA cryptography method to enhance the security level. However, the higher integrity rate was a challenging issue.

An image steganography technique was developed in [9] to securely embed patients' personal information into medical images, thereby enhancing the level of confidentiality. However, to reduce space complexity, image compression was not implemented. The authors of [10] designed a variational autoencoder algorithm for compressing the medical images. Security analysis was not performed even though the algorithm increases the performance of compression rate.

II. MAJOR CONTRIBUTIONS

The proposed MWTCSELS's major contributions are discussed in the following lines,

- The MWTCSELS technique, which involves preprocessing, compression, signcryption, and embedding, have been introduced to make the transmission of medical images more secure.
- To reduce the mean square error and improve the peak signal-to-noise ratio, the Wilcox indexive myriad filtering technique is applied. This filtering technique serves to perform denoising and enhancing image contrast.
- To improve the compression ratio, the MWTCSELS algorithm employs the Burrows-Wheeler Hilbert linear curve transform to compress the image, thereby minimizing the space complexity during transmission.
- To enhance the confidentiality and integrity, the Schmidt-Samoa cryptographic certificateless signcryption method is utilized to encrypt the input image.
- The Mar Wavelet Transformed Extreme Learning Machine is employed to embed confidential data into the encrypted image. This process enhances integrity and minimizes the embedding time.
- Finally, simulations are done using various metrics to measure the performance improvements of MWTCSELS over existing methods.

III. OUTLINE OF THE PAPER

The structure of the paper is as follows. Section 2 reviews the literature on related techniques. Section 3 describes the proposed MWTCSELS technique with various processes. The experimental results and performance evaluations are presented in Section 4, using both quantitative and qualitative analysis of medical images. Section 5 concludes the paper with a brief summary.

IV. RELATED WORKS

A JPEG compression processor was designed in [11] with stego-key based hardware steganography to enhance the secure transmission. A new approach for high-capacity reversible data hiding was designed in [12] utilizing intra-block lossless compression. However, the embedding capacity was not improved. An image encryption algorithm with visual asymmetry was introduced in [13]. This algorithm uses the SHA-3 and compressive sensing to embed the encrypted image. However, the algorithm did not achieve satisfactory performance in terms of both higher confidentiality and integrity. In [14], a high-capacity and robust JPEG steganography technique was developed using adversarial training to embed secret messages. However, this approach did not explore added advanced and multifaceted network structures to uplift the security and efficiency of end-to-end JPEG steganography. A modified least significant bit (LSB) technique was developed in [15] for preserving and hiding medical data. This approach enhances the embedding rate but it does not minimize the time consumption.

An improved image steganography approach was presented in reference [16] to enhance the hiding capacity of stego images. However, this approach failed to extend the high dimensional image modalities of various body parts. A highly secured technique was developed in [17] using IoT protocol and steganography to guarantee the higher data security, confidentiality, and integrity. However, minimizing the space consumption was not considered by the image compression.

In [18], an adaptive approach was developed to lessen the distortion caused by the embedding of medical images. But, the time involved in the process to embed the medical images was not minimized. In [19], a novel image steganographic algorithm was introduced integrating modified LSB and a chaotic map. However, the algorithm did not attain better integrity performance. Two specific secret-sharing techniques were developed in [20] based on traditional secret sharing and the other on matrix-based secret sharing. However, these techniques did not utilize efficient steganographic methods to achieve higher capacity.

V. PROPOSAL METHODOLOGY

The advancement in digital technologies directs to the transmission of the medical information over communication network. The transmission of information in these communication networks is not secure and patients may lose the privacy of medical contents since images are different from the text due to their two particular factors such as loss of information and confidentiality. To reduce loss of information and provide high level security, in this paper, a novel MWTCSELS technique is introduced. This main goal of the proposed MWTCSELS is to improve the security of medical images during their communication across public networks with higher storage efficiency.

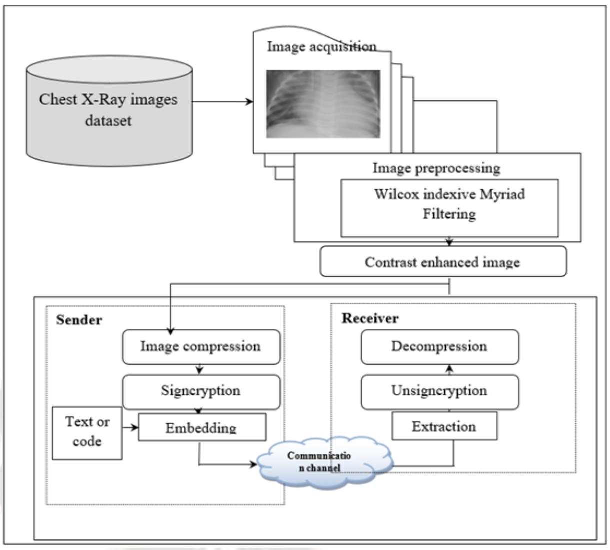


Figure 1 architecture of proposed MWTCSELS for secure medical image transmission

Figure 1 illustrates an architectural diagram of MWTCSELS, which comprises four major processes before transmission. As depicted in the figure, a number of X-Ray images denoted as $CI_1, CI_2, \dots, CI_n$ are collected from the dataset. Once the images are acquired, Wilcox indexive Myriad Filtering is applied to perform denoising and enhance image contrast. This is followed by Burrows-Wheeler Hilbert linear curve transform-based compression, Schmidt-Samoa cryptographic Certificateless Signcryption, and Mar Wavelet-transformed Extreme learning machine-based image steganography on the sender's side prior to transmission. Upon reception, the receiver carried out processes such as image extraction, unsigncryption, and decompression to retrieve the original image with enhanced confidentiality and integrity.

VI. WILCOX INDEXIVE MYRIAD FILTERING BASED IMAGE PREPROCESSING

Image preprocessing is a fundamental step in the field of imaging and analysis. It involves with the aim of improving the image quality, consistency, and usability of images before subjected to further analysis. As a result, employing an appropriate preprocessing technique is essential for improving image quality and facilitating accurate analysis. In this context, the proposed MWTCSELS technique utilizes the Wilcox indexive Myriad Filtering technique for preprocessing medical images. The Wilcox index is a qualitative analysis.

Let us consider the number of chest images $CI_1, CI_2, \dots, CI_n$ collected from the Chest X-Ray images dataset. For each image comprises of the number of pixels $P_1, P_2, P_3, \dots . P_m$. These pixels are arranged in the filtering 3*3 kernel window.

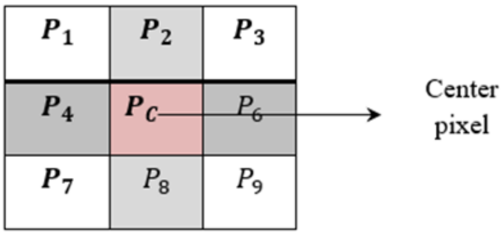


FIGURE 2 $\boldsymbol{3*3}$ FILTERING WINDOW

Figure 2 illustrates the $3*3$ filtering window pixel arrangement in the filtering window with row and columns. After the pixel arrangement, the center pixel chooses from the filtering window for noise removal process. The window undergoes the Wilcox indexive Myriad Filtering technique, which calculates the likelihood of similarity between the pixels at the center and those around it. Given below is the filtering process,

$F = arg\ min\ (q * \sum_{i=1}^{n} |\boldsymbol{P_c} - \boldsymbol{P_i}|)$ (1)

From (1), F indicates a filtered output, arg min denotes an argument of the minimum function, P_c denotes a center pixel and P_i indicates a 'n' number of neighboring pixels, q indicates a weight. The weight function in the above equation is used to control the blurring of the image. From (1) a pixel with the minimum deviation of neighboring pixels is said to be a normal. Noisy pixels are the pixels with the maximum deviation of neighboring pixels. Such noisy pixels are removed from the filtering window in result it uplifts the quality of input chest X-ray images. The algorithm of Wilcox indexive Myriad Filtering technique-based image denoising is described as given below,

// Algorithm 1: Wilcox indexive Myriad Filtering based image denoising

Input: Image dataset 'D' number of chest images '$CI_1, CI_2, CI_3, \ldots .CI_n$,

Output: Improve image contrast

```
Begin
    1.  Collect number of chest images $CI_1, CI_2, CI_3, \ldots .CI_n$ from dataset
    2.  For each image $CI_i$
    3.      Arrange pixels $P_1, P_2, P_3, \ldots .P_m$ in filtering window
    4.      Sort the pixels $P_1, P_2, P_3, \ldots .P_m$
    5.      Select the center value $P_C$
    6.      For each $P_C$
    7.          For each $P_i$
    8.              Measure the likelihood using (1)
    9.          End for
    10.     End for
    11.     Identify the noisy pixels and removed from the window
    12.     Return (contrast enhanced X-Ray image)
    13. End for
End
```

Algorithm 1 outlines the procedure for image denoising using the Wilcox indexive Myriad Filtering technique, aiming to decrease error and increase peak signal-to-noise ratio (PSNR). The process starts by collecting a set of input images from the dataset. Subsequently, denoising is executed during the preprocessing stage. In the context of the denoising process, the pixels within the chest image are organized within a kernel window, structured as rows and columns, with a particular pixel chosen as the central value. Noisy pixels are then identified through a maximum likelihood comparison between the central pixel and its neighboring pixels. Pixels exhibiting the greatest deviation from the central pixel are labeled as noisy pixels and it removed. This process contributes to the enhancement the of image contrast.

VII. BURROWS-WHEELER HILBERT LINEAR CURVE TRANSFORM BASED IMAGE COMPRESSION

After the image preprocessing, the proposed MWTCSELS technique performs the image compression to decrease the size of the input image in the communication. In Image compression the size of digital images can be decreased, which also preserves the essential visual information for more efficient storage and transmission. Therefore, the proposed MWTCSELS technique applies the Burrows-Wheeler Hilbert linear curve transform for lossless image compression.

The compressed version of an image does not lose any information and can be used to restore the original image exactly in lossless compression.

$$CI_{ij_{org}} = C_{ij\_comp} \quad (2)$$

Where, $CI_{ij_{org}}$ denotes the original preprocessed image and $CI_{ij_{Comp}}$ denotes the reconstructed image.

A digital chest image is shown by a two-dimensional array of pixels, which are stored in rows and columns denoted as a $m*n$ matrix.

$$CI_{ij} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{bmatrix} \quad (3)$$

Where P_{11} shows first row pixel and the first column of the image. The row and column of the image, P_{mn} shows the 'm' row and 'n' column of the image. An image comprises the likely pixels values varies from 0 and 255.

The proposed transform is used to convert a block of image pixels into a sequence of efficient form.

By applying a Hilbert linear curve in the transformation process scans every pixel in the matrix 'CI_{ij}'. The Hilbert curve is a square with one open side and it has four directions such as top, bottom, left and right. The second level of the Hilbert curve is sometimes utilized in lossless image compression techniques.

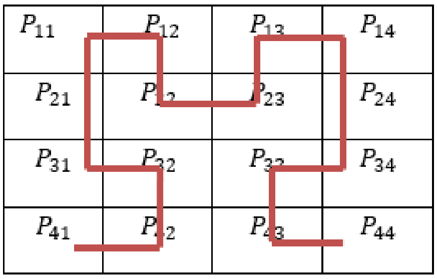


FIGURE 3 HILBERT CURVE ON IMAGE PIXELS IN MATRIX

Figure 3 illustrates the second-order Hilbert curve applied to image pixels. In the Hilbert space, the image pixels are organized within a rectangular block. The paths traced by the space-filling curve establish a linear order among the image pixels. This order is established by beginning at one end of the curve and following the subsequent path to the opposite end. The encoding of the Hilbert space curve is employed to transform the current direction into a unit value. The Hilbert curve is defined as a sequence of directions, where each direction is denoted by one of the terminal symbols {→ (right), ↑ (top), ← (left), ↓ (bottom)}. The transformation process is used to map the terminal symbol to the integer {0, 1, 2, 3}.

$$C_{ij\_comp} = T\{C_{ij\_pre}\} \quad (4)$$

Where, C_{ij_comp} denotes a compressed image, T indicates transformation, C_{ij_pre} denotes a preprocessed image pixel. The preprocessed input image on which transformation function 'T' is applied.

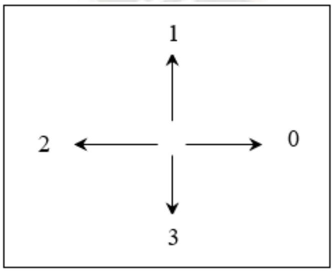


FIGURE 4 HILBERT DIRECTION AND INTEGER VALUE

Figure 4 illustrates a Hilbert integer Hilbert direction and integer value. From figure 3 and 4, the final transformed results are obtained as follows,

$$C_{ij\_comp} = \{012110301033230\} \quad (5)$$

Where, C_{ij_comp} denotes a compressed pixels of input image. In this manner, efficient compression is achieved, resulting in a better compression ratio.

Algorithm 2: Burrows-Wheeler Hilbert linear curve transform based image compression algorithm

Input: Preprocessed Chest image $CI_1, CI_2, CI_3 \ldots . CI_n$

Output: Compressed image

```
Begin
    1. Collect number of preprocessed images
    2.     For each preprocessed image
    3.         Formulate the pixel matrix '$CI_{ij}$'
    4.         Mapping the pixels space into Hilbert space using (4)
    5.         Convert current direction into unit value using (5)
    6.     End for
    7. Return (compressed pixels of input image)
End
```

Algorithm 2, as depicted above, outlines the processing steps for image compression utilizing the Burrows-Wheeler Hilbert linear curve transform. Initially, the preprocessed image is taken as input for a lossless compression process. The pixels in the input image are organized into a matrix with rows and columns. Subsequently, the pixel values are mapped onto the Hilbert space. This is followed by a transformation process that converts the current direction into a unit value. Finally, the compressed pixel values of the input image are obtained.

VIII. SIGNCRYPTION

Upon successful image compression, the signcryption process is carried out to improve the security of transmission through the communication channel. A cryptographic primitive that performs both digital signature and encryption in one step is called Certificateless Signcryption. On the contrast to conventional Certificateless Signcryption, the Schmidt-Samoa cryptography is implemented into the Certificateless Signcryption to further enhance the security. Setup, partial private key generation, full private key generation, public key generation, signcryption and unsigncryption are the various steps involved in the certificateless signcryption system.

The setup phase has the security parameter 'Q' and returns global system parameters (R) which has a Session Key (SK), image space (D), cipher image space (C). It is mentioned as,

$$R \rightarrow \langle SK, D, C \rangle (6)$$

Then the partial private key (k_{pp}) is attained as given below,

$$k_{pp} \rightarrow \langle \text{ID}, R, PV \rangle \quad (7)$$

The user identity (ID) takes an arbitrary value '0' and '1'. If the user identity is '1', then it returns a partial private key. If the user identity is '0', then it returns unauthorized entity, as of (4). Given the common parameters R, and the corresponding public value PV. Then the full private key is generated by using Schmidt-Samoa cryptography by considering two large prime numbers 'u'and 'v'

$$k_{fp} = {k_{pb}}^{-1} \, mod \, lcm \, (u-1, v-1) \; (8)$$

Where, k_{fp} denotes a full private key, k_{pb} denotes a public key,

$$k_{pb} = u^2 v \quad (9)$$

The public and full private key are used to perform the encryption and signature generation process together, after the key generation is finished.

The encryption is performed with receiver public key

$$\beta_E = CCI^{k_{pb}} \, mod \, k_{pb} \quad (10)$$

Where, k_{fp} denotes a full private key, k_{pb} denotes a public key,

The corresponding signature 'Sig' is generated as follows,

$$Sig = CCI^{k_{pp}} \, mod \, k_{pb} \quad (11)$$

Where, k_{fp} denotes a full private key, k_{pb} denotes a public key, CCI denotes a compressed chest image. In this way, the cipher text and signature are generated

IX. Marr Wavelet transformed Extreme learning machine-based image embedding

The embedding process is completed at the end to hide the secret data within an image, elevating the security of communication. Therefore, steganography becomes a significant technique for embedding the confidential information into an image. The proposed technique employs an encrypted image as the input for the embedding process. Steganography is combined with cryptography to enhance security. The image is encrypted before being embedded using steganography techniques, thereby increasing the complexity of discovering the original image.

In this work, a novel extreme learning machine is utilized for the embedding process. Unlike conventional deep learning algorithms, the proposed extreme learning machines consist of feed-forward neural networks with a direct solution that eliminates the need for any backpropagation concepts. This solution is both linear and highly efficient, producing a linear output. The main objective of extreme learning machines is to achieve rapid training speed and capability. Consequently, the technique employs the extreme learning classifier for precise embedding, minimizing the required time for the process.

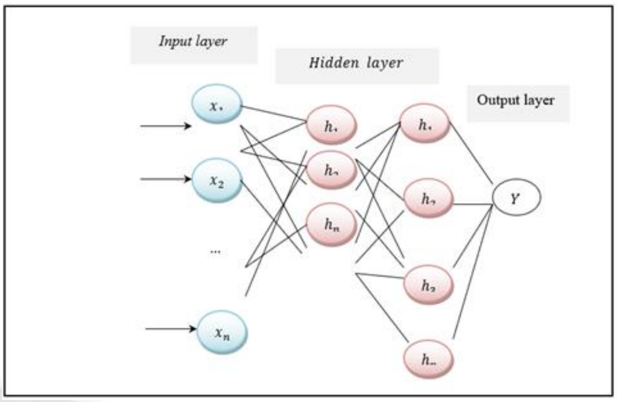


FIGURE 5 STRUCTURE OF EXTREME LEARNING MACHINE

Figure 5 depicts the structure of Extreme learning machines used for image embedding with a single layer or multiple layers of hidden nodes 'h'. The ELM structure comprises of input layer, hidden layers, and output layer. Related to deep neural network, it has two characteristics such as the parameters input weights and the biases are randomly initialized. As shown in the above figure, let us consider that the training set $\{ECI, Y\}$ where ECI denotes an encrypted chest image and a 'Y' representing its embedded output.

The input layer only receives the input image but it did not perform any computations, whereas the output layer provides the output results and did not require any iteration process. The certain computation process is performed in hidden layer. As shown in Figure 2, an Extreme learning machine receives the encrypted chest image 'ECI' and randomly set a weight '$\beta_1, \beta_2, \dots, \beta_m$' and added bias '$B$' in the hidden layer that stored the value is '1'.

$$x_i = \sum_{i=1}^{n} [ECI_i(t) * \beta_{ij}] + B \quad (12)$$

From equation (12), the activity of neurons at the input layer 'x_i', β_{ij} denotes a weight between the i^{th} input layer neuron and the j^{th} hidden layer neuron, B denotes a bias.

The input is transmitted into the first hidden layer. In that layer, image embedding process is performed. In the first hidden layer, Marr wavelet transform is applied to decompose the encrypted images into different sub-blocks for horizontal(x) and vertical (y) directions.

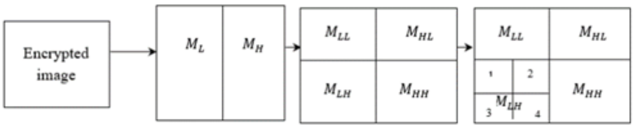


FIGURE 6 MARR WAVELET TRANSFORM BASED IMAGE DECOMPOSITION

Figure 6 illustrates the decomposition of the image using the Marr wavelet transform. The transformation process is achieved as follows:

Article Received: *25 November 2023* ***Revised:*** *12 December 2023* ***Accepted:*** *30 January 2024*

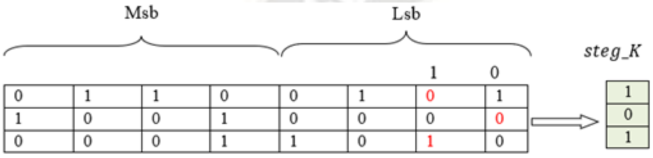
$$\varphi(t) = \frac{1}{\pi d^2}\left(1-\frac{1}{2}\left(\frac{x^2+y^2}{d^2}\right)^2\right)\exp\left(-0.5*\frac{x^2+y^2}{d^2}\right) \quad (13)$$

Where, above (13) used for normalized second derivative of a Gaussian function. From (13), $\varphi(t)$ denotes a transformation output that decomposes the input natural image at a time 't', d indicates a deviation. For the successive levels, down sampling is performed and the output of each level generates four sub blocks of pixels namelyM_{LL}, M_{HL}, M_{LH} and M_{HH} .

The stego key is used to perform the embedding process in the second hidden layer. Initially, the integer pixel values within the subblocks are transformed into binary form.

$$b = Convt(P_i) \quad (14)$$

Where, b denotes a binary representation of the pixels, $Convt$ denotes a conversion of the pixel in decimal. After the binary conversion, the least significant (Lsb) and most significant bit (Msb) are separated. Let us consider the confidential text or word in the form of bits is 001 for embedding.



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

1
0
1

Figure 7 Embedding Process

Figure 7 illustrates the embedding process to inserts each piece of confidential bit into the least significant bit of the image pixels. If the confidential bit embedded with 0th position of the Lsb, then the key value will be '0'. If the confidential bit embedded with 1th position of the Lsb, then the key value is '1'. From figure 7, the confidential bit '0' embedded in 1th position of the Lsb, then the stego key ($steg\_K$) value is '1'. The confidential bit '0' embedded in 0th position of the Lsb, then the stego key ($steg\_K$) value is '0'. The final the confidential bit '1' is embedded in 1^{th} position of the Lsb, then the stego key ($steg\_K$) value is '1'.

The embedding process is formulated as given below,

$$I_{emb} = bP_{Sub} * steg_K * b_C \quad (15)$$

Where, I_{emb} denotes an embedded image, bP_{Sub} denotes a binary representation of image pixels in sub band, $steg_K$ denotes a stego key, b_C denotes a confidential bit inserted into the image pixels. As a result, the final embedding result is obtained at output layer.

In this way, embedding process is performed and it sent to the receiver. First the receiver performs the extraction process to retrieve the encrypted image from the stegno images with similar stego key.

X. Image Extraction

In the same context, the process of retrieving the "confidential bit" from the image that has been embedded with it, using a similar stego key, is called the image extraction technique. The extraction process is obtained as follows,

$$ECI_{ext} = steg_K * bP_{Sub} \quad (16)$$

Where, ECI_{ext} denotes an extracted image, bP_{Sub} denotes a binary representation of image pixels in sub band, $steg_K$ denotes a stego key.

XI. Unsigncryption

After the image extraction, the unsigncryption is performed at receiver side to get the original image. It includes two major processes namely digital signature verification as well as decryption. First signature verification is carried out to confirm the authenticity of communication.

At the receiver side, the new signature is generated 'Sig_r' using Schmidt-Samoa cryptography. Finally, the generated signature is Sig_r' is verified with the signature 'Sig'. The receiver decrypts the ciphertext only if the two signatures are valid and match. Otherwise, the decryption is not possible.

$$CCI = ECI^{k_{fp}} \, mod \, (k_{pb}) \quad (17)$$

Where, CCI denotes a compressed chest image, ECI indicates a cipher image, k_{fp} represents receivers full private key, k_{pb}denotes a public key.

XII. Decompression

After the image decryption, the decompression performed using inverse process of the Burrows-Wheeler Hilbert linear curve transform. Finally, the decompressed image is obtained.

The algorithmic process of secure image transmission is given below,

Algorithm 3: Secured image transmission

Input: compressed image $CI_1, CI_2, CI_3 \ldots . CI_n$

Output: enhance the security

```
Begin
// Image encryption & signature generation
    1. for each compressed image $CCI_i$
    2. Generate full private key ' $k_{fp}$ ' and public key ' $k_{bp}$'
    3. Encrypt medical image using public key $\beta_E = CCI^{k_{pb}} \, mod \, k_{pb}$
    4. Generate digital signature '$Sig$'
    5. End for
// Image embedding
    6. Apply wavelet transform to decompose the image into subblocks using (13)
    7. Extract pixels in subblocks
```

```
        Convert pixels into binary representation (14)
        Separate Lsb and Msb
        Embed confidential bit into Lsb with Stego key using (15)
        Send to receiver
// Image extraction
    For each Stegno image '$SI$'
        Extract the encrypted image with similar Stego key using (16)
    End for
// Unsigncryption
    for each cipher image '$ECI$'
        Perform signature verification
        If signature is valid then
            Decrypt the image
        else
            Decryption is not performed
        end if
// Decompression
    For each compressed image $CCI$
        Perform decompression
        Apply reverse process of Burrows-Wheeler Hilbert linear curve transform
        Obtain the original chest image '$CI$'
    End for
End
```

Algorithm 3 outlines a method for secure medical image transmission between a sender and a receiver. The process starts by taking the compressed image as input. Subsequently, for key generation, encryption, and signature generation the Schmidt-Samoa cryptographic certificateless signcryption method is employed. The resulting encrypted image is then used as input for the embedding process. The extreme learning classifier, which comprises multiple layers, is responsible for analyzing the given input. The compressed image serves as the input to the initial layer, where random weights and biases are assigned. The subsequent hidden layer performs image decomposition using the Marr wavelet transform. This decomposition sets the stage for the embedding process in second hidden layer which inserts confidential data into the image pixels. Consequently, the resultant stego images are transmitted to the receiver.

Upon the reception, image extraction process is carried out at receiver side with similar stego key to retrieve the original image. Following this step, the unsigncryption process is performed to decrypt the image after the signature verification. Finally, the decompression technique is involved to bring back the original chest image. This comprehensive approach significantly enhances the security of image communication from the sender to the receiver, ensuring higher confidentiality.

XIII. EXPERIMENTAL SETUP

In this section, we perform experimental analysis of the MWTCSELS method and the existing CGST-FCM [1], and an enhanced medical image steganographic algorithm [2] using MATLAB coding. To conduct the experiment, we used medical Chest X-Ray images collected from the https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia. The chest X-ray imaging was collected as part of patients' routine clinical care. For the analysis of chest x-ray images, all chest radiographs were initially screened. The dataset consists of 5,863 X-Ray images (JPEG) and 2 categories (Pneumonia/Normal).

XIV. QUALITATIVE ANALYSIS

In Figure 8, qualitative analysis of different process of MWTCSELS is illustrated which is in this section.

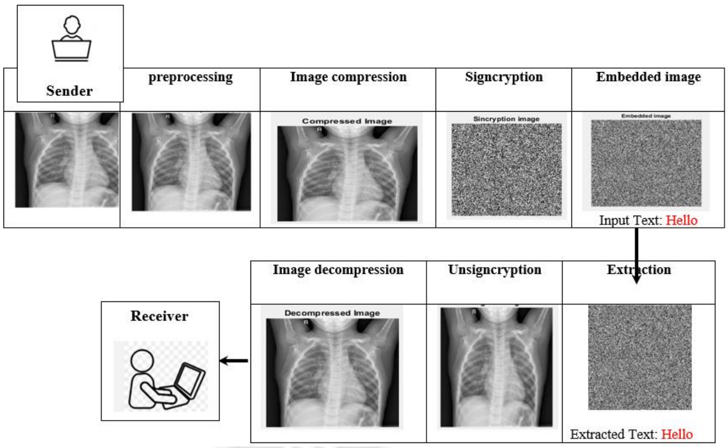


FIGURE 8 QUALITATIVE RESULTS OF MWTCSELS

The process begins by using the original medical chest X-Ray image from the dataset as input. To enhance the image contrast, Wilcox indexive myriad filtering is applied. Subsequently, the Burrows-Wheeler Hilbert linear curve transform is employed for image compression. Schmidt-Samoa cryptographic Certificateless Signcryption is used to convert the original image into a cipher image. Finally, Mar Wavelet transformed Extreme learning machine steganography is applied to embed text within the image. Upon reception, the image extraction process is conducted using the same stego key. This is followed by unsigncryption to decrypt the image. Finally, the receiver obtains the decompressed image.

XV. QUANTITATIVE ANALYSIS

The performance discussion involves three different techniques namely MWTCSELS method, the existing CGST-FCM [1], and an enhanced medical image steganographic algorithm [2]. Various performance metrics such as peak signal-to-noise ratio (PSNR), compression ratio, encryption time, confidentiality, and integrity, are evaluated across different sizes of input medical images.

XVI. IMPACT OF PEAK SIGNAL-TO-NOISE RATIO

The Peak Signal-to-Noise Ratio (PSNR) is a generally used metric in image processing to quantitatively quantity the quality of a denoised image in comparison to the original image. PSNR is calculated grounded on Mean Squared Error (MSE) between corresponding pixels of the two images. The formula for calculating PSNR is as follows:

$$PSNR = 10 \log 10 \left(\frac{L^2}{MSE}\right) \qquad (18)$$

Where, the peak signal-to-noise ratio '$PSNR$' is assessed on the basis of maximum probable pixel value 'L' and the mean square error 'MSE'

$$MSE = [DCI - CI] \qquad (19)$$

Where, the mean square error 'MSE' is evaluated based on the denoised chest images 'DCI' and the original chest image 'CI'.

TABLE 1 PEAK SIGNAL-TO-NOISE-RATIO (PSNR) COMPARISON

Image size (KB)	Peak signal-to-noise-ratio (dB)		
	MWTCSELS	CGST	Enhanced medical image steganographic algorithm
870.78	36.81	28.15	31.45
406.31	48.57	33.25	42.33
582.64	55.46	42.55	51.48
471.56	53.97	40.25	48.94
451.29	51.35	38.15	44.96
669.29	58.88	45.55	51.73
400.65	60.52	48.15	54.15
420.27	66.54	52.35	61.68
458.09	67.30	50.15	59.50
384.93	61.28	48.55	56.53

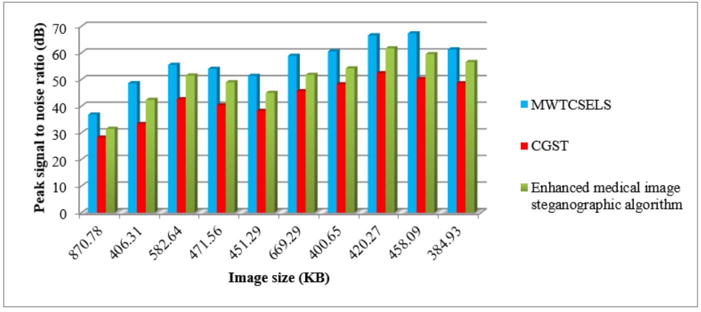


FIGURE 9 COMPARATIVE ANALYSIS OF PEAK SIGNAL-TO-NOISE-RATIO (PSNR)

Figure 9 proves the comparative analysis of the Peak Signal-to-Noise Ratio (PSNR) changes with different medical chest image sizes in kilobytes (KB). The different sizes are shown on the horizontal axis, while the associated Peak Signal-to-Noise Ratio (PSNR) outcomes are made known on the vertical axis. The results indicate that the proposed MWTCSELS method gets a higher Peak Signal-to-Noise Ratio (PSNR) related to the other two existing methods. This significant improvement is achieved through the application of the Wilcox indexive Myriad Filtering technique, which aims to minimize errors and increase the peak signal-to-noise ratio. The pixels with higher deviation from the central value, referred to as noisy pixels, are removed from the input images. This process contributes to enhance the image contrast. Upon comparing the proposed method with the existing ones, the analysis clearly demonstrates that the performance of the peak signal-to-noise ratio using the MWTCSELS technique has increased by 32% and 12% compared to the existing [1] & [2] respectively.

XVII. IMPACT OF COMPRESSION RATIO

Compression ratio is a metric used to quantify the effectiveness of a image compression algorithm in reducing the size of image. It is used for original image has been compressed without losing essential information. The size of the original uncompressed image divided by the size of the compressed image gives the compression ratio. The compression ratio is calculated mathematically as,

$$Com\_R = \left[\frac{OCI\ (KB)}{CCI\ (KB)}\right] \qquad (20)$$

Where, Com_R represents a compression ratio, $OCI\ (KB)$ shows an uncompressed chest image sizes in terms of KB, $CCI\ (KB)$is the compressed chest image sizes in terms of KB. Higher the compression ratio, the technique is more efficient.

TABLE 2 COMPARISONS OF COMPRESSION RATIO

Image size (KB)	compression ratio		
	MWTCSELS	CGST	Enhanced medical image steganographic algorithm
870.78	8.9	6.6	7.8
406.31	6.1	4.4	5
582.64	7.7	5.7	6.8
471.56	8	5.8	7.2
451.29	8.1	6.3	7.4
669.29	9.6	6.3	7.4

400.65	8.8	5.2	6.1
420.27	9.2	6.5	7.8
458.09	7.5	5	6.4
384.93	8.3	5.1	6.9

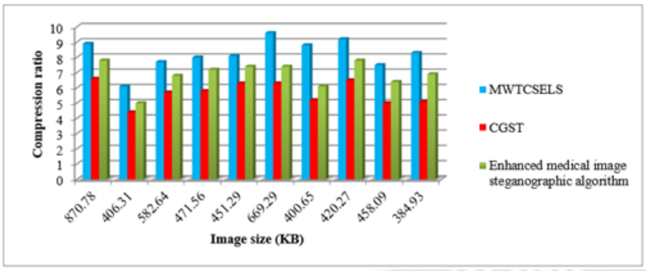


FIGURE 10 COMPARATIVE ANALYSIS OF COMPRESSION RATIO

Figure 10 illustrates the performance analysis of compression ratios for three methods namely MWTCSELS, existing CGST-FCM [1], and an enhanced medical image steganographic algorithm [2], using medical chest images of different sizes. The results obtained indicate that the MWTCSELS technique outperforms [1] and [2] in terms of compression ratio. This improvement is attributed to the application of the Burrows-Wheeler Hilbert linear curve transform. The process begins by taking a preprocessed image as input. The pixels of the input image are then mapped onto Hilbert space, converting directions into unit sequence values. This transformation finally provides the compressed images with superior compression ratios. The average results from ten iterations shows that the MWTCSELS technique strengthens the compression ratio by 45% compared to [1] and by 19% compared to [2]

XVIII. IMPACT OF EMBEDDING TIME

Embedding time is the amount of time taken by the medical image steganalysis algorithm to embed the given input cover image. The time is expressed mathematically as,

$$Emb_{time} = \sum_{i=1}^{n} CI_i[size] * Time\ [Emb] \quad (18)$$

Where, ‘ Emb_{time} ’ denotes a embedding time, ‘$CI_i[size]$’ denotes a size of the test image and the $Time\ [Emb]$ denotes a actual time consumed in the overall embedding process ‘

TABLE 3 COMPARISONS OF EMBEDDING TIME

Image size (KB)	Embedding time (ms)		
	MWTCSELS	CGST	Enhanced medical image steganographic algorithm
870.78	1.56	4.35	2.17
406.31	0.73	1.35	1.01
582.64	1.07	1.85	1.28
471.56	0.21	1.35	0.94
451.29	0.76	1.15	0.99
669.29	1.24	1.85	1.53
400.65	0.84	1.65	1.12
420.27	0.15	0.8	0.44
458.09	0.91	1.65	1.42
384.93	0.57	1.95	1.07

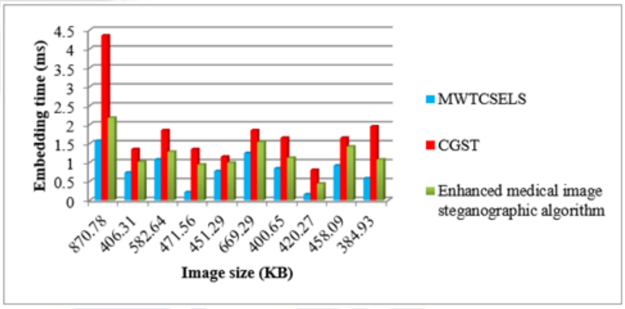


FIGURE 11 COMPARATIVE ANALYSIS OF EMBEDDING TIME

The figure 11 expresses the comparative analysis of the embedding time against various sizes of the medical images. The embedding time is not linear because of the different sizes of the images taken for simulation. In precise, the algorithm takes more time for larger size of the image and less time taken for small size of image. MWTCSELS technique performs image embedding with minimum time consumption compared to other three methods. The reason is, that the MWTCSELS technique uses Marr Wavelet transformed Extreme learning machine. The proposed cryptographic technique proficiently attains both encryption and signature generation to get the cipher medical image. From this, it is observed that the embedding time using MWTCSELS technique gets lessen by 55% compared to [1] and 37% compared to [2].

XIX. IMPACT OF CONFIDENTIALITY RATE

The confidentiality rate is achieved by dividing the number of authorized user accesses to medical images by the number of medical images provided for simulation. The confidentiality rate mathematically calculated using a formula which shown below:

$$CR = \sum_{i=1}^{n} \left(\frac{CI_{AAU}}{CI_i} \right) * 100 \quad (21)$$

Where, ‘ CR ’ denotes confidentiality rate, CI_{AAU} denotes a number of chess images accessed by authorized users based on the number of medical images’ CI_i ’ Therefore, the confidentiality rate is determined by the percentage (%).

TABLE 4 COMPARISONS OF COMPRESSION RATIO

Number of images	Confidentiality rate (%)		
	MWTCSELS	**CGST**	**Enhanced medical image steganographic algorithm**
100	95	90	92
200	94.5	87.5	90
300	94.33	85	88.33
400	93.75	83.75	86.25
500	93.6	83	85
600	92.5	81.66	84.16
700	91.42	80.71	83.57
800	90.62	80	81.87
900	88.77	78.33	80.55
1000	87	74.5	78.5

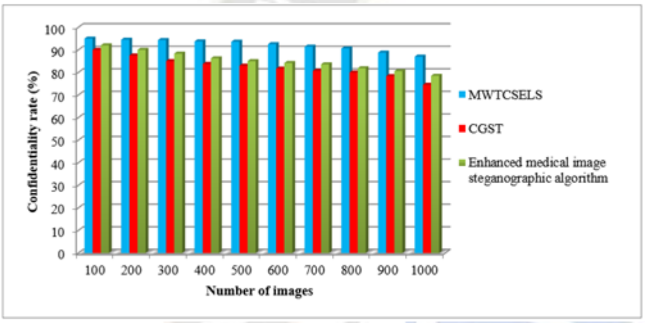


FIGURE 12 COMPARATIVE ANALYSIS OF CONFIDENTIALITY RATE

As shown in Figure 12, the confidentiality rates of three methods are depicted with varying numbers of input medical chest images. The results show that MWTCSELS gets a higher confidentiality rate than the other methods [1] [2]. This improvement is attained by using the Schmidt-Samoa cryptographic certificateless signcryption method to encrypt the input image and generate a signature. The sender then transmits the encrypted images and signature to the receiver. Subsequently, when the user accesses their data, the signature is verified first. Upon valid signature verification, the authorized receiver performs decryption to retrieve the original image. This process significantly enhances confidentiality. The comparison of ten results demonstrates that the confidentiality rate of MWTCSELS is enhanced by 12% compared to [1] and by 8% compared to [2].

XX. IMPACT OF INTEGRITY RATE

The integrity rate is a security parameter calculated by the ratio of the number of medical images that are not modified by any unauthorized users to the total number of medical images. The formula for calculating the integrity rate is provided below:

$$IR = \sum_{i=1}^{n} \left(\frac{CI_{na}}{CI_i}\right) * 100 \quad (22)$$

Where, IR shows an integrity rate, CI_{na} shows a number of medical images that were not changed by malicious users, and the total number of medical images 'CI_i'. The data integrity is measured as percentage (%).

TABLE 5 COMPARISONS OF INTEGRITY RATE

Number of images	Integrity rate (%)		
	MWTCSELS	**CGST**	**Enhanced medical image steganographic algorithm**
100	94	74	85
200	93.5	73	84
300	93.33	70	83.33
400	91.25	69.75	83
500	91	69.2	82
600	89.16	69.16	80.83
700	88.85	67.85	80
800	88.12	66.87	79.62
900	87.22	65	79.44
1000	86.5	63.8	78.5

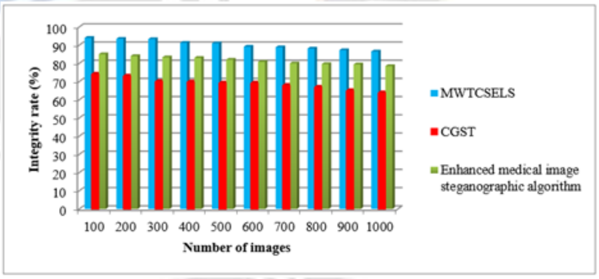


FIGURE 13 COMPARATIVE ANALYSIS OF INTEGRITY RATE

Figure 13 illustrates the performance analysis of the integrity rate in relation to three distinct methods namely MWTCSELS, the existing CGST-FCM [1], and an enhanced medical image steganographic algorithm [2]. The integrity rate is achieved through the MWTCSELS technique than the existing methods. This is due to the reason that the medical images that have not been altered or changed by any malicious users using MWTCSELS technique. The proposed technique involves a two-step process. Initially, the Schmidt-Samoa cryptographic Certificateless Signcryption method is employed to encrypt the input image. Subsequently, the Mar Wavelet Transformed Extreme Learning Machine is utilized to embed confidential data into the image using a Stego key. The resultant Stego images are then transmitted to the recipient. Upon reception, an extraction process is conducted to restore the original images from the Stego images. Followed by, an unsigncryption process is employed to retrieve the medical image with enhanced security. This approach increased the integrity rate by 31% compared to [11] and an 11% improvement compared to [2], respectively.

XXI. Conclusion

The security of digital image transmission, which contains a lot of sensitive information, is a challenge in the open internet network where computer and information technology are advancing rapidly. In this paper, novel image steganographic algorithm referred to as MWTCSELS is designed to effectively preserve the sensitive information within images. The process begins from preprocessing the medical images, aiming to reduce noise and enhance the Peak Signal-to-Noise Ratio (PSNR) subsequently. To optimize storage space during wireless network transmission, the algorithm utilizes a Burrows-Wheeler Hilbert linear curve transform-based image compression technique. The compressed images are then encrypted and embedded using a Mar Wavelet Transformed Extreme Learning Machine with a stego key. These processed images are subsequently transmitted through the network to the receiver. An authorized user can reconstruct the original image by employing the shared stego key. The ciphered images are decrypted using the appropriate key to retrieve the original medical image in a secure manner. The performance of the proposed method is compared and assessed with other methods using chest X-ray images and different measures such as Peak Signal-to-Noise Ratio (PSNR), compression ratio, embedding time, confidentiality, and integrity that evaluate the quality and security of the image. Experimental outcomes expressed that the proposed MWTCSELS algorithm guarantees security, and delivers high-quality performance in the transmission of medical images.

References

[1] Chandrashekhar Meshram, Agbotiname Lucky Imoize, Sajjad Shaukat Jamal, Adel R. Alharbi, Sarita Gajbhiye Meshram, Iqtadar Hussain, “CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps”, IEEE Access Volume 10, 2022, Pages 39853 – 39863. **DOI:** 10.1109/ACCESS.2022.3165565

[2] Mostafa A. Ahmad, Mourad Elloumi, Ahmed H. Samak, Ali M. Al-Sharafi, Ali Alqazzaz, Monir Abdullah Kaid, Costas Iliopoulos, “Hiding patients’ medical reports using an enhanced wavelet steganography algorithm in DICOM images”, Alexandria Engineering Journal, Elsevier, Volume 61, Issue 12, December 2022, Pages 10577-10592. https://doi.org/10.1016/j.aej.2022.03.056

[3] Yu-Guang Yang, Bo-Wen Guan, Yi-Hua Zhou & Wei-Min Shi, “Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach”, Multimedia Tools and Applications, Springer, Volume 80, 2021, Pages 691–710. https://doi.org/10.1007/s11042-020-09779-5

[4] Jing-Yi Dai, Yan Ma & Nan-Run Zhou, “Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map”, Quantum Information Processing, Springer, Volume 20, 2021, Pages 1-24. https://doi.org/10.1007/s11128-021-03187-w

[5] C. Thirumarai Selvi a, J. Amudha, R. Sudhakar, “A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission”, Biomedical Signal Processing and Control, Elsevier, Volume 66, April 2021, Pages 1-13. https://doi.org/10.1016/j.bspc.2021.102465

[6] Ji Xu, Jun Mou, Jian Liu & Jin Hao, “The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system”, The Visual Computer, Springer, Volume 38, 2022, Pages 1509-1526, https://doi.org/10.1007/s00371-021-02085-7

[7] Walid El-Shafai, Iman Almomani, Anees Ara & Aala Alkhayer, An optical-based encryption and authentication algorithm for color and grayscale medical images”, Multimedia Tools and Applications, Volume 82, 2023, Pages 23735-23770. https://doi.org/10.1007/s11042-022-14093-3

[8] Osama Fouad Abdel Wahab; Ashraf A. M. Khalaf; Aziza I. Hussein; Hesham F. A. Hamed, “Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques”, IEEE Access, Volume 9, 2021, Pages 31805 – 31815. **DOI:** 10.1109/ACCESS.2021.3060317

[9] Hussah N. AlEisa, “Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things”, Journal of Healthcare Engineering, Hindawi, Volume 2022, May 2022, Pages 1-11. https://doi.org/10.1155/2022/7528583

[10] Xuan Liu, Lu Zhang, Zihao Guo, Tailin Han, Mingchi Ju, Bo Xu, and Hong Liu, “Medical Image Compression Based on Variational Autoencoder”, Mathematical Problems in Engineering, Hindawi, Volume 2022, December 2022, Pages 1-12. https://doi.org/10.1155/2022/7088137

[11] Anirban Sengupta, Mahendra Rathor, “Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging

Systems", IEEE Access, Volume 8, 2020, Pages 6543 – 6565. **DOI:** 10.1109/ACCESS.2019.2963711

[12] Yaomin Wang, Zhanchuan Cai, Wenguang He, "High-Capacity Reversible Data Hiding in Encrypted Image Based on Intra-Block Lossless Compression", IEEE Transactions on Multimedia, Volume 23, 2020, Pages 1466 – 1473. **DOI:** 10.1109/TMM.2020.2999187

[13] Xiaoling Huang, Youxia Dong, Hongyong Zhu, Guodon g Ye, "Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image", Alexandria Engineering Journal, Elsevier, Volume 61, Issue 10, October 2022, Pages 7637-7647. https://doi.org/10.1016/j.aej.2022.01.015

[14] Jianhua Yang, Fei Shang, Yi Liao, and Yifang Chen, "Toward High Capacity and Robust JPEG Steganography Based on Adversarial Training", Security and Communication Networks, Hindawi, Volume 2023, February 2023, Pages 1-12. https://doi.org/10.1155/2023/3813977

[15] Roseline Oluwaseun Ogundokun and Oluwakemi Christiana Abikoye, "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography", International Journal of Digital Multimedia Broadcasting, Hindawi, Volume 2021, March 2021, Pages 1-8. https://doi.org/10.1155/2021/8827055

[16] Ghazanfar Farooq Siddiqui, Muhammad Zafar Iqbal, Khalid Saleem, Zafar Saeed, Adeel Ahmed, Ibrahim A. Hameed, And Muhammad Fahad Khan, "A Dynamic Three-Bit Image Steganography Algorithm for Medical and e-Healthcare Systems", IEEE Access, Volume 8, 2020, Pages 181893 – 181903. **DOI:** 10.1109/ACCESS.2020.3028315

[17] Sachin Dhawan, Chinmay Chakraborty, Jaroslav Frnda, Rashmi Gupta, Arun Kumar Rana, And Subhendu Kumar Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT", IEEE Access, Volume 9, 2021, Pages 87563 – 87578. **DOI:** 10.1109/ACCESS.2021.3089357

[18] Hamidreza Damghani, Farshid Babapour Mofrad, Leila Damghani, "Medical JPEG image steganography method according to the distortion reduction criterion based on an imperialist competitive algorithm", IET image processing, Wiley, Volume 15, Issue 3, 2021, Pages 705-714. https://doi.org/10.1049/ipr2.12055

[19] A. Karawia, "Medical image steganographic algorithm via modified LSB method and chaotic map", IET image processing, Wiley, Volume 15, Issue 11, 2021, Pages 2580-2590. https://doi.org/10.1049/ipr2.12246

[20] Faiza Al-Shaarani, Adnan Gutub, "Securing matrix counting-based secret-sharing involving crypto steganography", Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 34, Issue 9, 2022, Pages 6909-6924. https://doi.org/10.1016/j.jksuci.2021.09.009