International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8183
***Article Received:** 29 June 2023 **Revised:** 26 August 2023 **Accepted:** 08 September 2023*

Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption for Secure Image Transmission

J. Shaik Dawood Ansari[1], Dr. P. Tamilselvan[2]
[1]Research Scholar, Department of CS,
Karpagam Academy of Higher Education, India.
e-mail: jsdansari@gmail.com
[2]Research Supervisor, Department of CS,
Karpagam Academy of Higher Education, India.
e-mail: tamilselvancs@kahedu.edu.in

Abstract— Present-day evolution in communication and information technology dispenses straightforward and effortless access to data, but the most noteworthy condition is the formation of secure communication. Numerous approaches were designed for safety communication. One of the crucial approaches is image steganography. Moreover, provisioning of information security services is arrived at via cryptosystems where cryptosystems make certain the secure messages transmission between the users in an untrustworthy circumstance. The conventional method of providing encryption and signature is said to be first signing and then encryption, but both the computation and communication costs are found to be high. A certificateless signcryption mechanism is designed to transfer the medical data or images securely. This mechanism will minimize the storage and verification costs of public key certificates. The author of this article proposes a method named Lagrangian recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption for transferring the medical data or images securely. In two sections the LRS-HECS method is split. They are medical image steganalysis and certificateless signcryption. First with the Chest X-Ray images obtained as input, a Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model is applied to generate steg images. Second, to transfer the medical images securely the steg images provided as input is designed a model named a Hyper Elliptic Curve-based Certificateless Signcryption. The issue of providing the integrity and validity of the transmitted medical images and receiver anonymity is addressed by the application of Hyper Elliptic Curve. Chest X-Ray pictures were used in experimental simulations, and the findings showed that the LRS-HECS approach had more advantages over existing state-of-the-art methods in terms of higher peak signal to noise ratio with data integrity and with reduced encryption time and transmission cost.

Keywords-: Image Steganography, Codeword Correlated, Lagrangian, Recurrent Neural Network, Certificateless Signcryption.

I. INTRODUCTION

Electronic medical records and electronic commerce have greatly safeguarded from the use of content extraction signatures since the signature verifier can validate the extracted message's validity without having a thorough understanding of the signed message. Competence and privacy protection are crucial elements for secure transmission when it comes to the content extraction signature. The majority of content extraction signature techniques, however, were created using the traditional public key cryptosystem. Several customers have moved to certificateless signcryption over the past few years since no certificate is required, which solves the certificate management problems associated with traditional public key encryption. Binary classification model based on artificial neural networks was proposed in [1] for detecting the presence of LSB steganography on monochromatic still images. In this method the payload was differentiated between 0.1 and 0.5 for producing the steganograms with which image pairs of carriers and steganograms were acquired. With each steganogram as input, extracted features were standard deviation, kurtosis, range, skewness, median, complexity. As a result, the classification accuracy was said to be improved with better sensitivity, specificity and precision.

Despite advancements in sensitivity, specificity, and precision, the peak signal-to-noise ration and encryption time involved in image steganography was not focused. To address on these two-performance metrics, in our work, Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model is designed.

In [2], a method named, Fractional Chaotic Maps (FCM) for group-oriented signcryption (CGST), CGST-FCM was proposed. The CGST-FCM method's key feature was that any group signcrypter may encrypt the data through the group manager (GM). Using the public circumstances of the group, this deduced the legitimacy of signcrypted information. Nevertheless, they lacked the capability to link it to the signcrypter. As a result, only legitimate sign-encrypted data were claimed to be produced by the GM alone.

The GM also had the potentiality in divulging the signcrypted identity in case of difference of opinion. As a result, security was said to be guaranteed with minimum resource. However, the above method relies on complicated cryptographic methods and hence has high communication costs. To address this issue and also to improve data integrity rate, Hyper Elliptic Curve-based Certificateless Signcryption model is proposed that necessitates not only less computing power but also enhances the data integrity rate significantly.

Denoising Autoencoder and Local Binary Pattern (LBP) Operator integration was proposed as a unique technique for finding payload regions in stego images in [3]. Here, the Denoising Autoencoder was used to evaluate the cover image from the input stego image by understanding the associations between image pixels. Also, it was discovered that the LBP operator has the capacity to find local correlations inside neighborhood coordinates. The accuracy then increased as a result of this. Nonetheless, it is believed that maintaining security is a difficult process.

An image steganography method employing integration of several algorithms with encryption utilizing Binary bit-plane decomposition (BBPD) and adaptive embedding using Salp Swarm Optimization Algorithm (SSOA) were proposed in [4]. Finally, a hybrid Fuzzy Neural Network in addition to backpropagation learning was utilized in improving the stego image quality.

Over the past few years works in steganography have the threat of secret images being retrieved by malicious user. In [5], the cover image was split into distinct RGB components separately. Followed by which Multilevel Discrete Wavelet Transform (DWT) was applied to transformed image components. With this the error rate was found to be reduced in addition to the provisioning of security.

A means for security was also ensured in [6] by eliminating the introduction of third party via integration of particle swarm optimization and hash function. With this type of integration resulted in secured updating and sharing of medical information. However one of the biggest problems with steganography is still how to conceal a lot of sensitive information from an attacker.

The Color and Spacing Normalization Steganography (CSNTSteg) approach was developed in [7] with the aim of resolving the low capacity and invisibility problems that text steganography encounters. The conventional approaches described above in the literature have several disadvantages, such as longer encryption times, lower peak signal-to-noise ratios, and worse data confidentiality. Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS), a technique for secured medical image communication, is suggested to overcome the above-mentioned issues.

1.1 CONTRIBUTIONS

The main benefit of the suggested LRS-HECS approach is described in more detail below.

- A unique method named Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) is created to improve the security of medical image transmission. It uses the Codeword Correlated Lagrangian Recurrent Neural Network for image steganalysis and Hyper Elliptic Curve-based Certificateless Signcryption to generate steg signcrypted image in the central repository. The original rebuilt image is then obtained at the receiver side using a deep learning-based image decryption process.
- In the process of image steganalysis, the hidden layer of a recurrent neural network employs the Codeword Correlated Lagrangian function to divide and store the steg images into four separate blocks and make them available to four different users. As a result, the PSNR is enhanced and the performance of mean square error is decreased.
- To propose Hyper Elliptic Curve-based Certificateless Signcryption model that circumvents from the key escrow issue. The Hyper Elliptic Curve exploits the advantages of utilizing an 80-bit key size and hence warrants the security features.
- The proposed method is efficient specifically in terms of PSNR, encryption time, data integrity rate, and communication cost, according to a comparison with relevant state-of-the-art technologies.

1.2 ORGANIZATION OF THE PAPER

The article's synopsis is structured as follows: Section 2 elaborates on related efforts in the fields of certificateless signcryption and image steganalysis. In Section 3, the proposed Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) for secured medical image transmission is described in detail with figurative representation and algorithms. Sections 4 and 5 present experimental results and performance evaluations of the qualitative and quantitative analysis of medical images. In Section 6, a succinct conclusion is made.

II. RELATED WORKS

Images are easily acquired in the modern era using digital cameras, camcorders, and scanners. With these obtained images are said to be transmitted by means of several social media sites. In addition, due to the plethora of effortlessly attainable images online, sharing of information has also become straightforward. Nevertheless, image transmission can result in several drawbacks like, authentication, copyright violation, privacy, and so on.

A new encryption with image steganography model was designed in [8] with the purpose of ensuring security. However, the study has inferred that the existing method however incurred certain amount of security issues. Hence, an efficient secure image encryption technique was presented in [9]. With this not only security was ensured but with minimum time.

A review of mechanisms for performing image steganography concerning medical information was elaborated in [10]. Yet another survey of application of cryptography mechanism using neural networks was investigated in [11]. A secure cryptography-based medical image reclamation method integrating discrete cosine transform, steganography, and watermarking was presented in [12]. By means of integration the method was not only found to be robust but was also found to be hard stolen from malicious users. State-of-the-art methods on security and privacy in healthcare domain were investigated in [13].

Several types of multi-message and multi-receiver signcryption methods have been initiated by employing the conventional public key cryptography in order to securely communicate countless various health information observed by numerous different sensors to numerous subsequent healthcare users. This solution still faces problems with key escrow and certificate management, though. An effective multi-message and multi-receiver anonymous certificate-based signcryption method for healthcare was developed in [14] to address this issue.

To overcome the key escrow issue and offer data privacy, certificate-based encryption was combined with elliptic curve cryptography in this instance.

Over the past few years several CNN based steganography methods were presented with the purpose of enhancing the detection accuracy. A novel CNN architecture was presented in [15] that consisted of filter bank-based preprocessing depth-wise based feature extraction and finally separable convolutional layers for producing output image. With this the classification accuracy was found to be improved. On the other hand, the error involved at the steg process was not focused. A secured model built on deep learning was developed in [16] to address this problem. However, the communication cost performance metric was not focused. To concentrate on this aspect, certificateless signcryption scheme was proposed in [17].

A neural reversible steganography mechanism was presented in [18] employing long short-term memory to both improve the accuracy rate and concentrate on rate distortion. In [19], threshold signcryption was combined with certificateless cryptosystem with the purpose of ensuring a secure and significant secret sharing mechanism. Yet another certificateless signcryption method based on Elliptic Curve Discrete Logarithm was presented in [20] for secure data transmission.

III. METHODOLOGY

With the aim of enhancing the medical image steganalysis process and so ensuring safe transmission, the Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) method is proposed in this section. The suggested LRS-HECS method's structure is depicted in Figure 1.

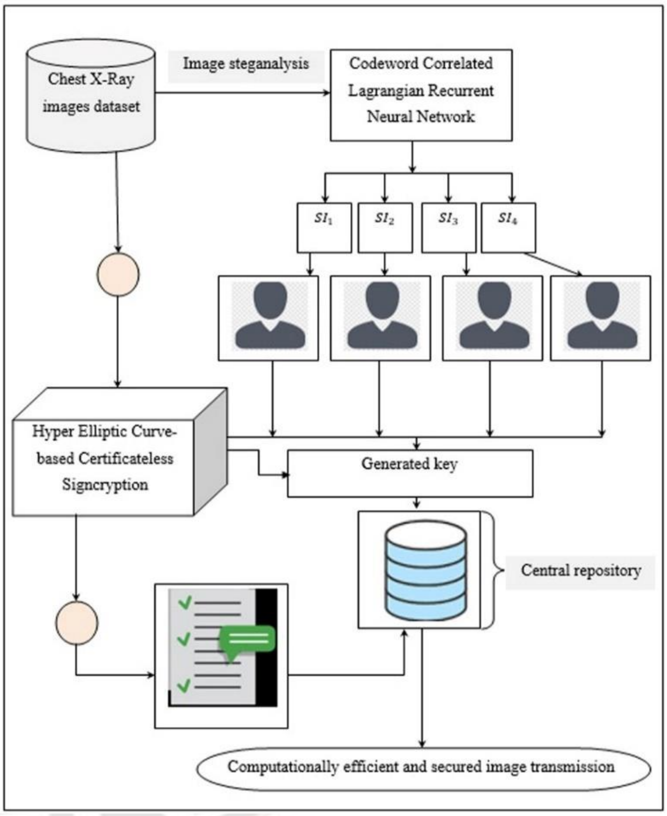

Chest X-Ray images dataset
Image steganalysis
Codeword Correlated Lagrangian Recurrent Neural Network
SI_1
SI_2
SI_3
SI_4
Hyper Elliptic Curve-based Certificateless Signcryption
Generated key
Central repository
Computationally efficient and secured image transmission

Figure 1 Block diagram of Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption method

The proposed LRS-HECS approach is divided into three sections, as seen in the above image. These are validation, certificateless signcryption, and image steganalysis. First, with the input medical images obtained from Chest X-Ray images dataset, Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model is applied. Here, the input cover image is split into four blocks and each block is encrypted separately, wherein, the encrypted blocks are sent to four different users.

Second, with the steg images acquired in the four blocks as input, Hyper Elliptic Curve-based Certificateless Signcryption is applied wherein the generated keys are concatenated and stored in the central repository. Finally, validation is performed in the central repository for secured medical image transmission. The detailed description of Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) for secured medical image transmission is presented in the parts that follow the initial description of the dataset.

1.3 DATASET DESCRIPTION

The Chest X-Ray photos from https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia were the dataset used in our work. The dataset is organized into three unique folders, titled training dataset, testing dataset, and validation dataset, respectively. Also, the collection includes subfolders for each image type (Pneumonia/Normal), totaling 5,863 X-Ray images (JPEG) from two different categories. The pediatric patients' retrospective cohorts from the Guangzhou Women and Children's Medical Center, in Guangzhou, were used to get the anterior and posterior chest X-ray pictures.

All chest radiographs were screened for quality control before being used for analysis of the chest X-ray images as part of the patients' routine clinical care. We eliminated all of the low-resolution images. Then, prior to the clearance process for AI training, two distinct expert doctors graded the image diagnostic. In addition, a third expert was engaged in to account for grading errors and evaluation.

1.4 CODEWORD CORRELATED LAGRANGIAN RECURRENT NEURAL NETWORK-BASED IMAGE STEGANOGRAPHY MODEL

Automatically generating high-quality medical images has always been complicated tasks owing to its high coding potentiality. Over the past few years, with the tremendous employment of recurrent neural network in image steganography, there have been an increasing numbers of secure medical image transmissions. In our work, a Codeword Correlated Recurrent Neural Network model is employed in embedding codeword to input images and then utilize Recurrent Neural Networks to generate steg images based on this input vector. Figure 2 shows the structure of Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model.

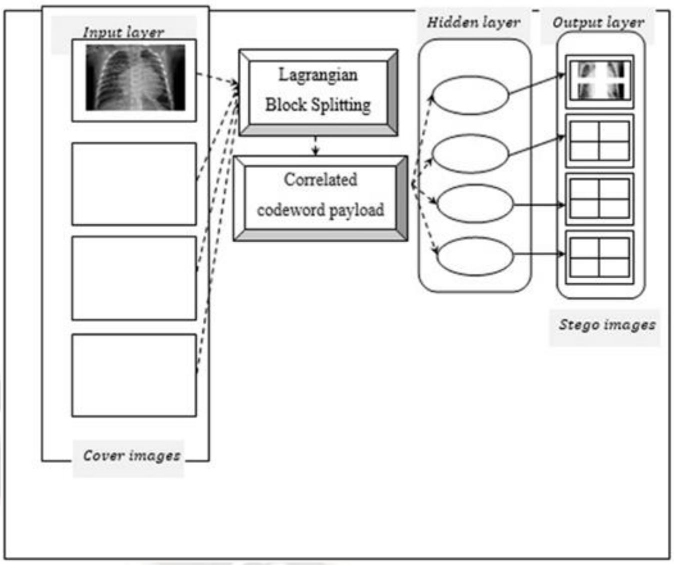


Figure 2 Structure of Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model

As shown in the above figure, the significant terms utilized in Codeword Correlated Recurrent Neural Network-based image steganography model are cover images, payload, stego image and embedding capacity. The chest images 'CI' (i.e., chest cover image) is first divided into blocks Blk = Blk$_1$, Blk$_2$, Blk$_3$, Blk$_4$' using the Chest X-Ray images dataset that is provided as input. The cover image in our work is the Chest X-Ray images which are utilized to hide the secret message using recurrent neural network-based embedding algorithm. In our work four blocks are employed for generating steg images.

Second, each block is encrypted separately utilizing recurrent neural network-based embedding algorithm and sent to four different users. The secret message utilized for hiding is referred as the payload. The Chest X-Ray cover image after embedding this payload is called as the Chest X-Ray stego image. The embedding capacity on the other hand is referred to as the maximum bits embedded in the Chest X-Ray cover image (i.e., bits per pixel (bpp)). Finally, the encrypted blocks are sent to four users.

The primary characteristic of a Recurrent Neural Network is that the network comprises of a feedback association during iteration, so that it can be broadened on the basis of the time factor, therefore resulting in a deep neural network in time dimension. Initially, the Chest X-Ray stego images are obtained as input and with only one hidden layer is mathematically stated as given below.

$$CI = [CI_1, CI_2, \dots, CI_n] \quad (1)$$
$$H_r = f_r(W_H . CI_r + U_r . H_{r-1} + B_H) \quad (2)$$

From the above equations (1) and (2), 'CI_r' represents the input vector of the '$r-th$' iteration, 'H_r' denoting the hidden layer, ‘W’, ‘U’ and ‘B’ denoting the learned weight and bias matrices utilizing softmax function ‘$fr\,()$’ respectively. With the Chest X-Ray cover image ‘CI’ obtained as input from the dataset ‘DS’, Lagrangian Block Splitting function is applied based on the proximity ‘Prox’. With this proximity function, the Chest X-Ray cover image ‘CI’ are split into ‘b’ blocks, where ‘$b = 4$’ by employing the Lagrangian Block Splitting function. This is mathematically stated as given below.

$$Blk = Prox_{\delta}\left[\left(H_r{}^{n-1} - \delta\nabla f\left(H_r{}^{n-1}\right)\right)\right] \qquad (3)$$

From the above equation (3), Chest X-Ray cover image ‘CI’ present in the hidden layer ‘H_r’ is split into blocks ‘Blk’ based on the proximity function. Here, the proximity function refers to more similar pixels are said to be in proximity than the dissimilar pixels. With the resultant Chest X-Ray cover image split into four blocks, each block are applied with the payload employing correlated codeword function separately. Let us consider ‘〖CW〗_ij’ as the ‘i-th’ codeword at pixel ‘j’ in the chest images ‘CI’ acquired from the dataset ‘DS’, where ‘j ∈ [1,t]’ and ‘t’ represents the time duration. So, the correlated codeword are mathematically stated as given below.

$$Emb = Blk_b\left[Prob\,\left(CW_{ij} = a \ \&\ CK_{kl} = b\right)\right], \forall\, i,k \in [1,n], \forall\, j,l \in [1,t] \qquad (4)$$

From above equation (4), probability of correlated codeword ‘Prob (CW)’ for image transmissions are obtained from codebook set ‘CB’. To obtain a codeword for chest image, correlation is determined. As given in the above equation, when both the left and right sides of the equation are not same, then some amount of correlation is said to exist between given images and vice versa. Higher amount of imbalance of both the left and right sides refers to higher correlation. Based on higher correlation factor, the codeword for each input chest images are introduced as payload. Accordingly, each block is applied with the payload employing correlated codeword function. Finally, the encrypted blocks or the stego images are provided to four different users in the output layer as given below.

$$Y_r = f_O(W_O . Emb_r + B_O) \qquad (5)$$

From the above equation (5), the output vector ‘Y’ at the ‘$r - th$’ iteration is obtained based on the ‘W’ and ‘B’ denoting the learned weight and bias matrices utilizing softmax function ‘$fO\,()$’ respectively. Shown below is a pseudocode representation of image steganography based on Codeword Correlated Lagrangian Recurrent Neural Networks.

Input: Dataset ‘DS’, Chest Images (i.e., Chest X-Ray cover image) ‘CI=(CI)$_1$,(CI)$_2$,⋯,(CI)$_n$’

```
Input: Dataset ‘DS’, Chest Images (i.e., Chest X-Ray cover image) ‘CI=(CI)1,(CI)2,⋯,(CI)n’
Output: Computationally-efficient and noise-improve image steganography
1: Initialize blocks ‘b=4’
2: Begin
3: For each Dataset ‘DS’ with Chest X-Ray cover image ‘CI’
//input layer
4: Obtain Chest Images ‘CI’ as input given in equation (1)
//Hidden layer
5: Evaluate hidden layer as given in equation (2)
//splitting input chest image into blocks obtained from hidden layer
6: Perform block operation as given in equation (3)
//perform payload operation using correlated codeword function
7: For each block ‘Blk’
8: Perform embedding as given in equation (4)
//output layer
9: Evaluate the output layer or obtain stego images as given in equation (5)
10: Return four stego images to four users
11: End for
12: End for
13: End
```

Algorithm 1 Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography

According to what was stated above, the peak signal-to-noise ratio and encryption time involved in image steganography are intended to be improved by the Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography algorithm. As mentioned previously, there are three layers involved: input layer, concealed layer, and output layer. First, with the Chest X-Ray images obtained as input (i.e., the cover image), each input image in the input layer is obtained as vector. The cover images are then split into blocks by employing Lagrangian Block Splitting function. For each cover image, four blocks are separated due to the proximity-based function, which is supposed to increase the peak signal-to-noise ratio because the Lagrangian Block Splitting function can denoise the blocks as they are split. Next, correlated codeword is used for encrypting each block and the stego images are then sent to four different users (i.e., from single Chest X-Ray cover image) via the output vector or output layer. With this as the stego images are obtained separately for each block, the encryption time is said to be reduced significantly.

1.5 HYPER ELLIPTIC CURVE-BASED CERTIFICATELESS SIGNCRYPTION MODEL

The suggested method employs Hyper Elliptic Curve-based Certificateless Signcryption for medical image encryption after the steganalysis procedure is completed successfully. Using public-key cryptography, the Hyper Elliptic Curve-based Certificateless Signcryption concurrently accomplishes digital signature and encryption. The Hyper Elliptic Curve-based Certificateless Signcryption Model's block diagram is shown in Figure.

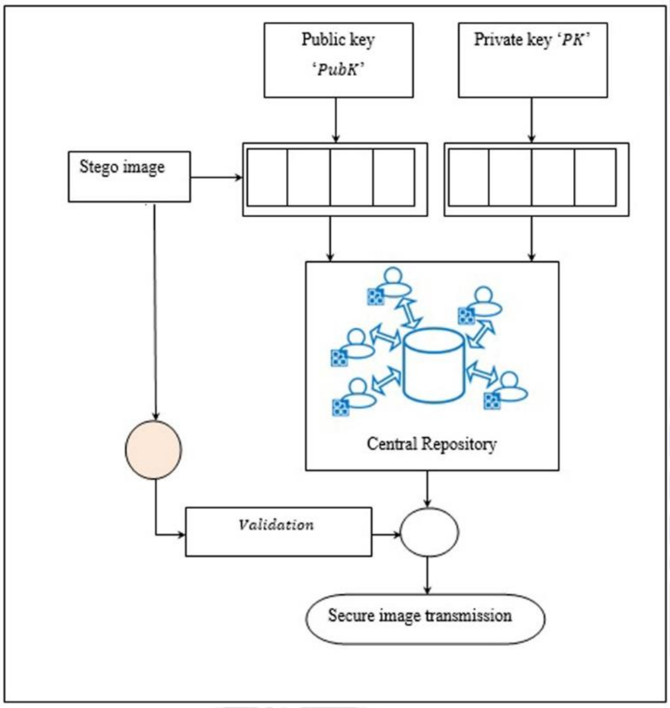


Figure 3 Block diagram of Hyper Elliptic Curve-based Certificateless Signcryption model

The stego images (four blocks for single cover images) collected as input are used to construct the public key and private key for the associated stego images, as shown in the above figure (i.e., public and private key generated separately for four different blocks). The steo images and the keys generated for each block are stored in the central repository. Finally, during the validation condition checking is performed to ensure secure medical image transmission.

Initially, for 'n' different Chest X-Ray cover image that obtains four stego images and provides to four distinct users, Hyper Elliptic Curve is utilized with a curve of genus 'g>1' or the number of input images that can be utilized for processing. Then, the Hyper Elliptic Curve for 'n' different Chest X-Ray cover image is mathematically represented as given below.

$$f(CI) = y^2 + h(CI)\, y \qquad (6)$$

From the above equation (6), '$h(CI)$' represents the polynomial of degree '$n = 2g + 1 > 4$' with 'n' different roots and '$h(CI)$' denoting the polynomial of degree '$< g + 2$'. With the required numbers of stego images for the input Chest X-Ray cover image generated using the Hyper Elliptic Curve in the key generation processes, key pairs are generated for encryption and signature with the objective of enhancing secured image transmission. The Hyper Elliptic Curve-based Certificateless Signcryption model consists of, setup, partial private key generation, full private key generation, encryption, and signature generation. To start with setup acquires a security parameter as input 'SP' that in turn generates the parameters 'param' and access key 'ak'

$$Setup\ (SP) \rightarrow (param, ak) \qquad (7)$$

From the above equation (7), the parameters '$param$' are said to be available publicly whereas the access key 'ak' is retained in a secret manner. Second, with the parameters '$param$' and the user identity 'ID' as input, user key 'UK' is generated as given below.

$$UK(param, ID) \rightarrow (PV, SV) \qquad (8)$$

From the above equation (8), a pivotal value 'PV' and an equivalent shared value 'SV' are returned as output. Third, using parameters '$param$', user identity 'ID', access key 'ak' and shared value 'SV', partial private key is extracted as given below.

$$PPK \rightarrow Extract(param, ak, ID, SV) \qquad (9)$$

With the extracted partial private key 'PPK' as obtained in the above equation (9) results, the actual private key is mathematically formulated as given below.

$$PK \rightarrow Extract\ (param, PV, PPK) \qquad (10)$$
$$PubK \rightarrow Extract\ (param, PV, PPK, SV) \qquad (11)$$

With the obtained actual private key 'PK' and the actual public key '$PubK$' from equations (10) and (11), the signcryption function performed separately for four different users are given below.

$$Steg_1U_1(PK_1, PubK_1) \rightarrow Sig\ [U_1] \qquad (12)$$
$$Steg_2U_2(PK_2, PubK_2) \rightarrow\ Sig\ [U_2] \qquad (13)$$
$$Steg_3U_3(PK_3, PubK_3) \rightarrow\ Sig\ [U_3] \qquad (14)$$
$$Steg_4U_4(PK_4, PubK_4) \rightarrow\ Sig\ [U_4] \qquad (15)$$

From the above equations (12), (13), (14) and (15), the steg images '$Steg_1$', '$Steg_2$', '$Steg_3$' and '$Steg_4$' for each users '$U1$', '$U2$', '$U3$' and '$U4$' are concatenated with the keys '$(PK, PubK)$' to produce the final output. The resultant final output is stored in the central repository for further validation process. Only upon the successful validation, the desteg images are obtained as output, therefore ensuring secured image transmission. The pseudo code representation of Hyper Elliptic Curve-based Certificateless Signcryption is given below.

Input: Dataset 'DS', Chest Images (i.e., Chest X-Ray cover image) '$CI = CI_1, CI_2, \ldots, CI_n$'

Output: Robust data confidential-based Certificateless signcryption

```
Initialize four stego images to four users (i.e., for each single Chest X-Ray cover image)
Initialize parameters '$param$'
Begin
  For each Dataset '$DS$' with Chest X-Ray cover image '$CI$'
    Formulate Hyper Elliptic Curve for '$n$' different Chest X-Ray cover image as given in equation (6)
    Formulate setup function as given in equation (7)
    Generate user key as given in equation (8)
    Generate partial-private key as given in equation (9)
    Generate private key and public key as given in equations (10) and (11)
    Concatenate steg images with the keys to produce the signcrypt form for each user or block as given in equations (12), (13), (14) and (15)
    //Validation for desteg
    If '$Steg_1 U_1(PK_1, PubK_1)$ && $Steg_2 U_2(PK_2, PubK_2)$ && $Steg_3 U_3(PK_3, PubK_3)$ && $Steg_4 U_4(PK_4, PubK_4) = CI$ '
      Then validation is successful
      Desteg the image
      Perform secure medical image transmission
    End if
    If '$Steg_1 U_1(PK_1, PubK_1)$ && $Steg_2 U_2(PK_2, PubK_2)$ && $Steg_3 U_3(PK_3, PubK_3)$ && $Steg_4 U_4(PK_4, PubK_4) <> CI$ '
      Then validation is not successful
      Continue with other set of medical image
    End if
  End for
End
```

Algorithm 2 Hyper Elliptic Curve-based Certificateless Signcryption

Hyper Elliptic Curve-based Certificateless Signcryption is designed with the goal of increasing the data integrity rate with the least amount of communication expense, as stated in the above algorithm. Here, by first constructing a Hyper Elliptic Curve for each medical image provided as input, the communication cost incurred during the signcryption process is said to be improved. Next, with the purpose of increasing the data integrity rate, Certificateless Signcryption mechanism using Hyper Elliptic Curve is formulated for each block (i.e., each user possessing four distinct stego images for each cover image). This formulation claimed that medical images that had not been altered by unauthorized users had been improved, greatly boosting the data confidentiality.

IV. EXPERIMENTAL SETUP

The experimental analysis of the Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) method and Binary classification model based on artificial neural networks [1] and CGST-FCM [2] method are performed. We used MATLAB coding with medical images obtained from Chest X-Ray images dataset collected from the https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia. Ten photos with different sizes are taken into consideration for the experiment in order to do statistical evaluation with a wide range of input parameters.

4.1 QUALITATIVE ANALYSIS

The Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) method's qualitative analysis is presented in this section. The overall LRS-HECS is split into two sections, namely, image steganalysis and certificateless signcryption. Figure 4 illustrates the results obtained after applying the Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography model.

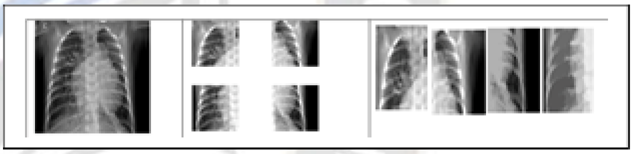
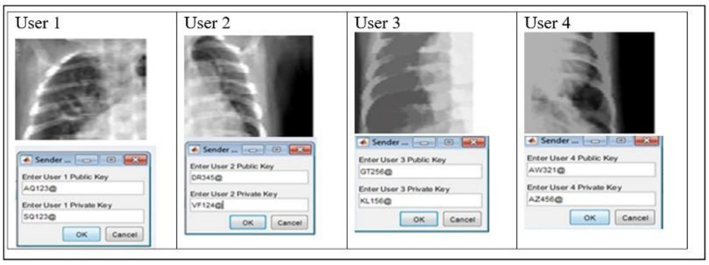


Figure 4 (a) input image (b) block split image (c) block of images provided to four users

From the above figure 4(a) specifies the input image obtained from Chest X-Ray stego images dataset, figure 4(b) shows the resultant images after applying the Lagrangian Block Splitting function to the input image. Finally, figure 4(c) shows the resultant block of images provided to four different users after applying the correlated codeword separately for each block. Next, the results of Hyper Elliptic Curve-based Certificateless Signcryption when applied to the steg images are provided in figure 5.



Enter User 1 Public Key: AQ123@
Enter User 1 Private Key: SQ123@

Enter User 2 Public Key: DR345@
Enter User 2 Private Key: VF124@

Enter User 3 Public Key: GT256@
Enter User 3 Private Key: KL156@

Enter User 4 Public Key: AW321@
Enter User 4 Private Key: AZ456@

Figure 5 (a) Public and private key of block 1 (i.e., user 1), (b) Public and private key of block 2 (i.e., user 2), (c) Public and private key of block 3 (i.e., user 3), (d) Public and private key of block 4 (i.e., user 4)

From the above figure, public and private keys are generated separately for each block (i.e., for four different users). Finally, the validation is performed by the central repository and only upon successful validation transmission process is initiated, therefore ensuring security.

4.2 QUANTITATIVE ANALYSIS

Peak signal-to-noise ratio, encryption time, transmission cost, and data integrity rate are four different metrics that are quantitatively analyzed in this section. Elaborate comparisons are made using the proposed LRS-HECS and two state-of-the-art methods, Binary classification model based on artificial neural networks [1] and CGST [2]. For fair comparison similar set of images and image sizes are utilized and an average of ten simulation runs are conducted.

4.2.1 PERFORMANCE ANALYSIS OF PEAK SIGNAL-TO-NOISE RATIO

This section analyzes the peak signal-to-noise ratio. It is the most significant performance metric since it is used to calculate the image steganography process's potential for denoising. So, the ratio is mathematically stated as given below.

$$PSNR = 10 \log 10 \left(\frac{L^2}{MSE}\right) \qquad (16)$$

The peak signal-to-noise ratio '' is calculated using the maximum possible pixel value 'L' and the mean square error 'MSE' which is mathematically expressed as provided below, using the results of equation (16) above.

$$MSE = [DCI - CI] \qquad (17)$$

The mean square error 'MSE' is calculated from equation (17) above using the denoised chest image 'DCI' and the original chest image 'CI'. The measurement term used is decibel (dB). First, Table 1 shows measurements of the peak signal to noise ratio for ten different medical photographs of various sizes. As shown in Table 1, ten medical images with various sizes were gathered as input for the experiment from the chest X-ray medical image database. A binary classification model based on artificial neural networks [1] and CGST [2] are shown in Table 1 as well as their respective PSNRs. According to the findings, LRS-HECS produces a higher PSNR than the currently used approaches. The use of the Lagrangian Block Splitting function is what led to this huge improvement. The proposed Lagrangian Block Splitting function splits the given images into four blocks and applies the image steganalysis process to the four blocks separately. The block splitting function itself removed the higher deviation pixels, also known as the noisy pixels, from the input cover images because it only takes the proximity function into account while block splitting. The input medical cover images are therefore smoothed out using the splitting technique before being sent for further processing. The proposed deep learning method's experimental findings were compared with those of the existing approaches. The performance of the LRS-HECS approach is determined to have improved by 12% compared to [1] and 23% compared to [2] respectively, according to a comparison of the proposed and existing methods.

TABLE 1 PEAK SIGNAL-TO-NOISE RATIO TABULATION FINDINGS

Image size (KB)	**Peak signal-to-noise-ratio (dB)**		
	LRS-HECS	Binary classification model based on artificial neural networks	CGST
870.78	28.15	30.25	33.55
406.31	33.25	39.35	45.85
582.64	42.55	48.15	53.15
471.56	40.25	42.35	50.55
451.29	38.15	40.55	47.25
669.29	45.55	49.55	53.55
400.65	48.15	52.35	58.65
420.27	52.35	58.65	63.15
458.09	50.15	55.15	61.05
384.93	48.55	52.55	58.25

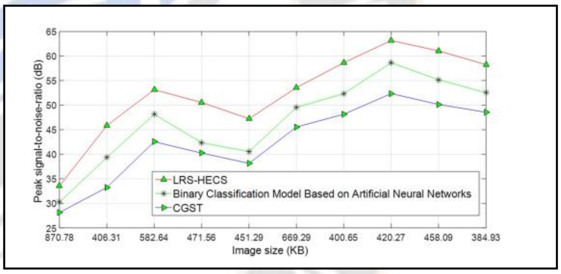


Figure 6 shows the PSNR graphically

The peak signal-to-noise ratio measurements are displayed graphically in Figure 6 above and are measured in decibels (dB). Several medial image sizes were used as the input and shown at the horizontal axis. The results of the peak signal to noise ratio values obtained using three different methods LRS-HECS, Binary classification model based on artificial neural networks [1] and CGST [2] are shown at the vertical axis. The proposed LRS-HECS method provides a higher peak signal to noise ratio than the two state-of-the-art methods, according to the graphical data.

4.2.2 PERFORMANCE ANALYSIS OF ENCRYPTION TIME

This section measures the length of time the medical image steganalysis takes to encrypt. The encryption time or the embedding time here states to the amount of time used by the medical image steganalysis algorithm to encrypt or embed the given input cover image and get resulting block images. The encryption time is mathematically stated as given below.

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

From the above equation (18), the encryption time 'Enc_{time} ' is measured based on the input cover image involved in the simulation process 'CIi' and the actual time consumed in the overall embedding process '$Time\ [Emb]$' for obtaining the resultant four blocks. Table 2 indicates various encryption results using three methods, LRS-HECS, Binary classification model based on artificial neural networks [1] and CGST [2]. By varying the sizes of input medical images results in the different encryption time also. As provided in table 2, the proposed LRS-HECS method outperforms in terms of encryption time upon comparison with other two existing methods, [1] and [2]. As different images possess different sizes and also different PSNR values, the encryption time is also not found to be proportion to the input medical image. Despite, the encryption time is found to be comparatively minimal using LRS-HECS than [1] and [2].

TABLE 2 SHOWS THE RESULTS OF THE ENCRYPTION TIME TABULATION

Image size (KB)	**Encryption time (ms)**		
	LRS-HECS	Binary classification model based on artificial neural networks	CGST
870.78	1.74	2.61	4.35
406.31	0.85	0.98	1.35
582.64	1.15	1.35	1.85
471.56	0.35	0.85	1.35
451.29	0.25	0.55	1.15
669.29	1.25	1.55	1.85
400.65	0.95	1.35	1.65
420.27	0.18	0.45	0.8
458.09	1.05	1.35	1.65
384.93	0.95	1.55	1.95

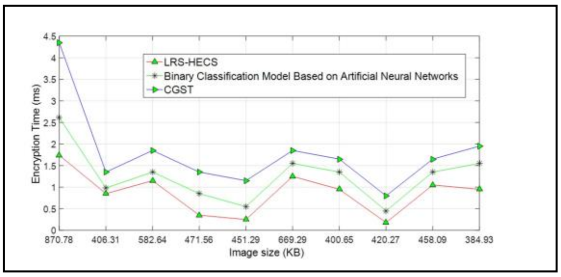


Figure 7 Graphical representation of encryption time

Figure 7 above shows ten different encryption time results. To perform fair comparison, same image size has been provided as input for all the three methods. The LRS-HECS method, out of the three, performs encryption with the least amount of time. The use of the Codeword Correlated Lagrangian Recurrent Neural Network-based image steganography algorithm was responsible for this improvement. Using this algorithm just after splitting the input medical images into blocks are allowed for further image steganalysis process. Here, only the correlated codeword was utilized for encrypting each blocks and followed by which the Stego images were then sent to four different users (i.e., from single Chest X-Ray cover image) via the output vector or output layer. The encryption time was also claimed to have been greatly decreased with LRS-HECS by 35% compared to [1] and 53% compared to [2], respectively, because the Stego images were said to be obtained separately for each block.

4.2.3 PERFORMANCE ANALYSIS OF COMMUNICATION COST

The cost incurred in performing a communication model that includes the cost of generating and verifying a signature.

$$CC = \sum_{i=1}^{n} CI_i + Cost\ [Gen + Val](Sig\ [U_1] + Sig\ [U_2] + Sig\ [U_3] + Sig\ [U_4]) \qquad (19)$$

From the above equation (19) the communication cost 'CC ' is measured based on the number of input medical images 'CIi ' involved in the simulation process and the cost of generating and validating a signature '$Cost\ [Gen + Val](Sig\ [U_1] + Sig\ [U_2] + Sig\ [U_3] + Sig\ [U_4])$ ' respectively. It is measured in terms of kilo bits (Kbits). Table 3 given below lists the communication cost results obtained by substituting the results from (19).

TABLE 3 TABULATION RESULTS OF COMMUNICATION COST

Image size (KB)	**Communication cost (Kbits)**		
	LRS-HECS	Binary classification model based on artificial neural networks	CGST
870.78	883.13	890.43	895.93
406.31	650.25	735.15	755.55
582.64	710.35	755.15	793.35
471.56	650.25	695.35	725.15
451.29	635.15	680.25	700.15
669.29	845.35	955.15	985.35
400.65	625.15	685.35	715.35
420.27	650.35	700.25	725.45
458.09	685.15	735.55	785.55
384.93	545	685.25	715.35

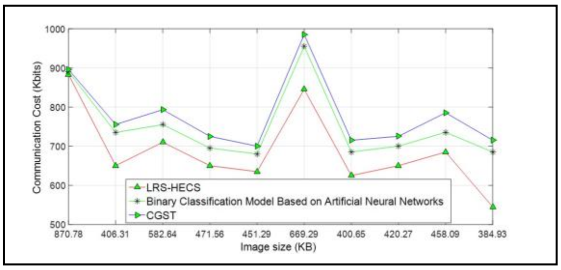


Figure 8 Graphical representation of communication cost

The graph of communication cost for 10 different images with changing sizes is displayed in Figure 8 above. To determine the communication cost, ten different simulation runs were carried out using the LRS-HECS, the Binary classification model based on artificial neural networks [1], and the CGST [2], respectively. From the above figure neither increasingly proportionate nor decreasingly proportionate graphs was found. The reason was due to different image sizes for different images. However, simulations performed for image with size 870.78KB, the communication cost using LRS-HECS was observed to be 883.13Kbits, 890.43Kbits using [1] and 895.95Kbits using [2]. Based on this result, LRS-HECS was shown to have lower communication costs than [1] and [2]. Owing to the application of Hyper Elliptic Curve function for obtaining various images for performing Certificateless Signcryption is the reason behind the improvement in communication cost. With this, it was discovered that the LRS-HECS method resulted in lower communication costs by 9% and 12%, respectively, when compared to [1] and [2].

4.2.4 PERFORMANCE ANALYSIS OF DATA INTEGRITY

One security criterion, known as data integrity, measures the proportion of medical images that have not been altered by unauthorized users to the total number of medical images used in simulation. The formula for the data integrity rate is shown below,

$$DIR = \sum_{i=1}^{n} \left(\frac{CI_{na}}{CI_i}\right) * 100 \qquad (20)$$

From the above equation (20), data integrity rate 'DIR' is measured based on the number of medical images that were not changed by malicious users '$CIna$' and the total number of medical images 'CIi' involved in simulation. The data integrity is measured in terms of percentage (%). Finally, table 4 given below lists the results of data integrity.

TABLE 4 SHOWS THE DATA INTEGRITY TABULATION RESULTS

Number of images	**Data integrity (%)**		
	LRS-HECS	Binary classification model based on artificial neural networks	CGST
15	93.33	86.66	73.33
30	91.35	83.25	70.25
45	90.25	81.15	68.35
60	88.15	80.55	65
75	85.35	77.35	64.15
90	81.25	75.15	62
105	80	73.15	60.35
120	78.35	71	58.55
135	75	68.25	55
150	71.45	65	53

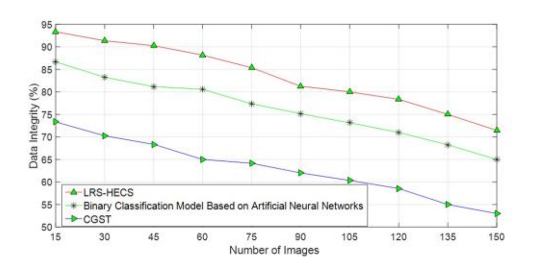


Figure 9 Graphical representation of data integrity

The graphical representation of data integrity for 150 different images is shown in Figure 9 given above. With the horizontal axis represents 150 images provided as input, the data integrity rate obtained using three different methods are shown in the y axis and is measured using terms of percentage (%). Based on the results, it can be determined that LRS-HECS has a higher data integrity rate than [1] and [2]. This comes from the results with 15 images, where 14 images were not said to be affected when applied with LRS-HECS, 13 images when applied with [1] and 11 images when applied with [2]. The Hyper Elliptic Curve-based Certificateless Signcryption algorithm is applied to the steg images. This certificateless signcryption process results in reducing the input image dimensionality as the public and private keys are obtained separately for each block when compared to other methods that generate keys for entire image. The steg medical images were then moved to a central repository, where the validation (i.e., desteg) were done in order to access the medical image. The data integrity rate results were compared with those of the currently used methods. The ten results on average show that the LRS-HECS approach improves data integrity rates by 10% and 33% in comparison to [1] and [2], respectively.

***Article Received:** 29 June 2023 **Revised:** 26 August 2023 **Accepted:** 08 September 2023*

V. CONCLUSION

Several methods of research used in medical diagnosis are based on images from medical studies. Image Steganography being an invisible communication has become significant research area in data security and image integrity. Moreover, certificateless signcryption on the other hand provide certificateless signature and encryption therefore ensuring secured medical image transmission. However, with the deficiency in the defensive course of actions, medical image transmission using Steganography-based Certificateless Signcryption may be unsafe. To address this issue, we introduced a method called, Lagrangian Recurrent Steganalysis and Hyper Elliptic Certificateless Signcryption (LRS-HECS) for secured medical image transmission. The LRS-HECS method is suited for use in medical image transmission since it produces steg images efficiently. Additionally, the suggested approach resolves the key escrow issue brought on by the certificateless cryptography process by including Hyper Elliptic Curve. The method, therefore, guarantees data integrity with improved peak signal-to-noise ratio. The communication cost analysis with the encryption time involved evident that the proposed method is better from other methods.

REFERENCES

[1] Julián D. Miranda, Diego J. Parada, “LSB steganography detection in monochromatic still images using artificial neural networks”, Multimedia Tools and Applications, Springer, Sep 2021 [Binary classification model based on artificial neural networks]

[2] 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, Apr 2022

[3] Punam Bedi, Anuradha Singhal, “Estimating cover image for universal payload region detection in stego images”, Journal of King Saud University – Computer and Information Scien, Elsevier, Jan 2022

[4] Sachin Dhawan, Chinmay Chakraborty, Jaroslav Frnda, Rashmi Gupta, Arun Kumar Rana, Subhendu Kumar Pani, “SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT”, IEEE Access, Jun 2021

[5] Ambika, Rajkumar L. Biradar & Vishwanath Burkpalli, “Encryption-based steganography of images by multiobjective whale optimal pixel selection”, International Journal of Computers and Applications, Oct 2019

[6] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, K. I. Mohammed, O. S. Albahri, A. S. Albahri, M. A. Alsalem, “PSO–Blockchain-based image steganography: towards a newmethod to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture”, Multimedia Tools and Applications, Springer, Dec 2020

[7] Reema Thanit, Nur Izura Udzir, Sharifah Md Yasin, Aziah Asmawi, Adnan Abdul-Aziz Gutub, “CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data”, IEEE Access, Jun 2022

[8] Sultan Alkhliwi, “Encryption-based Image Steganography Technique for Secure Medical Image Transmission During the COVID-19 Pandemic”, IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.3, March 2021

[9] Mohammad Kamrul Hasan, Shayla Islam, Rossilawati Sulaimain, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohmammad Islam, Saleh Alyahya, Musse Mohamed Ahmed, Samar Kamil, Md Arif Hassan, “Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications”, IEEE Access, Apr 2021

[10] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane, “Image Steganography: A Review of the Recent Advances”, IEEE Access, Feb 2021

[11] Ishak Meraouche, Sabyasachi Dutta, Haowen Tan, Kouichi Sakura, “Neural Networks-Based Cryptography: A Survey”, IEEE Access, Sep 2021

[12] Arwa Mashat, Surbhi Bhatia, Ankit Kumar, Pankaj Dadheech and Aliaa Alabdali, “Medical Image Transmission Using Novel Crypto-Compression Scheme”, Intelligent Automation & Soft Computing, Aug 2021

[13] Leonardo Horn Iwaya, Aakash Ahmad, M. Ali Babar, “Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study”, IEEE Access, Aug 2020

[14] Yang Ming, Xiaopeng Yu, Xiaoqin Shen, “Efficient Anonymous Certificate-Based Multi-Message and Multi-Receiver Signcryption Scheme for Healthcare Internet of Things”, IEEE Access, Sep 2020

[15] Tabares-Soto Reinel, Arteaga-Arteaga Harold Brayan, Bravo-Ortiz Mario Alejandro, Mora-Rubio Alejandro, Arias-Garzon Daniel, Alzate-Grisales Jesus Alejandro, Burbano-Jacome Alejandro Bueventura, Orozco-Arias Simon, Isaza Gustavo, Ramos-Pollan Raul, “GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis”, IEEE Access, Jan 2021

[16] Neerja Sahu, Dongming Peng, Hamid Sharif, “An innovative approach to integrate unequal protection-based steganography and progressive transmission of physiological data”, Springer, Oct 2020

[17] Xiaopeng Yu, Wei Zhao, Dianhua Tang, “Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing”, Journal of Systems Architecture, Elsevier, Mar 2022

[18] Ching-Chun Chang, “Neural Reversible Steganography with Long Short-Term Memory”, Security and Communication Networks, Wiley, Apr 2021

[19] Huifang Yu, Shengbing Wang, “Certificateless threshold signcryption scheme with secret sharing mechanism”, Knowledge-Based Systems, Elsevier, Mar 2021

[20] Caixue Zhou, “An improved lightweight certificateless generalized signcryption scheme for mobile-health system”, International Journal of Distributed Sensor Networks, Jan 2019.