

A crypto-steganography healthcare management: towards a secure communication channel for data COVID-19 updating

Mohanad Sameer Jabbar¹, Samer Saeed Issa²

¹Department of Technical College of Engineering, Medical Instruments Techniques Engg, Albayan University, Baghdad, Iraq

²Computer of Science Department, Al-Rafidain University College, Baghdad, Iraq

Article Info

Article history:

Received Jun 23, 2022

Revised Oct 1, 2022

Accepted Oct 24, 2022

Keywords:

Crypto-steganography

Hybrid cryptography

Inversing method

Random blocks

Virtual privet network

ABSTRACT

Nowadays, secure transmission massive volumes of medical data (such as COVID-19 data) are crucial but yet difficult in communication between hospitals. The confidentiality and integrity are two concerning challenges must be addressing to healthcare data. Also, the data availability challenge that related to network fail which may reason concerns to the arrival the COVID-19 data. The second challenge solved with the different tools such as virtual privet network (VPN) or blockchain technology. Towards overcoming the aforementioned for first challenges, a new scheme based on crypto steganography is proposed to secure updating (COVID-19) data. Three main contributions have been consisted within this study. The first contribution is responsible to encrypt the COVID-19 data prior to the embedding process, called hybrid cryptography (HC). The second contribution is related with the security in random blocks and pixels selection in hosting image. Three iterations of the Hénon Map function used with this contribution. The last contribution called inversing method which used with embedding process. Three important measurements were used the peak signal-to-noise ratio (PSNR), the Histogram analysis and structural similarity index measure (SSIM). Based on the findings, the present scheme gives evidence to increase capacity, imperceptibility, and security to ovoid the existing methods problem.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohanad sameer Jabbar

Department of Technical College of Engineering, Medical Instruments Techniques Engg

Albayan University

Baghdad, Iraq

Email: mohanad.s@albayan.edu.iq

1. INTRODUCTION

The coronavirus virus 2019 (COVID-19) pandemic, which has struck the whole world, has had a remarkable influence on people's life [1]. Technologies from several nations have contributed to helping medical professionals and medical-care providers halt this pandemic [2]. These contributions outline some of the main dangers to both individual and societal health, as well as the principles and suggestions that should be taken into account in order to mitigate them in the future [3].

To meet the demands of the present, sustainable health systems and social care must be improved [4]. To better understand the condition and to take environmental and lifestyle factors into account while treating the disease, a significant amount of healthcare data for COVID-19 is produced everyday by medical facilities, hospitals, and people. Additionally, collaboration between hospitals is required to aid medical professionals in providing COVID-19 therapy quickly [5]. Secure full-field communication lines between hospitals should be made possible by this integration. Five sequential questions are posed and addressed as follows for a comprehensive understanding of how to support the security of the healthcare system in integrating hospitals

with significant healthcare data for COVID-19 communication channels. The following are the four questions in order that are posed and addressed.

“What are the primary challenges and problems with this research?”, It is crucial yet difficult to update and share such vast volumes of healthcare data in an efficient and safe manner. Potential authors claim that these problems have not been fully examined [6]. More COVID-19 patients' private health information is being gathered and shared across hospitals and clinical labs, which presents further issues. Two problems must be resolved in particular to address the challenges of secure updating and sharing. First of all, hospitals and patients with COVID-19 are growing more concerned about the accuracy and privacy of their medical records. Modern methods concentrate on enhancing data providers' obligations to spot data disclosure actions [7]. However, there is an urgent need to safeguard patient data access and to promptly notify users when there is a risk of data leak. Second, while there are hundreds of health systems in operation today, the majority of them have a centralized design with a single point of failure, raising questions about the availability of data. Systems communicate and work together insufficiently, if at all, to secure patient data for COVID-19. In addition, healthcare professionals must adhere to regulations or norms (such as the Health Insurance Portability and Accountability Act of 1996). Many regulations, however, still do not apply to the many organizations that could have access to patient data and should be held responsible for their data operations, which also require audits [8].

“What technology are suggested for dealing with such problems and challenges?”, To overcome the difficulties with updating and sharing, two technologies are recommended [9]. First, steganographic transactions in dispersed hospitals can benefit from improved secrecy payload and resilience integrity thanks to steganography technology. With this method, good picture quality, high embedding capacity, and assault resistance can all be achieved. The integrity of secret data, however, has not yet been examined after being extracted from stego pictures and tampered with while being stored in the database. As a result, the data concealing mechanism requires fundamental modifications for data protection [10]. Conventional steganographic methods involve insecure channels that frequently cause sender privacy to be compromised. In order to achieve secrecy and integrity during the transmissions across the communication channels, hashes can be employed to create a novel steganography technique. Second, data may be encrypted using cryptography to increase security, enhance level of confidentiality, and retain data availability. In conclusion, the use of steganography in conjunction with cryptography can significantly increase the security of COVID-19 medical data.

“What are the current possibilities for academic writing that tries to apply steganography-based cryptography?”, Few attempts to apply steganography based on COVID19 frameworks or other medical data have been documented in the literature. Information confidentiality and integrity are maintained using two separate methods, steganography and cryptography [11]. Steganography is used to conceal hidden messages in digital material in a way that makes it impossible for anybody to discover their presence. Steganography's basic objective is to securely transmit hidden messages using images. Although steganography does not alter the structure of the hidden message, it conceals the change within the media to prevent detection. While cryptography modifies the meaning of communications to keep them from being read by unauthorized parties [12]. Steganography methods rely on the data encoding system's secrecy, if the encoding system is known, the steganography method can be identified or tracked. In cryptography obscures the integrity of the information so that it can only be understood by the sender and receiver [13], while steganography used to concealment the messages and transmitted via digital media. Information security components including data integrity, entity authenticity, and data authenticity are all related to the mathematical field of cryptography [14].

An image steganography that used the DES algorithm to encrypt text messages is proposed [15]. A 64-bit block size and 16 rounds are used in the approach. The image was divided into many segments and the data was embedded in each segment using the K-means pixel clustering technique. To segment images, a variety of clustering techniques were employed. A segmentation consists of a huge amount of data shown as pixels; each pixel has three components: red, green, and blue (RGB). They employed a least significant bit (LSB) approach to divide the encrypted message into K number of segments that are to be hidden in each cluster after forming the clusters. Due to the stated inadequacies of cryptography and steganography alone in transmitting data, a system based on the two technologies was developed in which it would be nearly hard for an outsider to compromise the system's security and extract sensitive information [16]. The encryption procedure of the proposed system utilized the recently created Two Fish algorithm, while the steganography process utilized the Adaptive B45 steganography approach. By combining the LSB algorithm with the AES algorithm, [17] presented a fusion of steganographic and cryptographic methods. The secret information was integrated into an image using the LSB approach, and the produced stego was encrypted using the AES algorithm. The research recommended using this methodology as a reliable way to send sensitive information with a higher level of security.

“What are the main contributions of proposed study?”, Using the steganography scheme, the secret or private data can be hidden within different media including the colour or grayscale image. Two important concepts are involved in the steganography technique so called stego and cover image. A stego image hosts the secret information with certain quality, whereas the object image is a pure image without containing

any secret information within it and is ready to host the secret information. The fundamental issues and difficulties concerning the performance of the existing state-of-the-art steganography schemes are related to the payload capacity, imperceptibility, and security [18].

The payload capacity of a steganography system is defined as the maximum size of the secret message that can be hidden into the image media. The imperceptibility of a steganography system signifies the carrier media quality that can be used for hiding the secret message following the algorithm embedding. The security of a steganography system [6] refers to its robustness against various statistical attacks such as the chi-square, human visual system (HVS), and histogram analysis. In this perception, the present research intends to resolve various issues related to the existing steganography system and improve its robustness in terms of high security, high payload capacity, and imperceptibility. The main contribution of this study is described as below:

- Hybrid cryptography (HC) is the first contribution. It describes the encryption method that is used to encrypt the secret information prior the embedding process.
- The second contribution of this study is new partitioning method using three iterations of the Hénon Map function.
- The third contribution is the inversing method (IM) is used for embedding encrypted messages. The inversing method makes the peak signal-to-noise ratio (PSNR) high as required which reflects more space to embed the secret message.

2. METHOD

Explaining research chronological pressing challenges in the context of a steganography system include security, imperceptibility, and capacity issues. Most researchers have highlighted the trade-offs between these issues. While the trade-offs between payload and security have been neglected by researchers, as fixing one issue has been indicated to affect the other, and vice versa [19]. Towards overcoming the aforementioned issues, a new scheme has been proposed for image steganography. The Figure 1 is mentioned the main steps of the proposed scheme.

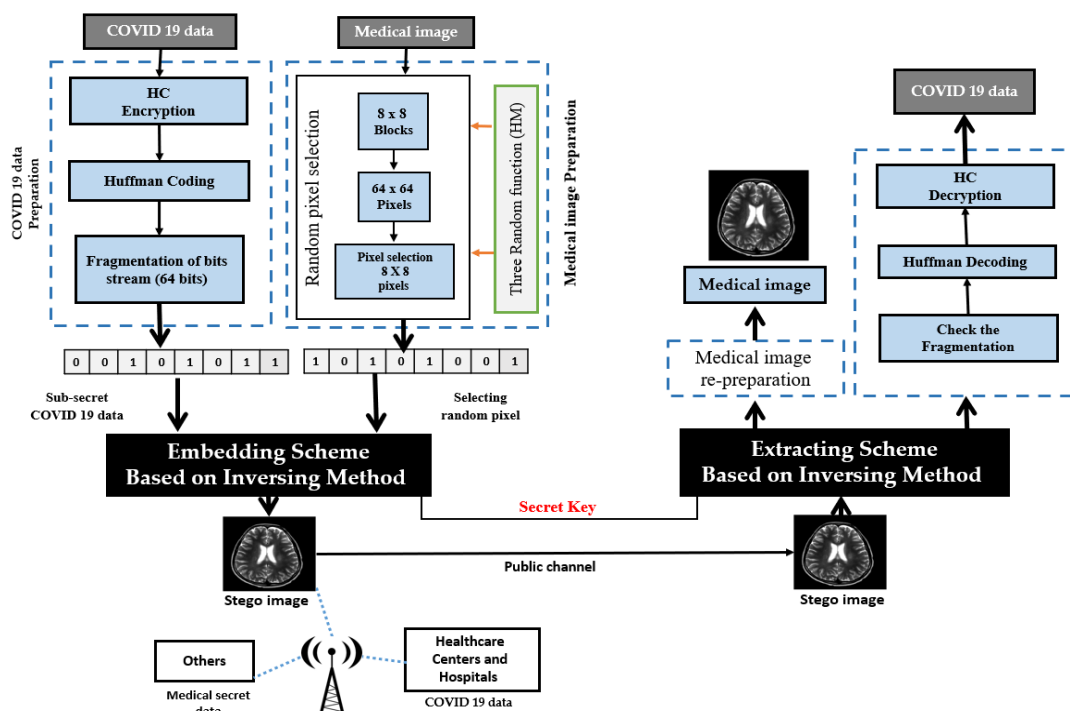


Figure 1. The structure of proposed scheme

The proposed scheme is divided into three main contributions. The first contribution is hybrid additive cryptography (HC), which is related to the encryption of secret messages prior to the embedding process. The second contribution is image partitioning method and last contribution is a bit interchange method (BIGM) [20], which is related to the embedding process. The next subsections describe the contributions in detail.

2.1. Hybrid additive cryptography (HC)

In this section, the hybrid additive cryptography (HAC) is discussed based on ElGamal elliptic curve cryptosystem with Cubic Bézier curve to achieve text confidentiality. The confidentiality and security of the Text before embedding is necessary and needful. The proposed cryptography is used to enhance security level features via using the novel hybrid cryptography approach that combines security concepts in Bézier curves techniques and the Elliptic curve EC points in order to produce a hybrid-key point (cipherkey) [21]. The proposed HC is shown in Figure 2.

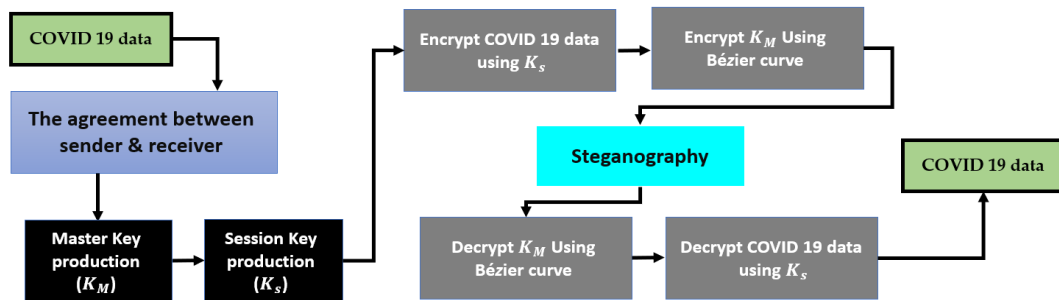


Figure 2. Illustration diagram of the proposed HC method

2.1.1. Agreement between sender and receiver

This agreement of the framework is done between the sender and the receiver. The authentication is used in order to emphasize to the receiver part that data was sent from a recognized sender part and did not modify in between by any unauthorized person. In this stage, a good method to generate a session key from the master key using Bézier curves equations and fitting the curve on the master key is proposed [22]. The process is achieved by concurrent monitoring points via a receiver and sender sides. The following process describe the agreement procedure:

- a) The elliptic-curve (EC) produce through finite field (FF) $E(Ep)$.
- b) Base point $B \in E(Ep)$.

In a secret way, control the secret point for Bézier:

$$BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3) \text{ and } t = (t_1, t_2) \in [0,1] \text{ and the compute } t \text{ by: } = (t_1, t_2) \in [0,1] \text{ Mod } p.$$

- c) Secretly on a base point P that related $E, (P \in E (Fp))$.

2.1.2. Key produce phase

This phase describes the production of the cryptography keys introduced in this work, the Master Key (K_M) and Session-Key (K_S). The K_M is the major key that produce the K_S , while the K_S is the key which uses to encrypt a text.

- a) Master Key production (K_M)

The major process for master key (K_M) within this work is to produce the K_S . This work introduces a new algorithm to produce the K_M via utilizing the ElGamal Elliptic Curve algorithm (EEC). The result is a point that represents the master key between sender and receiver.

- b) Session Key production (K_S)

In this phase, a new algorithm to produce the Q_a using the K_M . The master key K_M will convert into binary bit (Bin) then convert it to decimal (De). Finally, multiply De with the K_M . The resulting point is represented the K_S . The key generation process is explained in detail within following points:

- a) Receiver chosen random integer d as secret point.
- b) Compute the Public-Key Q_B using the d integer:
 $dB = Q_B$ and keep d as a secret integer.
- c) Chosen random integer e by sender as a secret pint.
- d) Compute the master key K_M by using e and Q_B
 $eQ_B = K_M = (x_4, y_4)$.
- e) Convert the Q_A to Bin and to De, compute $n = De \text{ Mod } p$.
- f) Compute the session key K_S by using n and K_M :
 $nK_M = K_S$.

2.1.3. Encryption stage

Information protection is the most important issue in the text encryption field. In the proposed method, the encryption stage includes two parts:

a) Encrypt the secret text process

After building the master key from the recipient's public key in this algorithm, we added a new technique in this part by converting the K_M into binary bits and then into decimal to generate the session key in order to increase the security and robustness of the algorithm. This technique is used as the authentication between the sender and receiver. This change will make the encryption process more secure than the existing algorithms process.

b) Encrypt the master key process

The K_M must transfer with the ciphertext to a receiver part. for that cause this algorithm must be encrypt the K_M before sending it. The cubic Bézier curve and agreed on control points (Bézier points) between the sender and receiver are used for encrypting the cipher key with the ciphertext. A clearer flowchart of the central idea of the proposed encryption process presented is shown in Figure 3.

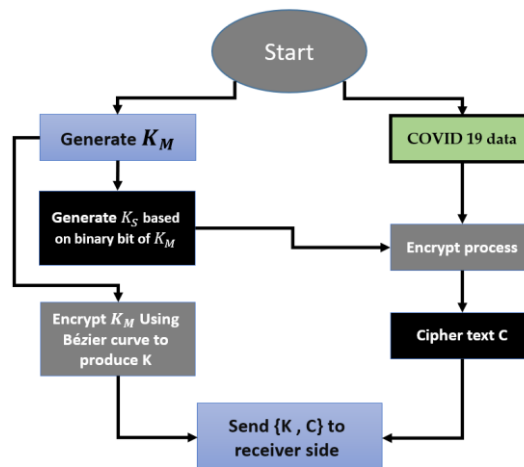


Figure 3. Encryption process

The full Algorithm of the proposed encryption method is explained in detail with proposed method with the following points:

- Select the secret text.
- Convert all the characters of text to ASCII value.
- Use point P to compute $m_i P = M, i = 1, 2, 3, \dots$
- Encrypt the message point M using Q_a via: $C = M + K_s$, C is ciphertext.
- Encrypt the $K_M = (x_4, y_4)$ using secret control points of Bézier: $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3)$ and $t = (t_1, t_2) \in [0, 1]$ and the compute t by: $= (t_1, t_2) \in [0, 1] \text{ Mod } p$, via:

$$K_1 = x_1(1 - t_1)^3 + 3x_2(1 - t_1)^2 t_1 + 3x_3(1 - t_1) t_1^2 + t_4 t_1^3 \text{ Mod } p$$

$$K_2 = y_1(1 - t_2)^3 + 3y_2(1 - t_2)^2 t_2 + 3y_3(1 - t_2) t_2^2 + y_4 t_2^3 \text{ Mod } p$$

$$K = (K_1, K_2) \text{ is cipher key.}$$
- Send {C,K} to receiver side.
- End

2.1.4. Decryption process

The aim of the decryption stage is to retrieve the original text during the reverse processes of the encryption algorithm. The recipient of the ciphertext and cipher key implements the decryption process first using the secret control points (Bézier points) and based on Bézier curves equations to decrypt the cipher key and to find the session key, and then use session key to decrypt the ciphertext. The proposed decryption algorithm is explained in detail within the following points:

- Receive {C,K} from sender side.
- Find the K_M via decrypt $K = (K_1, K_2)$ using $BP_1 = (x_1, y_1), BP_2 = (x_2, y_2), BP_3 = (x_3, y_3)$ and $t = (t_1, t_2) \in [0, 1] \text{ Mod } p$

$$x_4 = [k_1 - x_1(1 - t_1)^3 + 3x_2(1 - t_1)^2t_1 + 3x_3(1 - t_1)t_1].(t_1^3)^{-1} \text{ Mod } p$$

$$y_4 = [k_2 - y_2(1 - t_2)^3 + 3y_2(1 - t_2)^2t_1 + 3y_3(1 - t_2)t_2].(t_2^3)^{-1} \text{ Mod } p$$

$$K_M = (x_4, y_4) \text{ the master key.}$$

- 3- Convert the K_M to Bin and then to De , finally, compute $n = \text{De Mod } p$
- 4- Compute the K_S by using n and K_M : $nK_M = K_S$.
- 5- Decrypt the ciphertext C using the K_S via: $M = C - K_S$.
- 6- Using secret point P to solve DLP for $M = m_iP$.
- 7- Convert the value of m_i into ASCII characters
- 8- Obtained the text
- 9- End
- 10-

So, this is a proposed encryption example:

1. The Agreement Process Between Alice and Bob

- Publicly: Alice and Bob agree on an elliptic curve E over $F67$ ($E (F67)$) and $B = (887,292) \in E$, where $\# E = 919$ $E : y^2 = x^3 + 78x + 96 \text{ mod } 967$, where $a = 78$, $b = 96$ and $p = 967$ satisfy the condition $4a^3 + 27b^2 \text{ mod } p : [4 (78^3) + 27 (96^2)] \text{ mod } 967 = 300 = 0$.
- Secretly: Alice and Bob agree on Bézier point BP , $(215,115)$. $BP_2 (160,140)$, BP , $(100 , 75)$ and $t = (0.86,0.75) \in [0,1] \text{ mod } 967$, and they compute : $t (0.86,0.75) \in [0,1] \text{ mod } 967$ $t = (86.100 - 1 , 75 100 - 1) \text{ mod } 967$ $t = (86.938 , 75.938) \text{ mod } 967$ $t = (407,726)$.
- Secretly : Alice and Bob agree on another base point on E . let $P = (678,801)$.

3. Encryption Process (Alice)

- Chooses a text: " elgamal "
- Converts each characters into ASCII values : $e : m , mm ,$
- Uses the secret point $P = (678,801)$ to compute $101, 1 : m_2 = 108 , g : m_2 = 103 , a : m , -97 , 109 , a : m = 97 , 1 : m , = 108$.
- $m_2P 101 (678,801) (838,836) = M$.
- Encrypts the message M and based on session key Q by compute : $C = M + Qa (838,836) + (208,534) = (331,724)$.
- Encrypts the master key $QA (175,388)$ using BP , $= (225,366)BP$. $BP_2 (450,530)$. BP , $(100,75)$ and $t = (407,726)$ by : $k_1 = x_2 (1 - t_1)^3 + 3x_2 (1 - t_1)^2t_2 + 3x_2 (1 - t_1)t_1^2 + xt_1^3 \text{ mod } p - 215 (1-407)^3 + 3 (160) (1-407)^2 (407) + 3 (100) (1-407) (407^2) + (330) (407^3) \text{ mod } 967$ $19886095510 \text{ mod } 967 = 633$
- $k_2 = Y_1 (1 - t_2)^3 + 3y_2 (1 - t_2)^2t_2 + 3y_3 (1 - t_2)t_2^2 + yat_2 \text{ mod } p$
- $= 115 (1-726)^3 + 3 (140) (1-726)^2 (726) + 3 (75) (1-726) (726^2) + (235) (726^3) \text{ mod } 967$
- $= 120394754485 \text{ mod } 967$
- $= 530$.
- $K = (633,530)$ is ciphered session key .
- Sends (C,K) to Bob .

2. Key Generation Process

- Bob chooses a random integer $d = 612$ as a private key , and then computes the public key : $Q = dB = 612 (887,292) = (937,739)$, and keep d secret .
- Alice chooses a random integer $e = 521$ as a secret key , and uses Bob's public key to compute the master key : $QACQB 521 (937,739) = (330,235)$.
- Alice converts the master key $QA (330,235)$ to binary bits : $QA10100101011101011$, and then converts it to decimal Dec. 84715 , and computes $n = \text{Dec.mod } p$ $n = 84715 \text{ mod } 967 = 586$.
- Calculate the session key Qa by : $Qan QA = 586 (330,235)$ $Qa = (208,534)$

4. Decryption Process (Bob)

- Receives (C,K) .
- Decrypts $K = (633,530)$ using BP , $= (215,115)$.
- $BP_2 = (160 , 140)$. BP , $= (100,75)$ and $t = (407,726)$ by compute and find the master key : $\text{mod } p$ $x = [k_1 - x_1 (1 - t_1)^3 - 3x_2 (1 - t_2)^3t_2 - 3x_2 (1 - t_2)t_1^2] (t_2^3)^{-1} = [633-215 (1-407) -3 (160) (1-407) (407) -3 (100) (1-407) (407)] . (407^3) \text{ mod } 967 = (2362222313) (319) \text{ mod } 967 = 330$, $y = [k_2 - y_1 (1 - t_2)^3 - 3y_2 (1 - t_2)^2t_2 - 3y_2 (1 - t_2)t_2^2 (t_2^3) \text{ mod } p = [530-115 (1-726) -3 (140) (1-726) (726) -3 (75) (1-726) (726) - (726) \text{ mod } 967 = (-30470317595) (74) \text{ mod } 967$ $235 QA = (330,235)$ is the master key .
- Converts the master key $QA = (330,235)$ to binary bits : $QA = 10100101011101011$, and then converts it to decimal Dec.= 84715 , and computes n m $\text{Dec.mod } p$ $n = 84715 \text{ mod } 967 = 586$.
- Calculate the session key Qa by : $Qa = n QA = 586 (330,235)$ $Qa = (208,534)$.
- Decrypts the ciphertext $C = (331,724)$ to find the message M by compute : $M = C - \% (331,724) - (208,534) = (331,724) + (208 , - 534 \text{ mod } 967) = (331,724) + (208 , 433) = (838,836)$.
- Uses the secret point $P = (678,801)$ to solve DLP for $M = m_2P (838,836) = m_2 (678,801)$ $P = (678,801)$, $2P = (540,950)$, $3P = (690,221)$, $4P = (216,77)$, $SP = (400,497) .. 101P = (838,836) = M$.
- then , $m , 101 - \text{character " e "}$.
- By the same way, for each remaining characters.

2.2. Huffman coding

In compression theory and computer science, Huffman coding is an algorithm that produces a lossless data compression. The algorithm exploits the letters hesitation (weight) and the text file's length or text stream. The ordering of text stream lengths is necessary for the algorithm in this system to perform their full purpose. A suitable length or fragment of the text stream makes the system more reliable and robust. Fragment methods are detailed in [23]. The main goal of the Huffman coding algorithm is to reduce the size of the text before embedding it in the image. The main process of the Huffman algorithm depends on reducing frequent letters and giving them priority codes or short paths in a Huffman tree. Taha *et al*, [23], the authors illustrate strategies for reducing text frequency (redundancy) through Huffman coding.

2.3. Blocks and pixels random selection (BPRS)

A new random selection is used in this study to improve the security of image steganography called BPRS. This method partitions an image into three phases to secure final pixel for embedding. There are various advantages of using randomization algorithm, as follows:

- Simplicity for solving various problems.
- Highly efficient.
- Easy implementation.
- Optimum output is produced with a very high probability of achieving randomization goal.

For these reasons, the proposed BPRS has used a random approach with the proposed scheme. The BPRS has two phases, the first phase responsible for image partitioning while the second phase responsible for random pixel selection based on henon map function (HM). Both phases are working together for achieving the level of security in proposed work. three phases in image partitioning will be performed. As an initial partitioning, the image is partitioned into an 8×8 block (comprising of 64 blocks). The second partitioning selects a block out of the 64 blocks and further partitions it into a block of 64×64 pixels (4096 pixels). The final partitioning selects a sub pixel out of the 4096 pixels and partitions it into a block of 8x8 pixels (64 pixels). Figure illustrates image partitioning of the proposed method.

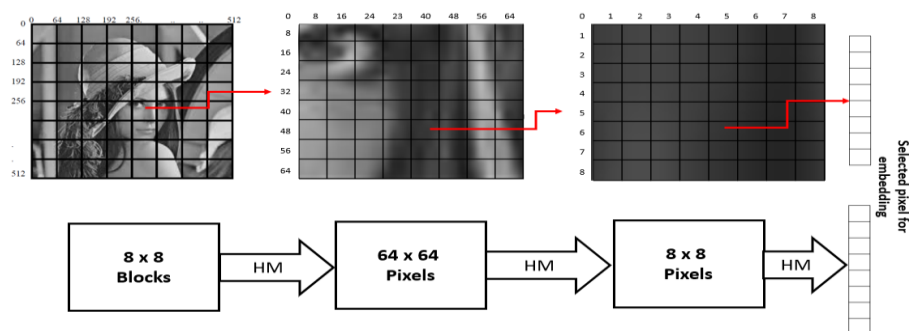


Figure 4. Image partitioning based on the proposed BPRS

In order to achieve an enhanced security in a secret message, three control parameters in the authors' random function based on the Henon map function, have been implemented in this study. In most past studies, researchers have commonly implemented a single parameter to choose the number, whereby an initial condition for this function (single) is 10^{15} , while the probability of finding the number is 2^{50} . On the other hand, the Henon map function increases the complexity in the attempts of finding the number by 10^{30} , which is a rough equivalent of 2^{100} . This is sufficient to secure the secret text within an image. The HM is an idea about dynamic function (DF) with a chaotic behaviour [24]. The Henon map has two initial parameters: ($a = 1.4$) and ($b = 0.3$) which serve a chose behaviour for the chaotic function. The function depends primarily on a and b parameters and can be illustrated as coordinate point (X_n, Y_n) on a plane. New points that would be produced upon using this function are as (1):

$$\begin{cases} X_{n+1} = 1 - a X_n^2 + Y_n \\ Y_{n+1} = b X_n \end{cases} \quad (1)$$

The main objective of using three steps (for block and pixel) with a random map is to increase security of message embedded in an image. In order to achieve a random distribution of pixels, matching pixel values with secret data value is needed.

2.4. Embedding process based on inversing method (IM)

Proposed IM aims to keep the stego image which involves the secret message looking like the original image. In this regard, no one can notice if there is a secret inside it or not. After selecting the pixels using BPRS, now ready for embedding. Before embedding process, the secret message is divided into 64 bits. At this stage, we have 64 bits (last stage of BPRS) will replace with 64 bits (from secret message). Before replacing, check the match between the bits in the original image and the bits in the secret message. If the number of matching bits is less than the number of non-matching bits, the secret message is exchanged and embedded. Otherwise directly embed the secret bits [25]. As shown in Figure 5. In this figure, black bits represent mismatch bits and green bits represent match bits.

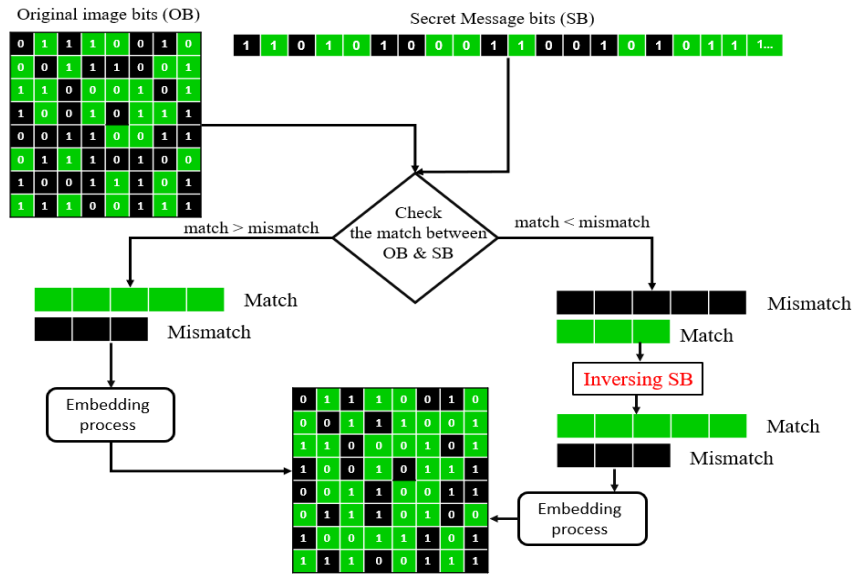


Figure 5. The main procedure of inverting method (IM)

The pixels for each cycle checked its LSBs and compared them with corresponding bit in the secret message. The IM procedure is considered whenever much conformity is occurred between cover image LSBs and secret bits. This procedure condition stored in stego key to retrieve the information later whenever extracted by the receiver [26]. Stego key is built through embedding method and consisted of a lot of information about embedding process in sequence [27]. The other side inverted this procedure to extract the secret message. The pseudo-code in Algorithm 1 explains embedding procedure. The payload capacity of secret message is estimated for bitplane (1) using: $(512 \times 512)/8 = 32768$ bits.

Algorithm 1: Inverting Method (IM)

Input : vectors (RND) : bits of secret message :
Output : embedded pixels
Begin
For all RND vector **do**
 if Oldvalue - Newvalue then Nchange- Nchange +1
 Else Change Change +1
 If Change > Nchange then (embed directly from secret to pixel
 Set Bitmap in vector RND (64) -1
 Else (invert the secret message then embed
 Set Bitmap in vector RND (64) 0
End

when using LSB ones, we need to divide by 8, implying the use of 1/8 of cover image for payload. Irrespective of the inversion of the secret during embedding, all embedding occurs in bit-plane (1) as illustrated in Figure 5. When the majority did not correspond to the matching bits, the secret message is inverted and embedded. Otherwise, the secret message is inserted directly into the cover image. The most important procedure is to mark all the pixels into the block map called the BPRS block. Figure 6 shows the details of this procedure. Simplistically in IM the embedding follows certain condition which is the matching between bits of secret message and bits in LSB image if many should be embed directly or else inverting is needed then embed.

It is important to checking LSB of the bit because all the information related to inspection is also stored in IM block as seen in Figure 6. Tracking of the pixel is impossible without IM block so that mapping the procedure is necessary. Insertion of the secret message directly increases the PSNR of the system, but it is still necessary to avoid HVS attack which is sensitive to any regular changes. During the checking of matching pixels, it is necessary to keep the messy of the bit distribution as much as possible, so that HVS attack can be avoided.

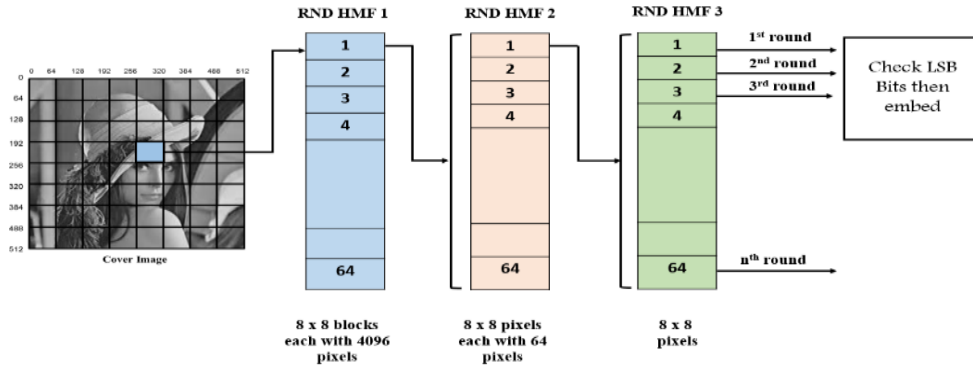


Figure 6. The procedure of BPRS method with checking LSB before embedding

3. RESULTS AND DISCUSSION

In this section, The approaches for evaluating the stego image can be characterized as objective or subjective. The objective evaluation methods use mathematical criteria and a variety of other criteria, such as ground truth or prior information from statistical concerns, to determine the discrepancies between the stego picture and the cover image. Subjective evaluation approaches, on the other hand, rely on human observation and judgment rather than any reference standards. The outcomes will be described in detail.

3.1. Evaluation criteria

Various types of steganalysis (stego analysis) methods have been proposed to test stego image performance prior to sending it out to receivers. Leading methods to simulate attacks on steganography performance in the literature include Chi-square, human visual system (HVS) attack, Mean Squar Error (MSE), PSNR, Histogram analysis, and structural similarity index measure (SSIM).

$$MSE = \frac{1}{M*N} \sum_{i=1}^M \sum_{j=1}^N (a(i, j) - b(i, j))^2 \tag{1}$$

$$PSNR = 10 \log_{10} \frac{i_{max}^2}{MSE} \tag{2}$$

$$SSIM = \frac{(2P_O Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2 Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)} \tag{3}$$

In MSE and PSNR, the three embeddings include simple LSB, pixel value different (PVD), and proposed method, as shown in Table 1. When the result of the proposed system is compared against the performance of existing methods in data hiding, a distinguishable performance difference is noted, as shown in Table 2. Table 3 compares the findings obtained using the SSIM and MSE to those obtained using existing state-of-the-art approaches. The proposed method's evaluation findings were found to be superior to those published in the literature. The cover image is viewed as the stego image in the image histogram, and this is the major goal of the image steganography histogram, as illustrated in Figure 7 for color and grayscale images, respectively.

Table 1. Different result related to MSE and PSNR with different techniques with proposed method

Results of PSNR for Lena image with different payloads					Results of PSNR for Lena image with different payloads				
Payload (bytes)	Embedding percent	MSE (LSB)	MSE (PVD)	MSE (Proposed work)	Payload (bytes)	Embedding percent	PSNR (LSB)	PSNR (PVD)	PSNR (proposed work)
16384	6.25%	0.3322	0.2122	0.1011	16384	6.25%	63.2	71.32	73.05
32768	12.5%	0.6452	0.5021	0.2012	32768	12.5%	62.1	67.63	71.21
49152	18.75%	0.9331	0.8321	0.6013	49152	18.75%	55.76	63.16	67.92
65536	25%	1.3221	0.9882	0.8022	65536	25%	50.82	55.91	62.43

Table 2. PSNR benchmarking at 16384 bytes of capacity payload data

Reference	Payload capacity (bytes)	Lena	Papper
Sridevi <i>et al.</i> , [17]	16384	64.54	64.72
Sahu and Swain [28]	16384	72.09	71.32
Kadhim <i>et al.</i> [20]	16384	68.34	68.26
Sabeti <i>et al.</i> , [14]	16384	71.27	71.21
Proposed work	16384	73.05	73.15

Table 3. Shows the results of the suggested scheme vs the state of the art in SSIM and MSE

Reference	Dataset/Image size	EP %	SSIM	MSE
Seyyedi <i>et al.</i> , [29]	USC-SIPI 512 × 512	6.25%	0.9961	0.0127
Setiadi and Jumanto [22]	USC-SIPI 512 × 512	6.25%	0.9957	0.0240
Sahu and Swain [28]	USC-SIPI 512 × 512	6.25%	0.9968	0.0236
Proposed Study	USC-SIPI 512 × 512	6.25%	1	0.0101

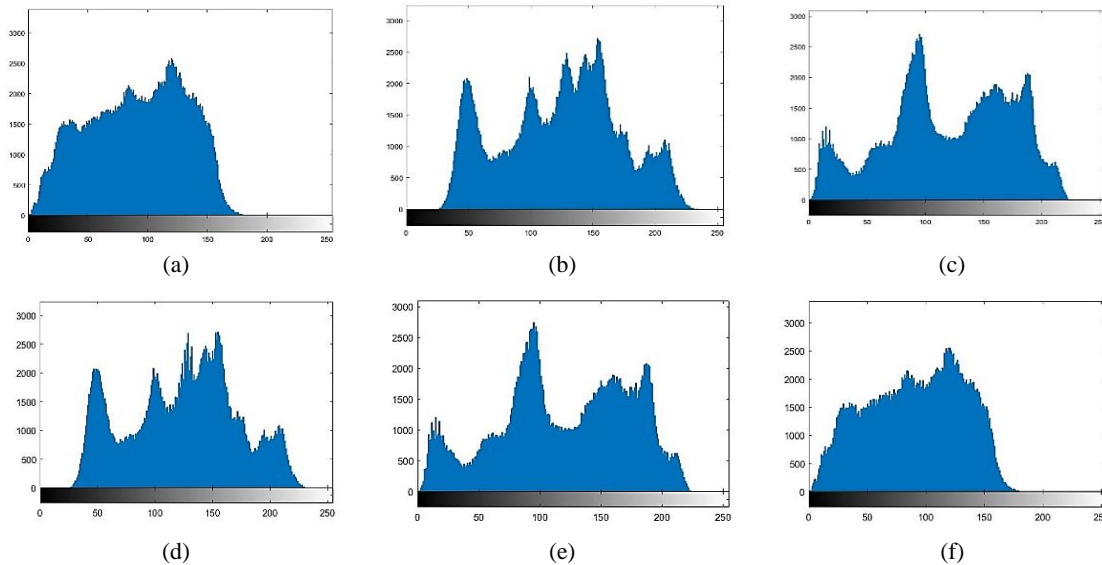


Figure 7. Histograms of the original carrier images and the corresponding stego images, (a) Original carrier image Zelda, (b) Original carrier image Lena, (c) Original carrier image Papper, (d) Corresponding stego image Lena, (e) Corresponding stego image Papper, and (f) Corresponding stego image Zelda

4. CONCLUSION

This study introduces a new technique for disguising confidential medical information that may be used as a new framework and covert means of sharing patient information about COVID-19 patients with hospitals. The main objective of this paper is to enhance the proposed image steganography system by increasing security of COVID 19 data by maintaining the PSNR value. In this paper, a high payload capacity of the secret message is required to be hidden. The results achieved in this study indicate that the proposed system is efficient in terms of security and capacity. However, the current study has many valuable contributions which are like BPRS, HC, and IM. These contributions achieve the objectives of image steganography such as security and produced a high value of imperceptibility. In addition, the plan for the exploration towards improving and continuing this research has been emphasized. In short, the newly designed steganography scheme owing to its outperforming attributes could improve the security, robustness, capacity, imperceptibility, and immunity against unknown attacks.

REFERENCES

- [1] A. S. Albahri *et al.*, “Role of biological data mining and machine learning techniques in detecting and diagnosing the novel coronavirus (COVID-19): a systematic review,” *J. Med. Syst.*, vol. 44, no. 7, pp. 1–11, 2020, doi: 10.1007/s10916-020-01582-x.
- [2] A. S. Albahri *et al.*, “Multi-biological laboratory examination framework for the prioritization of patients with COVID-19 based on integrated AHP and group VIKOR methods,” *Int. J. Inf. Technol. Decis.* vol. 19, pp. 1247–1269, 2020, doi: 10.1142/S0219622020500285.
- [3] M. Yildirim, “Steganography-based voice hiding in medical images of COVID-19 patients,” *Nonlinear Dyn.*, vol. 105, no. 3, pp. 2677–2692, 2021, doi: 10.1007/s11071-021-06700-z.
- [4] M. K. Abed, M. M. Kareem, R. K. Ibrahim, M. M. Hashim, S. Kurnaz, and A. H. Ali, “Secure medical image steganography method based on pixels variance value and eight neighbors,” in *2021 International Conference on Advanced Computer Applications (ACA)*, 2021, pp. 199–205, doi: 10.1109/ACA52198.2021.9626807.
- [5] A. H. Mohsin *et al.*, “PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture,” *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 14137–14161, 2021, doi: 10.1007/s11042-020-10284-y.
- [6] A. Durafe and V. Patidar, “Securing the COVID patients’ medical records using encrypted image steganography,” in *ICT Systems and Sustainability*, Springer, 2022, pp. 421–440, doi: 10.1007/978-981-16-5987-4_43.
- [7] K. Karampidis, E. Linardos, and E. Kavallieratou, “Stegopass–utilization of steganography to produce a novel unbreakable biometric based password authentication scheme,” in *Computational Intelligence in Security for Information Systems Conference*, 2021, pp. 146–155, doi: 10.1007/978-3-030-87872-6_15.




- [8] M. M. Hashim, S. H. Rhaif, A. A. Abdulrazzaq, A. H. Ali, and M. S. Taha, "Based on IoT healthcare application for medical data authentication: Towards a new secure framework using steganography," in *IOP Conference Series: Materials Science and Engineering*, vol. 881, no. 1, 2020, p. 12120, doi:10.1088/1757-899X/881/1/012120.
- [9] K. D. Abel, S. Misra, A. Agrawal, R. Maskeliunas, and R. Damasevicius, "Data security using cryptography and steganography technique on the cloud," in *Computational Intelligence in Machine Learning*, 2022, pp. 475–481, doi: 10.1007/978-981-16-8484-5_46.
- [10] A. H. Ali, A. D. Farhood, and K. N. Maham, "Analysis of a framework implementation of the transceiver performances for integrating optical technologies and wireless LAN based on OFDM-RoF," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, p. 4252, 2020, doi: 10.11591/ijece.v10i4.pp4252-4260.
- [11] M. Du, T. Luo, H. Xu, Y. Song, C. Wang, and L. Li, "Robust HDR video watermarking method based on the HVS model and T-QR," *Multimed. Tools Appl.*, pp. 1–21, 2022, doi: 10.1007/s11042-022-13145-y.
- [12] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, 2021, doi: 10.1007/s11042-020-10035-z.
- [13] V. Nandal and P. Singh, "Hybrid optimized image steganography with cryptography," in *Computational Methods and Data Engineering*, Springer, 2021, pp. 79–84, doi: 10.1007/978-981-15-7907-3_6.
- [14] V. Sabeti, M. Sobhani, and S. M. H. Hasheminejad, "An adaptive image steganography method based on integer wavelet transform using genetic algorithm," *Comput. Electr. Eng.*, vol. 99, p. 107809, 2022, doi: 10.1016/j.compeleceng.2022.107809.
- [15] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 2308–2312, doi: 10.1109/WiSPNET.2016.7566554.
- [16] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016, pp. 1206–1211, doi: 10.1109/ICACCI.2016.7732209.
- [17] D. R. Sridevi, P. Vijaya, and K. S. Rao, "Image steganography combined with cryptography," *Counc. Innov. Res. Peer Rev. Res. Publ. Syst. J. IJCT*, vol. 9, no. 1, 2013, doi: 10.24297/ijct.v9i1.4160.
- [18] M. M. Kareem, S. A. S. Lafta, H. F. Hashim, R. K. Al-Azzawi, and A. H. Ali, "Analyzing the BER and optical fiber length performances in OFDM RoF links," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 23, no. 3, pp. 1501–1509, 2021, doi: 10.11591/ijeecs.v23i3.pp1501-1509.
- [19] C. A. Sari, G. Ardiansyah, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *TELKOMNIKA (Telecommunication Comput. Electron. Control.)*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
- [20] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cogn. Syst. Res.*, vol. 60, pp. 20–32, 2020, doi: 10.1016/j.cogsys.2019.11.002.
- [21] A. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, "Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP," *J. Inf. Secur. Appl.*, vol. 58, p. 102808, 2021, doi: 10.1016/j.jisa.2021.102808.
- [22] D. R. I. M. Setiadi and J. Jumanto, "An enhanced LSB-image steganography using the hybrid canny-sobel edge detection," *Cybern. Inf. Technol.*, vol. 18, no. 2, pp. 74–88, 2018, doi: 10.2478/cait-2018-0029.
- [23] M. S. Taha, M. S. M. Rahem, M. M. Hashim, and H. N. Khalid, "High payload image steganography scheme with minimum distortion based on distinction grade value method," *Multimed. Tools Appl.*, pp. 1–34, 2022, doi: 10.1007/s11042-022-12691-9.
- [24] B. H. Hameed, A. Y. Taher, A. H. Ali, and Y. A. Hussein, "Based on mesh sensor network: design and implementation of security monitoring system with Bluetooth technology," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 26, no. 3, pp. 1781–1790, 2022, doi: 10.11591/ijeecs.v26i3.pp1781-1790.
- [25] M. J. Mnati, R. F. Chisab, A. M. Al-Rawi, A. H. Ali, and A. Van den Bossche, "An open-source non-contact thermometer using low-cost electronic components," *HardwareX*, vol. 9, p. e00183, 2021, doi: 10.1016/j.ohx.2021.e00183.
- [26] S. A. S. Lafta, M. M. Abdulkareem, R. K. Ibrahim, M. M. Kareem, and A. H. Ali, "Quality of service performances of video and voice transmission in universal mobile telecommunications system network based on OPNET," *Bull. Electr. Eng. Informatics*, vol. 10, no. 6, pp. 3202–3210, 2021, doi: 10.11591/eei.v10i6.3139.
- [27] M. A. Saad *et al.*, "Total energy consumption analysis in wireless Mobile ad hoc network with varying mobile nodes," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 2, 2019, doi: 10.11591/ijeecs.v20i3.pp1397-1405.
- [28] A. K. Sahu and G. Swain, "An optimal information hiding approach based on pixel value differencing and modulus function," *Wirel. Pers. Comm.*, vol. 108, no. 1, pp. 159–174, 2019, doi: 10.1007/s11277-019-06393-z.
- [29] S. A. Seyyedi, V. Sadau, and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *Int. J. Netw. Secur.*, vol. 18, no. 1, pp. 124–132, 2016, doi: 10.1109/WICT.2012.6409175.

BIOGRAPHIES OF AUTHORS



Mohanad Sameer Jabbar    is Assistant professor at Al-Bayan University, Baghdad, Iraq in Technical College of Engineering, medical instruments techniques Engineering Department where he has been a faculty member since 2021. His graduated with a B.Sc. degree in mathematics since from Mustansiriyah university, Baghdad, Iraq and an M.Sc. in computer science since from university of Singhania-Jhunjhunu, India in 2010. and Ph.D in computer science specialized in network and communication from university of Singhania-Jhunjhunu, India in 2013. He researches interest in the area of network, communication, and network security. He can be contacted at email: mohanad.s@albayan.edu.iq.



Samer Saeed Issa    is Assistant Professor at Al-Rafidain University College, Baghdad, Iraq, where he has been a faculty member since 2010. His graduated with a BSc. Degree in computer science from University of Technology-Baghdad, Iraq, in 1999, and an M.Sc. in Data Security from University of Technology-Baghdad, Iraq, in 2002, and Ph. D from Iraqi Commission for Computers and Informatics/Informatics institute for post graduate Studies-Baghdad in 2006. He researches interests in the area of network and data security. He can be contacted at email: Samer.saeed.elc@ruc.edu.iq.