IEEE *Access*

SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT

SACHIN DHAWAN [ID]1, CHINMAY CHAKRABORTY [ID]2,
JAROSLAV FRNDA [ID]3, (Senior Member, IEEE),
RASHMI GUPTA1, ARUN KUMAR RANA4,
AND SUBHENDU KUMAR PANI [ID]5

1NSUT, East Campus [Formerly AIACTR, Delhi 110031, India (Affiliated to Guru Gobind Singh Inderaprastha University)], Dwarka 110078, India
2Department of Electronics and Communication Engineering, Birla Institute of Technology, Mesra 835215, India
3Department of Quantitative Methods and Economic Informatics, Faculty of Operation and Economics of Transport and Communications, University of Žilina,
01026 Žilina, Slovakia
4Panipat Institute of Engineering and Technology, Samalkha 132102, India
5Krupajal Computer Academy, Biju Patnaik University of Technology (BPUT), Rourkela 751002, India

Corresponding author: Chinmay Chakraborty (cchakrabarty@bitmesra.ac.in)

This work was supported by Slovak Grant Agency for Science (VEGA) under Grant 1/0157/21.

ABSTRACT Internet of Things (IoT) is a domain where the transfer of big data is taking place every single second. The security of these data is a challenging task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are crucial when dealing with user authentication and data privacy. In the proposed work, a highly secured technique is proposed using IoT protocol and steganography. This work proposes an image steganography procedure by utilizing the combination of various algorithms that build the security of the secret data by utilizing Binary bit-plane decomposition (BBPD) based image encryption technique. Thereafter a Salp Swarm Optimization Algorithm (SSOA) based adaptive embedding process is proposed to increase the payload capacity by setting different parameters in the steganographic embedding function for edge and smooth blocks. Here the SSOA algorithm is used to localize the edge and smooth blocks efficiently. Then, the hybrid Fuzzy Neural Network with a backpropagation learning algorithm is used to enhance the quality of the stego images. Then these stego images are transferred to the destination in the highly secured protocol of IoT. The proposed steganography technique shows better results in terms of security, image quality, and payload capacity in comparison with the existing state of art methods.

INDEX TERMS Steganography, encryption, embedding process, salp swarm optimization, hybrid fuzzy neural network.

I. INTRODUCTION

In today's era security of confidential data is most important and developments in the field of computer security have presented steganography as a better method of obtaining secured data [1], [2]. Steganography is the process of hiding secret data that can be in the form of a message, audio, image, or video into another image, audio, message, or video using embedding processes [3]–[5]. It is employed to protect secret data from malicious attacks [6], [7]. The amount of data

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Khurram Khan [ID].

exchanged via the internet is increasing nowadays. Hence, Data security is termed as a serious issue while communication of data is processed over the internet. Dual techniques namely steganography and cryptography are used to provide secure information [8], [9]. To provide more security to the data, cryptography is used together with the steganography technique [10], [11]. Both methods play a significant role in information security [12].

With the help of cryptography, secret data can be easily encrypted [13]. Some of the main goals of cryptography are integrity, authentication, and confidentiality [14]. Then, the steganography process hides the encrypted data so that

nobody can suspect that there exists secret data [15]. Normally, the steganography system includes three components such as cover-object, secret data, and stego-object. If the information is embedded in an image file (cover image) then the outcome is a stego-image object. Likewise, for the case of video, audio, and text for embedding with the following outcomes as stego-video, stego-audio, and stego-text respectively [16]. There are different types of covers in which secret information can be embedded. The Steganography approach seems to be a good one if it considers three parameters for the processing which means capacity, security, and image quality.

Generally, the steganography methods conceal an equal number of secret bits into each pixel of the cover image. Hence, they cause an equal degree of embedding distortion in the cover image. But, the individual pixels of any digital image exhibits complex statistical dependencies between them. Thus, the quality of the image is automatically reduced while performing an equal number of bits changes in all pixels of the cover image. To tackle these issues different adaptive embedding processes have been introduced in the steganography process [17]. This adaptive embedding process embeds a variable number of bits in each pixel of the cover image [18]. Thus, most of the researchers focused on these adaptive techniques to improve the security of steganography methods [19]. Furthermore, the quality of edge pixels is not much affected after making changes during the embedding process. Thus, more secret bits can be embedded into edge pixels than smooth pixels [20]. The metaheuristic algorithms are used in most applications to solve optimization issues [21].

NarasimhaRao [22] proposed a work to protect IoT communicated data in the cloud which is connected through the internet. A complex encryption and decryption technique is proposed to provide high data security. Only encryption and decryption is implemented, but data hiding is presenting in this paper and has more advantage that the existing works.

Shehab *et al.* [23], surveyed a comprehensive study on security issues in IoT networks. Various security requirements such as authentication, integrity, confidentiality were discussed. A comparative study of different types of attacks, their behavior, and their threat level that categorized into low-level, medium-level, high-level, and extremely high-level attacks and suggested possible solutions encounter these attacks were provided.

Now a day's protection of data with high payload capacity is the most important task while communicating secret data. In our proposed technique combination of Salp Swarm Optimization Algorithm and adaptive embedding, provides higher security as well as high payload capacity. Moreover, based on the proposed technique, various real-world tasks can be achieved easily. In the medical field, this technique will be very helpful like in an X-Ray copy, the details of the patient and their health problem can be stored without disturbing the X-ray film quality. This detail can only be detected with a key available to the diagnosing doctor. Similarly, the details of an original artist can be hidden within a painting/artwork.

A. MOTIVATION AND CONTRIBUTION

This work is principally motivated toward the improvement of new techniques to survive these impediments and to give better protection from existing steganalysis techniques. The particular issues in such a manner are momentarily examined underneath: One of the significant disadvantages of embedding in different bit planes is that a huge amount of noise is added because of this interaction. The interloper may attempt a counter assault by making a few changes to counter existing strategies. This is the motivation that there is a need to generate a technique for producing robust techniques with high-quality stego images and a high payload capacity of steganography.

The main contribution of this work is summarized as follows:

1. In this paper, a secured image steganography method is proposed based on an adaptive embedding process.
2. To increase the security of the hidden (secret) image, the hidden image is initially encrypted using a bit-level image encryption algorithm. This encryption method requires a single round of bit-level permutations but in two phases (diffusion and confusion stage) for giving excellent performance.
3. Also, a Salp Swarm Optimization Algorithm-based adaptive embedding process is proposed to embed the encrypted data into the cover image. This process embeds the secret data efficiently by setting optimal parameter values to smooth and edge blocks. Thus, the proposed method automatically increases the payload capacity with less distortion rate.
4. A hybrid Fuzzy Neural Network with a backpropagation learning algorithm is used to enhance the quality of the stego images. Then these stego images are transferred to the destination in the highly secured protocol of IoT.
5. The experiment is tried with different secret pictures and cover pictures and ensured that the created stego-picture has no noise or information loss.

The rest of the paper is structured as follows: Section 2 provides some related works on image steganography. Section 3 gives the detail about the proposed steganography method. Section 5 presents the simulation results and a comparison with existing works. Finally, the paper is concluded in Section 6.

II. RELATED WORKS

Some of the recent related works on image steganography are listed as follows:

Sun *et al.* [24] proposed Cloud Eyes, a cloud-based anti-malware system. The proposed system provided efficiently and trusted security services to the devices in the IoT network. Ukil *et al.* [25] studied the requirements of embedded security, provided methods and solutions for resisting cyber-attacks, and provided technology for tamper-proofing the embedded devices based on the concept of trusted computing.

Bairagi *et al.* [26] proposed three-color image steganography approaches for protecting information in an IoT infrastructure. The first and third approaches use three (red, green, and blue) channels, while the second approach uses two (green and blue) channels for carrying information. Dynamic positioning techniques have been used for hiding information in the deeper layer of the image channels with the help of a shared secret key.

Anwar *et al.* [27], developed a technique to secure any type of image especially medical images. They aimed to maintain the integrity of electronic medical information, ensuring the availability of that information, and authentication of that information to ensure that authorized people only can access the information. First, the AES encryption technique was applied in the first part. The ear print was also embedded in this work, where seven values were extracted as feature vectors from the ear image. The proposed technique improved the security of medical images by sending them via the internet and secured these images from being accessed by any unauthorized person.

Abdelaziz *et al.* [28], surveyed the analysis of the security vulnerabilities and the risk factors detected in mobile medical apps. According to risk factor standards, these apps can be categorized into remote monitoring, diagnostic support, treatment support, medical information, education and awareness, and communication and training for healthcare workers. Eight security vulnerabilities and ten risk factors detected by the World Health Organization (OWASP) mobile security project in 2014 have been analyzed.

Abdur *et al.* [29], proposed a fused security approach based on encryption, steganography, and watermarking techniques. It decomposed into three stages; (1) encrypting the cover image using XOR operation, (2) embedding process done using least significant bits (LSBs) for generating the stego-image, then (3) watermarking the stego-image in both spatial and frequency domains. Experimental results proved that the proposed method was very much efficient and secured.

Jain *et al.* [30], proposed a new technique for transferring the patient's medical information into the medical cover image by hiding the data using the decision tree concept. The coding is done in the form of different blocks that are evenly distributed. In concealment, secret code blocks are assigned to the cover image to insert the data by the mapping mechanism based on breadth-first search. RSA algorithm was used to encipher the data before embeddings.

Yehia *et al.* [31], surveyed various healthcare applications based on wireless medical sensor networks (WMSN) [32] that can be implemented in an IoT environment. Also, discussed the security techniques are used for handling the security issues of healthcare systems especially hybrid security techniques. Zin May Zaw [33], presented an algorithm based on dividing the original image into a group of blocks, where these blocks are arranged in the form of turns using a transformation algorithm. After that, the transformed image is encrypted using the Blowfish algorithm. It was found

that the correlation decreases and the entropy increase by increasing the number of blocks through using smaller block sizes.

Anupriya and Sarita [34] discussed the performance evaluation of secret image steganography approaches for data and image security. Pranab *et al.* [35] developed Modified LSB (MLSB) substitution and data mapping methods for image steganography. At first, the secret image was pre-processed using the data mapping approach and embedded into the host image using MLSB.

In general, most of the LSB methods were not depending on pixel correlation and the contents of the images. Thus, it could be identified through RS analysis. Hence, there is a requirement for certain protective measures for increasing the security of LSB-based steganography methods. To tackle this issue, an edge detection process has been included in the LSB-based steganography method. Also, the secret images should be encrypted before embedding them into the cover image for increasing the security level. The security level of certain existing methods has been reduced because of the lack of encryption algorithms before the embedding process. Odelu *et al.* [36] proposed another RSA-based CP-ABE conspire with consistent size secret keys and ciphertexts. Then demonstrated to be secure against a picked ciphertext foe, just as being an effective arrangement with the expressive AND door access structures. The proposed plot in this paper is appropriate for arrangement on battery-restricted cell phones.

Yaseen *et al.* [37] used Vernam cipher algorithm to encrypt the secret image. Here, the keystream was generated with the help of Geffe Generator. But, this Geffe Generator is not a secure one. Then, hybrid Kirchand Sobel edge detectors were used to localize the edges of the cover image. Then, the LSB method was used to hide the secret image into the cover image. Hemalatha *et al.* [38] utilize the behavior of animals i.e particle swarm optimization algorithm for better embedding rate and better visual quality. Maheshwari *et al.* [39] utilize the two optimization techniques Genetic Algorithm (GA) and Particle Swarm Optimization used for improving the performance of the hiding process of steganography system. Mohsin *et al.* [40] give novel image steganography based on particle swarm optimization (PSO) algorithm in which secret data concealed based on pixel selection in the spatial domain, for high embedment capacity. Fazli *et al.* [41] give the technique of Particle Swarm Optimization (PSO) [62] algorithm to search best ways and to search best substitution matrix for transforming the secret message in each block, instead of finding only one optimal substitution matrix for the whole cover-image.

The character-based bunch check conspire was recently proposed to make VANET safer and productive for practical use. Tzeng *et al.* [42] bring up that the current IBV conspire exists some security hazards. This paper gives an improved plan that can fulfill the security and protection wanted by vehicles. The proposed plot gives the provable security in the arbitrary prophet model.

Mohsin *et al.* [40] give the novel strategy of Image Steganography in Spatial Domain based on Particle Swarm Optimisation Algorithm for High Embedding Capacity.

Khan [43] unique mark biometric-based self-validation and deniable confirmation plans, which empower a recipient to recognize the wellspring of the message however not to demonstrate the personality of the sender to an outsider.

EL-Latif *et al.* [44] present another system for secure data in fog cloud IoT. In the system, the client in one area installs his/her significant information through the proposed quantum steganography convention and transfers the covered information to the haze cloud. The proposed recipient in another area gets the information from the mist cloud and concentrates the planned substance through the proposed extraction approach.

Khan and Alghathbar [45] give the technique to conquer the inborn security shortcomings of the 2-factor authentication technique, we propose enhancements and security fixes that endeavor to fix the susceptibilities of his plan. The proposed security upgrades can be joined in the 2-factor authentication technique for accomplishing a safer and vigorous two-consider client verification WSNs.

Elhoseny *et al.* [46] give a hybrid security model for getting the indicative content information in medical images. The proposed mixture encryption blueprint is fabricated utilizing a combination of Progressed Encryption Standard, and Rivest, Shamir, and Adleman calculations.

Waqar *et al.* [47] propose a technique for cloud users' data privacy dependent on information base construction updates and dynamic reproduction of meta information for the conservation of security.

Khari *et al.* [12] proposed the elliptic Galois cryptography protocol. In this protocol, a cryptography technique is used to encrypt confidential data that came from different medical sources.

Horng *et al.* [48] give a safe plan that can accomplish the security and protection prerequisites, and conquer the shortcomings of SPECS. Additionally, this paper shows the effectiveness benefits of the plan through execution assessments as far as confirmation postponement and transmission overhead.

Meng *et al.* [49] proposed novel steganography dependent on picture to-picture interpretation by adding steganography module and steganalysis module to CycleGAN, adjusting to the secret correspondence and protection safeguarding of the IoT [60], [61]. Steganalysis network is utilized to improve the counter recognition capacity of stego picture

One of the most mainstream versatile hiding processes is pixel difference histogram (PVD) steganography. This strategy implanted more confidential information into edge portions and less information into smooth portions. Pradhan *et al.* [50] joined LSB, PVD, and Exploiting modification direction (EMD) techniques to shape another half and half picture steganography algorithm. Here, the edge zone utilized consolidated LSB and PVD, while the smooth zone utilized the combined LSB and EMD approach. However, they have not utilized any encryption cycle for mystery

pictures and there is no ideal calculation for edge and smooth pixel ID. The proposed algorithm attempts to take care of all the issues related to the current algorithms by building up effective mystery picture encryption calculations and a proficient Salp Swarm Optimization Algorithm-based versatile installing measure.

III. PROPOSED METHODOLOGY

In this work, IoT-based Secured and high-quality Steganography is proposed using hybrid algorithms for Big Data. Steganography technique is proposed for communicating secret data based on encryption. Normally, the digital image includes dissimilar picture elements named pixels. In this work, a grayscale image is used as a cover image. Therefore, an image is represented by an array that includes many bytes. The proposed system mainly includes four sections: Image encryption, Embedding phase, Quality enhancement, and Extraction phase. The block diagram of the proposed steganography scheme is shown in Figure 1. As shown in figure 1, Initially, the image of Lena is considered as cover, and the image of the Aeroplane is considered as a hidden image. Here, the size of the secret data should be less than the size of the cover image. Then, the hidden image is converted into a cipher image using Binary bit-plane decomposition (BBPD) based image encryption. This encryption algorithm is worked based on piecewise linear chaotic maps (PWLCM).

The next stage is the embedding phase, where the secret data gets embedded into the cover image. In this embedding process, the smooth and edge portion of the image is obtained by setting an objective function for *Salp Swarm Optimization Algorithm* based on the Manhattan Distance operator. The bigger the output of the objective functions the high the probability of edge presence. Hence, the automatic thresholding function is used to identify the edge pixels in the image. Then, the pixel values in the hidden image are embedded into the cover image based on the steganographic embedding function. This process will use different parameter values for edge and smooth areas. Finally, we will obtain the stego-image. But, the quality of this stego image is not good enough. Thus, a hybrid Fuzzy Neural Network (HFNN) with a back-propagation learning algorithm is used to enhance the quality of the stego images. This network contains two sections: a fuzzy processing unit and a conventional backpropagation network. A membership function is used in the fuzzy processing unit to process the inputs and the processed data will be given as input to the backpropagation network for further processing. Then, the output is compared with the expected output and the network connection weights are adjusted based on the mean squared error to obtain good quality images. Further, stego images with enhanced quality are transferred through IoT protocol with higher security as shown in the figure. As shown in Figure 1, the IoT makes it possible to connect a wide range of smart devices to the internet. The evolution of medicine can be aided by IoT by incorporating sensors such as environmental sensors inside the internal
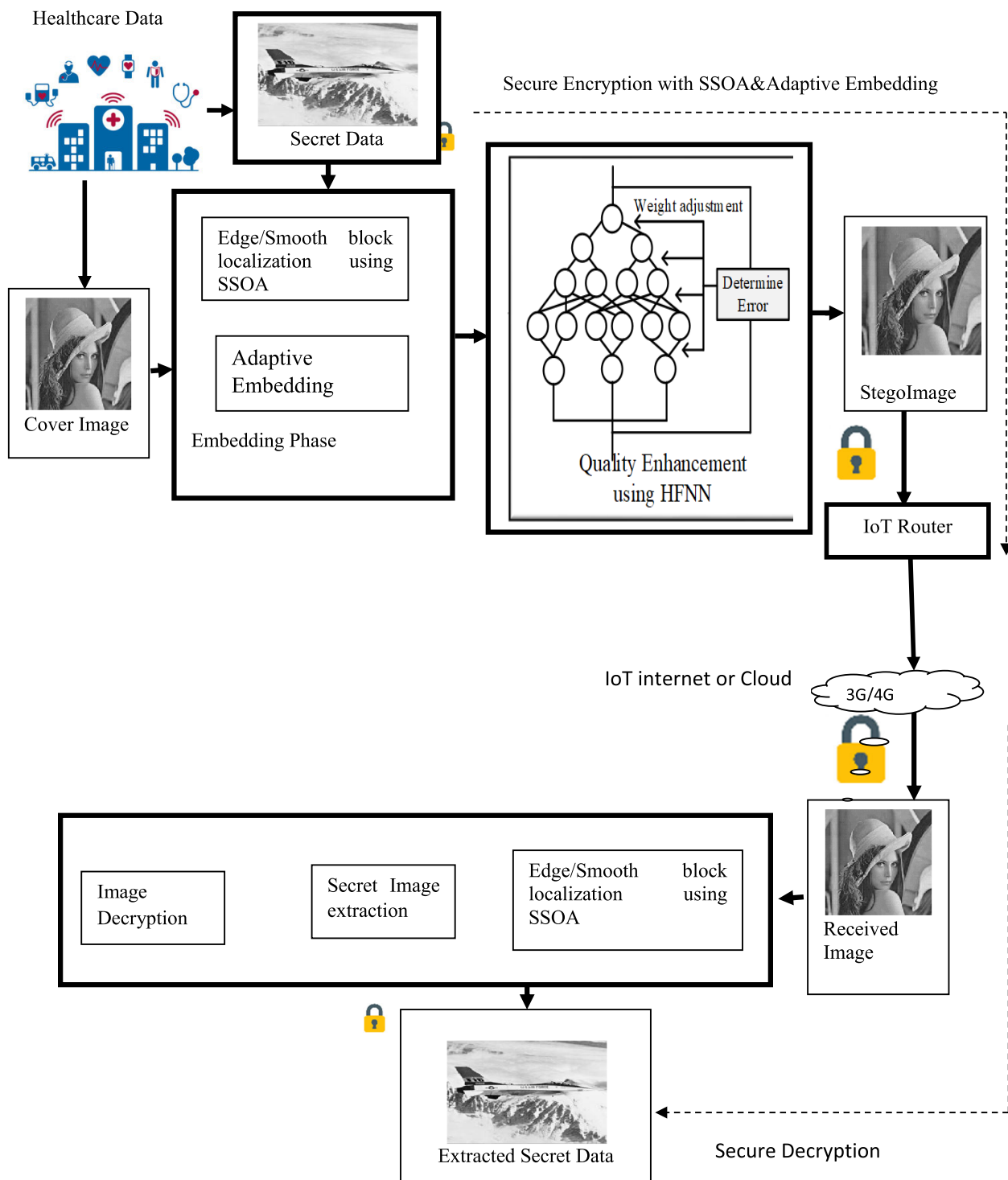
FIGURE 1. Block diagram of the proposed steganography scheme.

environment of a small room with the specific purpose of monitoring a person's health with a type of assistance that can be controlled remotely. In this paper, IoT is used to propose digital image steganography as a method to improve medical data security, confidentiality, and integrity. When embedding additional data within medical images, medical image steganography requires extreme caution because the additional data must not degrade the image quality. Many of the medical diagnosis exploration systems are based on medical study images. In the IoT scenario, combining encryption

and steganography can ensure secure data transfer over the internet.

The next process is extraction which includes the same steps for data embedding but in reversible order.

A. IMAGE ENCRYPTION

In the hidden image encryption process, a BBPD method is used to decompose the hidden image into eight binary bitplanes [51]. This BBPD method gives binary representation $(b_{m-1}, \ldots, b_1, b_0)$ for the non-negative decimal number D as given below:

$$D = \sum_{j=0}^{m-1} b_j \cdot 2^j = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \ldots + b_{m-1} \cdot 2^{m-1} \quad (1)$$

The pixel values of the grayscale images are in the range of [0, 255]. Hence, they are decomposed into eight binary bitplanes.

The encryption module contains two Stages: The diffusion stage and the Confusion stage. Here, two binary keystreams are generated with the help of a secret key, $K_1 (y_0, \delta_1)$ before entering into the diffusion and confusion stage. The key streams are generated using a piecewise linear chaotic map (PWLCM). The PWLCM [30] is defined as follows:

$$y_{j+1} = F\left(y_j, \delta\right) = \begin{cases} y_j / \delta & y_j \in [0, \delta) \\ (y_j - \delta) / (0.5 - \delta) & y_j \in [\delta, 0.5) \\ F\left(1 - y_j, \delta\right) & y_j \in (0.5, 1) \end{cases} \quad (2)$$

where $\delta \in (0, 0.5)$ represents the control parameter and $y_j \in (0, 1)$ represents the initial condition for PWLCM. The initial value of y_0 and δ_1 should be set for encrypting the hidden image of size $M \times N$. Then, the PWLCM map is iterated $M \times N$ times to obtain the chaotic sequence or keystream $Y = \{y_1, y_2, \ldots y_{MN}\}$. Then, this $Y(j)$ is converted into an integer sequence $Y_1(j)$ using the following expression:

$$Y_1 = \mod \left(floor \left(Y \times 10^{14} \right), 256 \right) \quad (3)$$

Then, BBPD is used to decompose the keystream Y into 8 bitplanes. Then, these bitplanes are grouped into two groups to obtain binary sequences k_1 and k_2. These groups are formed by arranging the bits from left to right and higher bitplane to lower bitplane.

1) DIFFUSION STAGE

The following steps are performed in the diffusion stage.

1. Add all the elements P_2 as given below:

$$S_1 = \sum_{j=1}^{4MN} P_2(j) \quad (4)$$

2. Perform cyclic shift operation in P_1 the matrix to obtain P_{11}. Here, the elements in P_1 the matrix are right-shifted by S_1 bits.
3. Encrypt the 1st element of P_{11} with the previous element of P_{11} and the 1st element of P_2 with the first element

of k_1 as given below:

$$Q_1(j) = P_{11}(j) \oplus P_{11}(j-1) \oplus P_2(j) \oplus k_1(j) \quad (5)$$

4. Add all the elements Q_1 as given below:

$$S_2 = \sum_{j=1}^{4MN} Q_1(j) \quad (6)$$

5. Perform cyclic shift operation in P_2 the matrix to obtain P_{22}. Here, the elements in P_2 the matrix are right-shifted by S_2 bits.
6. Encrypt the 1st element of P_{22} with the previous element of P_{22} and the 1st element of Q_1 with the first element of k_2 as given below:

$$Q_2(j) = p_{22}(j) \oplus p_{22}(j-1) \oplus Q_1(j) \oplus k_2(j) \quad (7)$$

2) CONFUSION STAGE

The following steps are performed in the confusion stage:

1. Add all the elements in Q_1 and Q_2 as given below:

$$S_3 = \sum_{j=1}^{4MN} Q_1(j) + Q_2(j) \quad (8)$$

2. Generate keystream Z_1 and Z_2 using the secret key $K_2(z_0, \delta_2)$. The following expression is used to generate the initial value a_0

$$a_0 = \mod \left(z_0 + S_3 / 4MN, 1 \right) \quad (9)$$

Generate a new chaotic sequence $A = \{a_1, a_2, \ldots a_{2MN}\}$ by iterating PWLCM $2 \times 4MN$ times. Subsequently, A is divided into two equal sequences:

$$A_1 = \{a_1, a_2, \ldots a_{4MN}\} \quad (10)$$
$$A_2 = \{a_{MN+1}, a_{MN+2}, \ldots a_{4MN}\} \quad (11)$$

Then, these sequences A_1 and A_2 are converted into integer sequence Z_1 and Z_1 using the following expression:

$$Z_1 = \mod \left(floor \left(A_1 \times 10^{14} \right), 4MN \right) + 1 \quad (12)$$
$$Z_2 = \mod \left(floor \left(A_2 \times 10^{14} \right), 4MN \right) + 1 \quad (13)$$

3. Obtain the encrypted row vector R_1 by swapping the elements in Q_1 and Q_2 as given below:

$$temp = Q_1(j) \quad (14)$$
$$Q_1(j) = Q_2(Z_1(j)) \quad (15)$$
$$Q_2(Z_1(j)) = temp \quad (16)$$

4. Obtain the encrypted row vector R_2 by swapping the elements in Q_1 and Q_2 as given below:

$$temp = Q_2(j) \quad (17)$$
$$Q_2(j) = Q_1(Z_2(j)) \quad (18)$$
$$Q_1(Z_2(j)) = temp \quad (19)$$

5. Transform the row vectors R_1 and R_2 into $M \times N$ the image to obtain the cipher image.

B. SALP SWARM OPTIMIZATION ALGORITHM (SSOA) BASED ADAPTIVE EMBEDDING

The pixel values of the cover images are in the range of [0, 255]. In this work, the secret image data is embedded in both smooth region and edge region by setting different parameter values in the steganography embedding function. In the proposed embedding process, the smooth and edge pixels of the image are obtained by setting an objective function for *Salp Swarm Optimization Algorithm (SSOA)* [52] based on the Manhattan Distance operator (l_1-norm) [53]. The maximum value of the objective function represents the existence of edges. Then, the secret bit values are embedded into the cover image based on the steganography embedding function [54]. This process will use different parameter values for edge and smooth areas. Finally, we will obtain the stego-image.

1) EDGE/SMOOTH BLOCK LOCALIZATION

In this work, an SSOA algorithm is proposed to localize the edge/smooth pixels in the cover image by identifying optimal threshold value based on the maximization of the objective function (Manhattan Distance operator (l_1-norm)). The SSOA is a population-based optimization algorithm that mimics the swarm behavior of salps in nature. The SSOA begins with the random initialization of individuals. The swarm of salps consists of two kinds of individuals: a leader and followers.

To localize the edge/smooth block, m salps are dispensed on an image C with a size of $M \times N$ in a random manner. The 2-D representation for the swarm S of m salps is given in (20). Here, the food source (i.e., optimal threshold) is considered as the target of this swarm in the search space called T. After initializing the population as in (20), the fitness of each search agent should be determined to obtain the optimal threshold value for edge detection. Here, the l_1-norm is computed by each salp in the SSOA. When any salp discovers itself in the pixel positioned at (i, j) of cover image C, the Manhattan Distance of all 8-neighboring pixels from the center pixel r is calculated using (21).

$$
S_i = \begin{bmatrix} s_1^1 & s_2^1 & \cdots & s_n^1 \\ s_1^2 & s_2^2 & \cdots & s_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^m & s_2^m & \cdots & s_n^m \end{bmatrix}
\tag{20}
$$

This objective function determines the discrete derivatives of the neighboring pixels to provide evidence for the existence of edge pixels. The maximum value of the objective function represents the higher chance of edges.

$$
\begin{aligned}
f = & \left| C_{((i-1),(j-1))} - r \right| + \left| C_{(i-1,j)} - r \right| + \left| C_{(i-1,j+1)} - r \right| \\
& + \left| C_{(i,j-1)} - r \right| + \left| C_{(i,j+1)} - r \right| + \left| C_{(i+1,j-1)} - r \right| \\
& + \left| C_{(i+1,j)} - r \right| + \left| C_{i+1,j+1} - r \right|
\end{aligned}
\tag{21}
$$

where $|\cdot|$ represents the operator for getting absolute values and r represents the center pixel at a position (i, j) within the

cover image C, wherein the latest salp is positioned. After obtaining the fitness of all salps, the best search agent is considered the leader salp. In SSOA, the location of the leader particle is computed as:

$$
s_j^1 = \begin{cases} T_j + \varepsilon_1 \left(\left(B_U^j - B_L^j \right) \varepsilon_2 + B_L^j \right) & \varepsilon_3 \geq 0.5 \\ T_j - \varepsilon_1 \left(\left(B_U^j - B_L^j \right) \varepsilon_2 + B_L^j \right) & \varepsilon_3 < 0.5 \end{cases}
\tag{22}
$$

where s_j^1 represents the position of leader and T_j represents the position vector of food source, B_U^j and B_L^j represents the upper and lower bounds respectively. ε_2 and ε_3 are random values in the range of 0 and 1. The important parameter ε_1 is determined using the following expression

$$
\varepsilon_1 = 2 e^{-\left(\frac{4n}{N_{\max}} \right)^2}
\tag{23}
$$

Here, n and $N_{\max}$ represents the present and a maximum number of iteration. Afterward, SSOA updates the follower's positions using

$$
s_j^i = 0.5 \times \left(s_j^i + s_j^{i-1} \right)
\tag{24}
$$

where s_j^i represents the position of ith follower in j^{th} dimension. In SSOA, all the salps are initiated randomly. Then, the fittest salp is selected by evaluating the objective function of all salps. Equations (22) and (24) are used to update the position vectors of leaders and followers respectively. In the meantime, the parameter ε_1 is updated using (23). These processes are repeated until the maximum number of iterations to return the best threshold value T for edge detection. The algorithm for getting optimal threshold using the SSOA algorithm is provided in Algorithm 1.

After obtaining the edge/smooth pixels of the cover images using the optimal threshold value, the cover image is divided into non-overlapping k-pixel blocks and their corresponding gray values are $g = (g_1, g_2, \ldots g_k)$. Based on the presence of edge pixels, the blocks are identified as edge block and smooth block as given in (25)

$$
class = \begin{cases} edgeblock & if \ N_e > N_s \\ smoothblock & if \ N_e < N_s \end{cases}
\tag{25}
$$

where, N_e and N_s represent several edge pixels and smooth pixels respectively.

2) EMBEDDING PROCESS

During the embedding process, the proposed method uses two different parameter values in the steganography embedding function. Specifically, the low parameter values ρ_l and $b_s = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_l}{j} \times 2^j$ are used by the smooth blocks. Alternatively, high parameter values ρ_h and $b_e = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_h}{j} \times 2^j$ are used by the edge blocks. The detailed steps for the embedding process of each k-pixel block are listed below:

Algorithm 1 SSOA Algorithm for Edge/Smooth Pixel Localization

1. Initialize a maximum number of iterations $N_{\max}$, population size m, parameters of SSOA, and define the objective function.
2. Initialize the positions of salps on cover image C in a random manner
3. Set $n := 1$
4. Repeat
5. Calculate the fitness function of each search agent positioned at the coordinate (i, j) of the cover image C using (21)
6. Select T as the best search agent
7. Adjust the main parameter of SSOA ε_1 using (23)
8. for $(i = 1 : i \leq m)$ do
9.   if $i == 1$ then
10.   Update leader's position using (22)
11.   else
12.   Update follower's positions using (24)
13.   end for
14. Check whether any search agent does not belong to the upper and lower bounds and amend it.
15. Determine the fitness function of the search agent.
16. Update T if there is a better solution
17. Set $n = n + 1$
18. until $n < N_{\max}$
19. Return optimal T

---

1. Compute the steganography embedding function $F(g) = Ag^T \bmod b_1$, where $b_1 = b_s$ and $\rho_1 = \rho_l$ for smooth block, $b_1 = b_e$ and $\rho_1 = \rho_h$ edge block. Also, $A = (a_1, a_2, \ldots a_k)$, $a_j = (2\rho_1 + 1)^{j-1}$
2. Compute $u = \bmod(s, b_1)$ and $d = u - F(g) \bmod b_1$, where, s represents the encrypted bit values in the secret image. The pixels in the k-pixel block are not modified when $d = 0$. Then, the secret value s is replaced with $(s - u)/b_1$ and the pixel values are modified by running the next k-pixel block. If $d > 0$ the move to step 3.
3. Determine the vector v by considering the condition $F(v) = d$ and $\|v\|_1 \leq \rho$.
4. Compute $g' = (g'_1, g'_2, \ldots g'_k)$ using $g' = g + v$ and $g' = (g'_1, g'_2, \ldots g'_k)$ is adjusted to $g'' = (g''_1, g''_2, \ldots g''_k)$, if the stego-pixel value is affected by over/underflow problems as given below:

$$g'' = \begin{cases} g' - b_1 & g' > 255 \\ g' + b_1 & g' < 0 \\ g' & 0 \leq g' \leq 255 \end{cases} \quad (26)$$

5. Check the block $g'' = (g''_1, g''_2, \ldots g''_k)$ using the optimal threshold value obtained from the proposed edge localization algorithm to identify whether it belongs to smooth block or edge block. When the block type (edge/smooth) of g'' is as same g, no modification is needed. Because the secret digits have been embedded

effectively. Then, the block g and the secret value s are replaced with block g'' and $(s - u)/b_1$ respectively. When the block type g'' is not the same as g efficient extraction of the secret digit is not possible at the receiver side. Thus, one should move to adapt step 6.
6. This adapting step contains two events:
Event 1: Modify the pixels values for guaranteeing the same block type as the block before embedding. Determine $v^1 = v^1_1, v^1_2, \ldots v^1_k$ by considering the following conditions. (i) block g and $g' = g + v^1$ should be in the same block type. (ii) $F(g + v^1) = u$. (iii) $0 \leq g + v^1 \leq 255$. (iv) the value $\|v^1\|_2$ is minimized.
Event 2: Adjust the embedding secret digit in the k-pixel block. If $b_1 = b_s$ then $b_2 = b_e$, Otherwise, $b_2 = b_s$. Compute $u' = \bmod(s, b_2)$. Then, the digit u' is embedded into the block. Determine $v^2 = v^2_1, v^2_2, \ldots v^2_k$ by considering the following conditions: (i) block g and $g' = g + v^2$ should be indifferent block types. (ii) $F(g + v^2) = u'$. (iii) $0 \leq g + v^2 \leq 255$. (iv) the value $\|v^2\|_2$ is minimized.
7. Here, event 1 will provide a higher payload with minimum embedding distortion when $\frac{\log_2 b_1}{\|v^1\|_2} > \frac{\log_2 b_2}{\|v^2\|_2}$. Then, the block g and the secret value s are replaced with block $g + v^1$ and $(s - u)/b_1$. For the other condition, event 2 will provide a higher payload with minimum embedding distortion. In this event, the block g and the secret value s are replaced with block $g + v^2$ and $(s - u')/b_2$ respectively. Repeat the above steps up $s = 0$ for obtaining the stego image. The example for embedding using SSOA optimized adaptive embedding process is shown in Figure 2.

In this example, the image is divided into the 4-pixel block. Then, the parameter value for the smooth and edge blocks are considered as $\rho_l = 2$ and $\rho_h = 3$. Here, the secret bits from the hidden image are considered as $s = 11010000$. Then the secret data is embedded using the steps (1-7) presented in the embedding process to get the stego image. But, the quality of this stego image is not good enough. Thus, the quality of this stego image is enhanced using HFNN with a backpropagation learning algorithm.

C. QUALITY ENHANCEMENT USING HFNN WITH BACKPROPAGATION LEARNING

The quality of the obtained stego image is not good enough. Hence, there is a requirement for a post-processing method based on the specific intelligent system. This stage is required for the reduction of probabilities of statistical identification and other kinds of image manipulation attacks. In this work, an HFNN with a Backpropagation learning algorithm is used to enhance the quality of the image. Generally, neural networks resemble inhomogeneous HFNN. Neural networks are defined as a framework that can mimic the way the human brain learns [55]. The block diagram representation for stego image quality enhancement using HFNN is shown in Figure 3. Here, the stego image is converted into binary bit
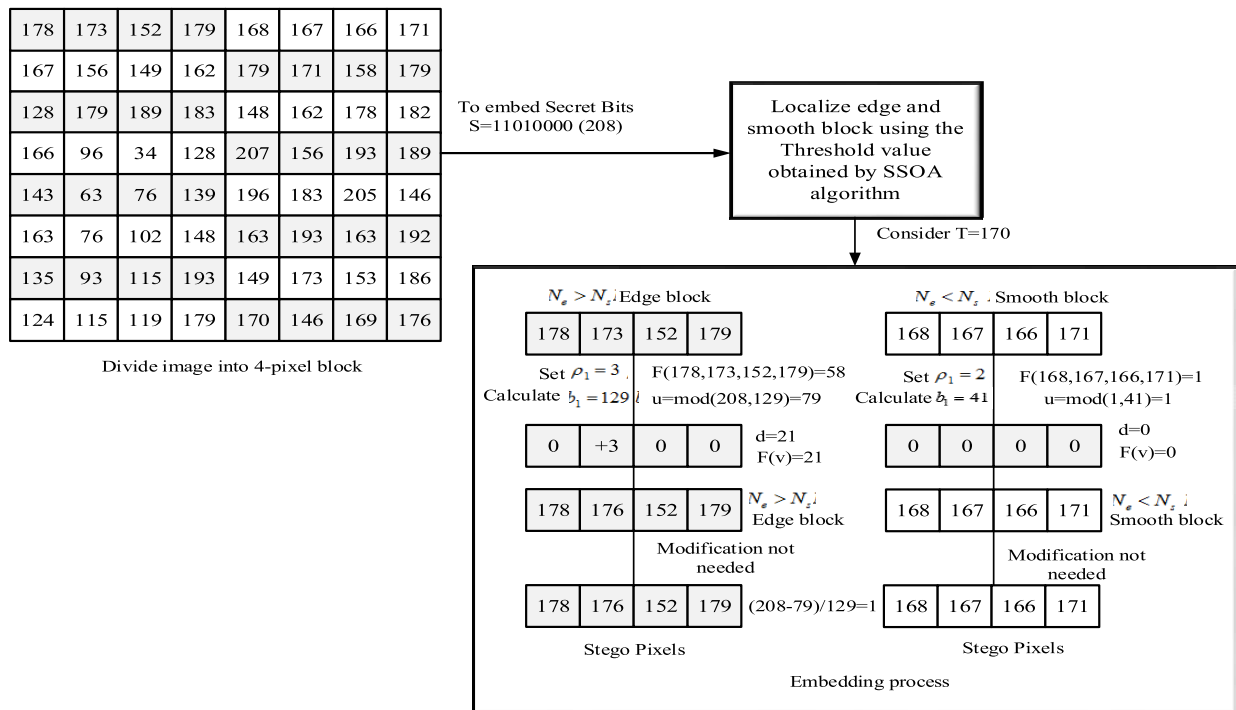
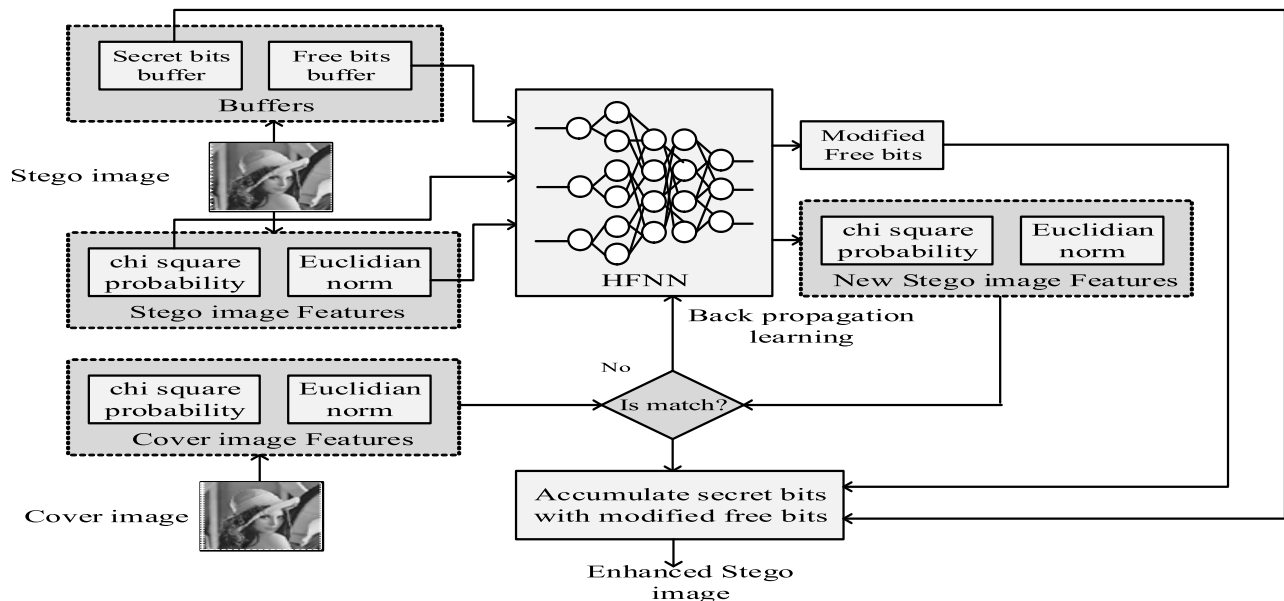**FIGURE 2.** Example for SSOA optimized adaptive embedding.

FIGURE 3. Stego image quality enhancement using HFNN.

values for the identification of the free bits and the bits that embrace secret bits. A buffer is constructed for holding the free bits that are not utilized by the embedding process.

Furthermore, the statistical and visual features [63] are extracted from the stego and cover images. Here, the chi-square probability and the Euclidian norm are used to represent the statistical and visual features respectively. The free bits buffer and the two features of the stego image are given as input to the HFNN. Then, the cover features are compared with the outputs of HFNN. If the outputs are matched with the features of the cover image, a new stego image is formed by assembling the modified free bits with the secret bits. If not, the weights of HFNN are adjusted through a backpropagation learning algorithm.

There are five layers in HFNN, they are denoted as the input layer, fuzzification layer, rule layer, inference layer, and defuzzification layer as in [55]. The HFNN has been trained using five layers back-propagation, the input neurons obtain inputs from free bits buffer, statistical and visual features. After that, the inputs are broadcasted to all hidden neurons in the second layer (fuzzification layer). In this layer, fuzzy processing is performed on input features using the membership function. Here, the bell-shaped Gaussian membership function is used for the good approximation of input space. This bell-shaped function gives different forms of membership functions for the input features by varying the parameter values. In the rule layer, the firing strength of the fuzzy rules is computed using the logical 'AND' operator. The inference layer performs OR operations on fuzzy inference. The defuzzification layer will give the output of HFNN. In HFNN, the nodes of all layers are connected through the weight parameter.

D. EXTRACTION PHASE

The hidden image extraction process includes the same steps as embedding but in reversible order. Here, the original cover image is not required to extract the secret image. Initially, the optimal threshold value is calculated by the SSOA algorithm for the reduction of smooth and edge blocks in the stego image. Subsequently, the enhanced stego image is divided into k-pixel blocks as same as the embedding process.

IV. SIMULATION RESULTS AND DISCUSSION

In this section, the performance of the proposed steganography scheme is evaluated in terms of stego image quality, payload capacity, and security. Also, the performance analysis of the proposed scheme is validated by comparing it with other existing works like the Vernam Algorithm [37] and the hybrid method of LSB Substitution, PVD, and EMD [50]. The proposed steganography scheme is simulated in a Matlab R2019 environment with intel 8 GB RAM under the Windows 10 operating system. The 8-bit grey-level images such as Lena, Bell pepper, and Baboon are taken as the sample cover images each with a pixel size of 225 × 225. Also, 8-bit grey-level images such as Cameraman (64 × 64), Airplane images (128 × 128), and Barbara (192 × 192) are taken as sample hidden images with three different file sizes 5kB, 10kB, and 15kB respectively.

These cover and hidden images are taken from the USC-SIPI image database [56] and they are illustrated in Figure 4. For the evaluations of this paper, we have implemented this technique on approximately 100 images, out of these, three different hidden images are embedded separately into three cover images. The corresponding stego images obtained by the proposed steganography scheme are shown in Figure 5(c). Here, the detailed steps for the proposed steganography scheme have been analyzed by taking an example of embedding of secret Barbara image into the Lena cover image. Initially, the secret Barbara image is encrypted using BBPD based image encryption algorithm.
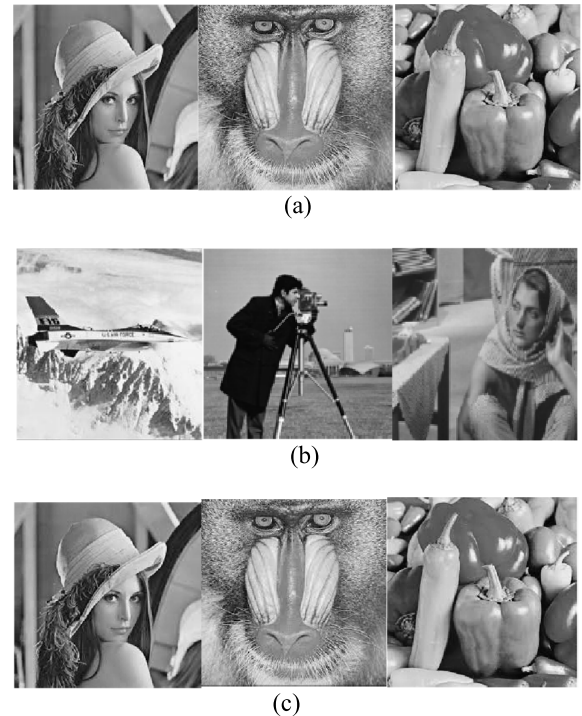

FIGURE 4. Sample image sets (a) cover images (b) hidden images (c) stego images.

The encryption process of the secret Barbara image is shown in Figure 5. Here, the BBPD method is initially used to decompose the hidden image into eight binary planes as shown in Figure 5(b). Then, the binary bit planes are encrypted by performing a diffusion and confusion process using the keystream generated through PWLCM. The Encrypted image for Barbara's hidden image is shown in Figure 5(c).

In the proposed embedding stage, the edge pixels of the cover image are identified by the SSOA algorithm. Then, the encrypted hidden image is embedded into the cover image by setting different parameter values for edge and smooth blocks. Figure 6 illustrates the embedding process output of the proposed steganography method.

During the extraction stage, the embedding process is performed in reverse order to extract the encrypted hidden image from the received stego image. It does not require the cover image. Then, the extracted hidden image is decrypted as shown in Figure 7. From this figure, one can understand that the proposed method can efficiently extract the hidden image without affecting the quality of the image.

A. IMAGE QUALITY ANALYSIS

The image quality metrics are used to determine the quality of the stego image. The image quality analysis of the proposed work based on different performance metrics is explained in this section.

Here, the learning algorithm used is the backpropagation method. This learning method reduces the sum of square error
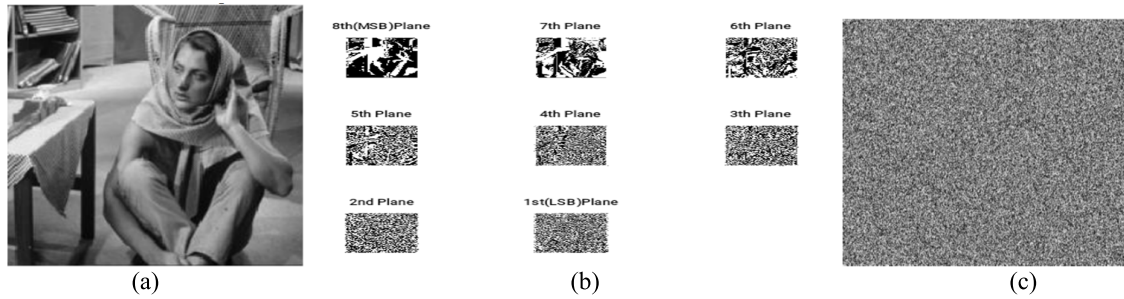
FIGURE 5. Image encryption (a) hidden image (b) binary bit planes (d) encrypted image.
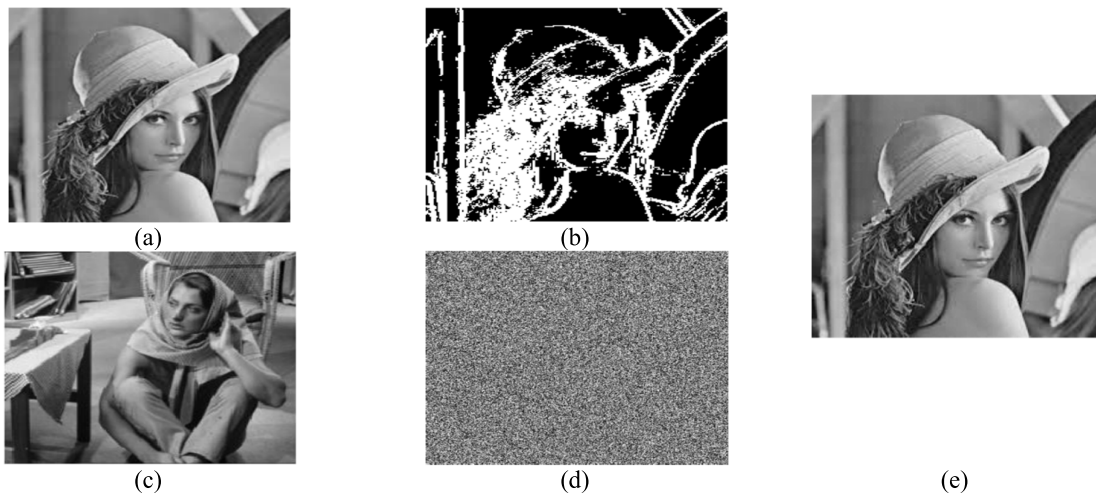

FIGURE 6. Embedding process (a) cover image (b) edge pixels of cover image (c) hidden image (d) encrpted hidden image (e) output stego image.
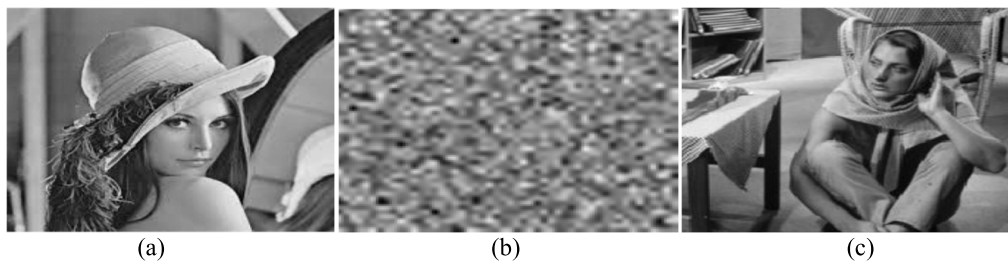

FIGURE 7. Extraction phase output (a) received stego image (b) extracted hidden image (b) decrypted hidden image.

between the desired output and actual output value over each iteration.

$$E = \frac{1}{2} \sum (D_i - O_i)^2 \qquad (27)$$

where, D_i and O_i represent desired and actual output ith node in the output layer respectively. Here, the weight values of all the layers in HFNN are adjusted by the training pattern of the backpropagation algorithm up to matching is achieved.

The distortion and similarity extent of an image can be quantified by Mean Square Error (MSE) to measure the reliability as given below:

$$MSE = \frac{1}{m} \sum_{i=C,S}^{m} (C - S)^2 \qquad (28)$$

where m represents a total number of pixels in the cover image. C and S represent the cover and stego image respectively. The Peak Signal to Noise Ratio (PSNR) determines the statistical difference between the dynamic range of cover images and secret image invisibility. The PSNR can be expressed as follows:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \qquad (29)$$

TABLE 1. Stego image quality analysis in terms of PSNR and MSE.

Cover image	Hidden Image	Vernam Algorithm[37]		LSB+PVD+EMD[50]		Proposed	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
Lena	Cameraman	48.1323	0.9996	51.6375	0.4459	60.822	0.0537
	Airplane	47.0360	1.2866	50.2906	0.6081	57.727	0.1097
	Barbara	45.5886	1.7956	49.4191	0.7433	55.991	0.1636
Bell Pepper	Cameraman	48.5557	0.9067	51.8657	0.4231	60.760	0.0545
	Airplane	47.4486	1.1700	50.5187	0.5770	57.603	0.1129
	Barbara	45.9962	1.6347	49.6472	0.7052	55.907	0.1668
Baboon	Cameraman	44.0428	2.5632	54.0849	0.2538	60.773	0.0544
	Airplane	42.9645	3.2856	52.7379	0.3461	57.676	0.1110
	Barbara	41.4936	4.6101	51.8664	0.4230	55.937	0.1656

TABLE 2. Stego image quality analysis in terms of SSIM and MSE.

Cover image	Hidden Image	Vernam Algorithm[37]		LSB+PVD+EMD[50]		Proposed	
		IF	SSIM	IF	SSIM	IF	SSIM
Lena	Cameraman	0.759717	0.957373	0.957879	0.983574	0.999684	0.998022
	Airplane	0.758717	0.956223	0.956810	0.982574	0.999355	0.997489
	Barbara	0.757717	0.955183	0.955969	0.981574	0.999037	0.996948
Bell Pepper	Cameraman	0.768072	0.961408	0.961594	0.986040	0.999675	0.998079
	Airplane	0.767072	0.960260	0.960472	0.985032	0.999328	0.997535
	Barbara	0.766072	0.958989	0.959543	0.984402	0.999007	0.997169
Baboon	Cameraman	0.862774	0.946602	0.899530	0.987878	0.999679	0.999279
	Airplane	0.861775	0.945574	0.898802	0.986879	0.999347	0.999019
	Barbara	0.860774	0.944578	0.897695	0.985878	0.999024	0.998861

The visual quality of the stego image can be measured by structural similarity (SSIM) measure [57]. This SSIM measure includes three distortion parameters namely, loss of correlation, luminance distortion, and contrast distortion. The SSIM is defined as:

$$SSIM(C, S) = \ell(C, S) \cdot \zeta(C, S) \cdot \delta(C, S) \qquad (30)$$

$$\ell(C, S) = \frac{2\mu_C\mu_S + b_1}{\mu_C^2 + \mu_S^2 + b_1}; \quad \zeta(C, S) = \frac{2\sigma_C\sigma_S + b_2}{\sigma_C^2 + \sigma_S^2 + b_2};$$

$$\delta(C, S) = \frac{\sigma_{CS} + b_3}{\sigma_C\sigma_S + b_3} \qquad (31)$$

where, $\ell(C, S)$ represents the luminance function for measuring the proximity between mean luminance (μ_C, μ_S) of cover and stego images. $\zeta(C, S)$ represents the contrast function for measuring the proximity between the contrast of the two images. Here, the standard deviation σ_C and σ_S is used to measure the contrast. $\delta(C, S)$ represents the structural function for measuring the correlation coefficient between cover and stego images. σ_{CS} represents the covariance between the images C and S. b_1, b_2 and b_3 are positive constants.

The robustness of the proposed scheme can also be validated by Image fidelity [58] as given below:

$$IF = 1 - \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}(C(i, j) - S(i, j))^2}{\sum_{i=0}^{M}\sum_{j=0}^{N}C(i, j) \times S(i, j)} \qquad (32)$$

Table 1 and Table 2 compares the stego image quality of the proposed method in terms of MSE, PSNR, SSIM, and IF with the existing methods namely Vernam Algorithm [37] and hybrid method of LSB Substitution, PVD, and EMD [50]. The proposed method gives a lesser MSE value because it alters less number of bits in each smooth pixel. Also, the perceptual stego image quality of the proposed method is proved by achieving higher image fidelity values.

B. PAYLOAD CAPACITY ANALYSIS

The volume of hidden data that can be embedded into the cover image without destroying the performance of the cover image is known as payload capacity. The payload capacity is generally represented by bits per pixel (bpp) unit.

$$\text{Payload Capacity} = \frac{\text{number of secret bits embedded}}{\text{Total no. of pixel in cover image}} \qquad (33)$$

If the payload capacity is increased then, the PSNR value will drop significantly. Figure 8 compares the performance of the proposed steganography method for three different cover images by varying the payload capacity.

This figure shows that every steganography method will provide good quality stego image when the payload capacity is very low. However, the existing methods decrease the quality of the stego image while increasing the payload capacity. Instead, the quality of the stego image obtained by the proposed method is very high for all test cover images. In the meantime, the proposed scheme does not deteriorate
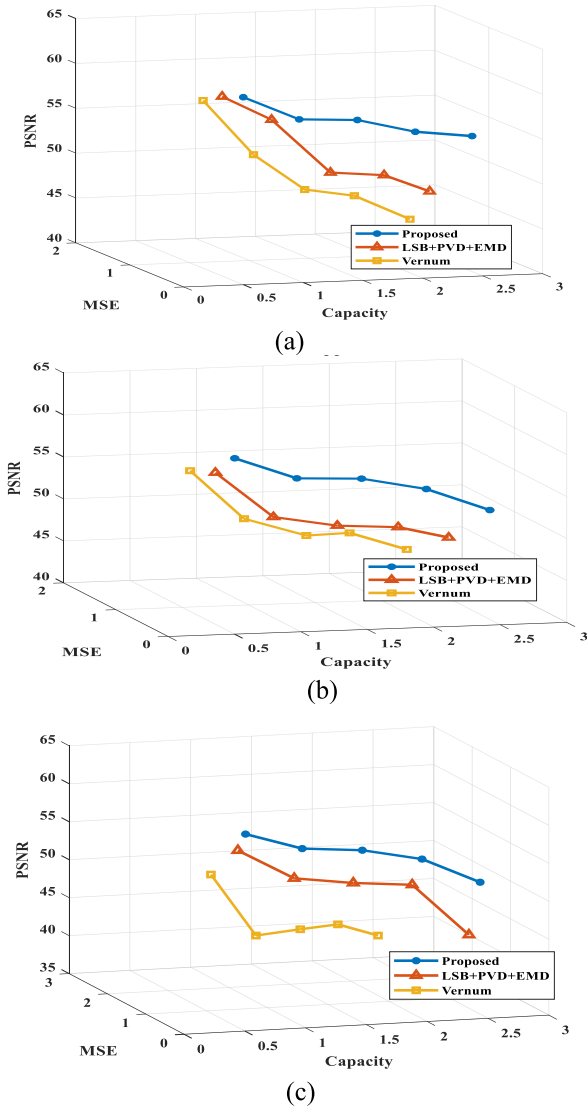
FIGURE 8. Payload capacity analysis for different cover images (a) lena (b) bell pepper (c) baboon.

FIGURE 9. Security measures for different cover images (a) lena (b) bell pepper (c) Baboon.

the quality of the stego image while increasing payload capacity. If the payload capacity is increased to 2.5bpp then, the PSNR of the proposed method is higher than 52dB for all test cases. But, the PSNR of the existing methods is less than 47dB. Because the proposed scheme embeds the secret bits into both smooth region and edge region by setting different parameter values in the steganography embedding function. The edges are less affected by the changes after hiding secret data.

C. SECURITY ANALYSIS

In this section, the security of the proposed steganography scheme is measured using KL divergence [59]. This is the basic method for measuring the security of the steganography scheme because it exactly measures the difference between two distributions. Let H_1 and H_2 be the cover image histogram and stego image histogram respectively. The following expressions are used to estimate the K-L divergence from H_1 to H_2 and from H_2 to H_1.
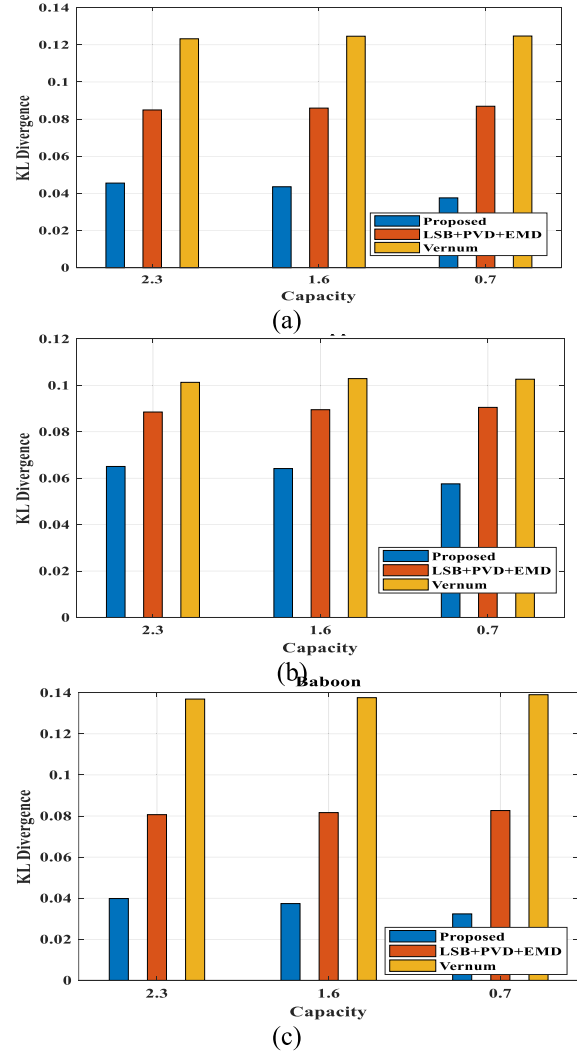
Here, KLD_1 and KLD_2 values are averaged to get the actual value of K-L divergence. When the stego image is as same as the cover image, the K-L divergence value will be equivalent to zero. In Figure 9, the security measure (KL divergence) value of the proposed steganography scheme is compared with the existing methods by varying the payload capacity.

$$KLD_1 = \sum_{i=0}^{255} H_1(i) \times \log \frac{H_1(i)}{H_2(i)} \qquad (34)$$

$$KLD_2 = \sum_{i=0}^{255} H_2(i) \times \log \frac{H_2(i)}{H_1(i)} \qquad (35)$$

Figure 9 shows that the security level of the proposed method is higher than the existing methods while increasing the payload capacity from 0.7 to 2.3bpp.

This adaptive embedding process has been embedded in the secret image by selecting optimal parameters for smooth and edge blocks. Thus, the overall security level of the proposed steganography scheme has been improved.

V. CONCLUSION

In this paper, a highly secured IoT protocol is utilized to transfer stego images to their destination and a secure and improved image quality steganography framework is proposed for the secure transmission of hidden images. This technique focused on image quality, payload capacity, and security of the image steganography method. The proposed SSOA optimized adaptive embedding method has selected suitable parameter values for edge and smooth blocks by determining the optimal threshold value for maintaining the high visual quality when the embedding density is high. The proposed edge/smooth block localization method provides much better results rather than using generic edge detection systems. In this paper, IoT is used to propose improved steganography as a method to improve medical data security, confidentiality, and integrity. When embedding additional data within medical images, medical image steganography requires extreme caution because the additional data must not degrade the image quality. In our proposed paper, the Internet of Things scenario, combining encryption and steganography ensures secure and high-quality data transfer over the internet for medical image steganography. The experimental result also shows that the performance is much better in different perspectives like stego-image quality, payload capacity, and security. Thus, the stego images can't be detected by the unauthorized attacker and therefore the hidden secret image remains safe.

REFERENCES

[1] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data security using cryptography and steganography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 6, pp. 390–397, 2016.

[2] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El-Rabaie, and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," in *Proc. 4th IEEE Int. Colloq. Inf. Sci. Technol. (CiSt)*. Tangier, Morocco: IEEE, Oct. 2016, doi: 10.1109/CIST.2016.7805079.

[3] A. Febryan, T. W. Purboyo, and R. E. Saputra, "Steganography methods on text, audio, image and video: A survey," *Int. J. Appl. Eng. Res.*, vol. 12, no. 21, pp. 10485–10490, 2017.

[4] S. A. Hasso, "Steganography in video files," *Int. J. Comput. Sci. Issues*, vol. 13, no. 1, pp. 32–35, 2016.

[5] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Inf. Secur. J. Global Perspective*, vol. 30, no. 2, pp. 1–25, 2020.

[6] P. Singh, "A comparative study of audio steganography techniques," *Int. Res. J. Eng. Technol.*, vol. 3, no. 4, pp. 580–585, 2016.

[7] M. M. Hashim and M. S. M. Rahim, "Image steganography based on odd/even pixels distribution scheme and two parameters random function," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 22, pp. 5977–5986, 2017.

[8] Y. Inan, "Assesment of the image distortion in using various bit lengths of steganographic LSB," in *Proc. ITM Web Conf.*, vol. 1026, 2018, pp. 1–10.

[9] N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2018, pp. 81–84.

[10] M. H. Abood, "Steganography with RC4 and pixel shuffling encryption algorithms," in *Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT)*. Baghdad, Iraq: IEEE, Jul. 2017, pp. 7–9, doi: 10.1109/NTICT.2017.7976154.

[11] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by steganography and cryptography techniques," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Aug. 2016, pp. 531–534.

[12] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 73–80, Jan. 2020.

[13] C. Biswas, U. D. Gupta, and M. M. Haque, "An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography," in *Proc. 2nd Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–5.

[14] S. Bhat and V. Kapoor, "Secure and efficient data privacy, authentication and integrity schemes using hybrid cryptography," in *Proc. Int. Conf. Adv. Comput. Netw. Inform.*, vol. 870. Singapore: Springer, 2019, pp. 279–285.

[15] S. Harnal and R. K. Chauhan, "Hybrid cryptography based E2EE for integrity & identiality in multimedia cloud computing," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 918–924, 2019.

[16] S. Chauhan, Jyotsna, J. Kumar, and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," in *Proc. 3rd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2017, pp. 1–7.

[17] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Process.*, vol. 153, pp. 109–122, Dec. 2018.

[18] Q. Giboulot and J. Fridrich, "Payload scaling for adaptive steganography: An empirical study," *IEEE Signal Process. Lett.*, vol. 26, no. 9, pp. 1339–1343, Sep. 2019.

[19] Q. Li, X. Liao, G. Chen, and L. Ding, "A novel game-theoretic model for content-adaptive image steganography," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2017, pp. 232–237.

[20] S. I. Nipanikar, V. H. Deepthi, and N. Kulkarni, "A sparse representation based image steganography using particle swarm optimization and wavelet transform," *Alexandria Eng. J.*, vol. 57, no. 4, pp. 2343–2356, Dec. 2018.

[21] R. Lima, W. Gramacho, and A. Henrique, "Optimizing image steganography using particle swarm optimization algorithm," *Int. J. Comput. Appl.*, vol. 164, no. 7, pp. 1–5, Apr. 2017.

[22] Y. NarasimhaRao, P. S. Chandra, V. Revathi, and N. S. Kumar, "Providing enhanced security in IoT based smart weather system," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 18, no. 1, pp. 9–15, 2019.

[23] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.

[24] Y. Sun, Y. Lu, X. Yan, L. Liu, and L. Li, "Robust secret image sharing scheme against noise in shadow images," *IEEE Access*, vol. 9, pp. 23284–23300, 2021.

[25] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS)*, Mar. 2011, pp. 50–55.

[26] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Secur. J.*, vol. 25, nos. 4–6, pp. 197–212, Dec. 2016.

[27] A. S. Anwar, K. K. A. Ghany, and H. El Mahdy, "Improving the security of images transmission," *Int. J.*, vol. 3, no. 4, pp. 7–13, 2015.

[28] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," *Meas. J. Int. Meas. Ed.*, vol. 119, pp. 117–128, Apr. 2018.

[29] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, "Digital image security: Fusion of encryption, steganography and watermarking," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 1–5, 2017.

[30] M. Jain, R. C. Choudhary, and A. Kumar, "Secure medical image steganography with RSA cryptography using decision tree," in *Proc. 2nd Int. Conf. Contemp. Comput. Informat. (ICI)*, Dec. 2016, pp. 291–295.

[31] L. Yehia, A. Khedr, and A. Darwish, "Hybrid security techniques for Internet of Things healthcare applications," *Adv. Internet Things*, vol. 5, no. 3, pp. 21–25, 2015.

[32] M. Y. Aalsalem, W. Z. Khan, W. Gharibi, M. K. Khan, and Q. Arshad, "Wireless sensor networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges," *J. Netw. Comput. Appl.*, vol. 113, pp. 87–97, Jul. 2018.

[33] Z. M. Zaw and S. W. Phyo, "Security enhancement system based on the integration of cryptography and steganography," *Int. J. Comput.*, vol. 19, no. 1, pp. 26–39, 2015.

[34] A. Arya and S. Soni, "Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method," *Int. J. Comput. Sci. Trends Technol.*, vol. 6, no. 2, pp. 160–165, 2018.

[35] P. K. Dhar, A. Kaium, and T. Shimamura, "Image steganography based on modified LSB substitution method and data mapping," *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 3, pp. 155–160, 2018.

[36] V. Odelu, A. K. Das, M. K. Khan, K.-K.-R. Choo, and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," *IEEE Access*, vol. 5, pp. 3273–3283, 2017.

[37] Z. F. Yaseen and A. A. Kareem, "Image steganography based on hybrid edge detector to hide encrypted image using vernam algorithm," in *Proc. 2nd Sci. Conf. Comput. Sci. (SCCS)*, Mar. 2019, pp. 75–80.

[38] M. Hemalatha, U. E. Kumar, K. Vijayaprabakaran, and M. Pravin, "A PSO based prediction and reversible histogram shifting a PSO based prediction and reversible histogram shifting," *Int. J. Comput. Sci. Mobile Appl.*, vol. 2, no. 3, pp. 124–127, Mar. 2014.

[39] S. U. Maheswari and D. J. Hemanth, "Performance enhanced image steganography systems using transforms and optimization techniques," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 415–436, Jan. 2017.

[40] A. H. Mohsin, A. N. Jasim, A. H. Shareef, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, S. Nidhal, and N. S. Jalood, "New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity," *IEEE Access*, vol. 7, pp. 168994–169010, 2019.

[41] S. Fazli and M. Kiamini, "A high_performance steganographic method using JPEG and PSO algorithm," in *Proc. IEEE Int. Multitopic Conf.*, Dec. 2008, pp. 100–105.

[42] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[43] M. K. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world," *IETE Tech. Rev.*, vol. 26, no. 3, pp. 191–195, 2009.

[44] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[45] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010.

[46] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[47] A. Waqar, A. Raza, H. Abbas, and M. K. Khan, "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 235–248, Jan. 2013.

[48] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[49] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A steganography algorithm based on CycleGAN for covert communication in the Internet of Things," *IEEE Access*, vol. 7, pp. 90574–90584, 2019.

[50] A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," *Math. Problems Eng.*, vol. 2018, pp. 1–11, Sep. 2018.

[51] Y. Zhou, W. Cao, and C. L. Philip Chen, "Image encryption using binary bitplane," *Signal Process.*, vol. 100, pp. 197–207, Jul. 2014.

[52] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems," *Adv. Eng. Softw.*, vol. 114, pp. 163–191, Dec. 2017.

[53] S. Veerashetty and N. B. Patil, "Manhattan distance-based histogram of oriented gradients for content-based medical image retrieval," *Int. J. Comput. Appl.*, vol. 114, pp. 163–191, Dec. 2017.

[54] H. Faris, S. Mirjalili, I. Aljarah, M. Mafarja, and A. A. Heidari, "Salp swarm algorithm: Theory, literature review, and application in extreme learning machines," in *Nature-Inspired Optimizers*. Cham, Switzerland: Springer, 2020.

[55] R. J. Kuo, Y. S. Tseng, and Z.-Y. Chen, "Integration of fuzzy neural network and artificial immune system-based back-propagation neural network for sales forecasting using qualitative and quantitative data," *J. Intell. Manuf.*, vol. 27, no. 6, p. 1207, Dec. 2016, Art. no. 4, doi: 10.1007/s10845-014-0944-1.

[56] A. Weber, "The USC-SIPI image database: Version 5, original release, signal and image processing institute," Dept. Elect. Eng., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep., 1997.

[57] A. Horé and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 2366–2369.

[58] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 935–946, 2020.

[59] R. Kapoor, R. Gupta, L. H. Son, S. Jha, and R. Kumar, "Boosting performance of power quality event identification with KL divergence measure and standard deviation," *Meas. J. Int. Meas. Confederation*, vol. 126, pp. 134–142, Oct. 2018.

[60] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, and G. Garg, "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model," *IEEE Access*, vol. 8, pp. 159402–159414, 2020, doi: 10.1109/ACCESS.2020.3020513.

[61] Y. Shelke and C. Chakraborty, "Augmented reality and virtual reality transforming spinal imaging landscape: A feasibility study," *IEEE Comput. Graph. Appl.*, vol. 41, no. 3, pp. 124–138, May 2021, doi: 10.1109/MCG.2020.3000359.

[62] C. Chakraborty, "Chronic wound image analysis by particle swarm optimization technique for tele-wound network," *Wireless Pers. Commun.*, vol. 96, no. 3, pp. 3655–3671, Oct. 2017, doi: 10.1007/s11277-017-4281-5.

[63] H. Bhuyan, D. C. Chakraborty, S. Pani, and V. Ravi, "Feature and sub-feature selection for classification using correlation coefficient and fuzzy model," *IEEE Trans. Eng. Manag.*, early access, Apr. 19, 2021, doi: 10.1109/TEM.2021.3065699.

SACHIN DHAWAN received the B.Tech. degree from Kurukshetra University, Kurukshetra, in 2008, and the M.Tech. degree in electronics and communication engineering from the University Institute of Engineering and Technology, Kurukshetra University, in 2011. He is currently pursuing the Ph.D. degree in electronics and communication engineering from AIACTR, Guru Gobind Singh Indraprastha University, Dwarka, India. He was an Assistant Professor at the Geeta Institute of Management and Technology, Kurukshetra, from July 2011 to July 2012. He has been working with the Panipat Institute of Engineering and Technology, Samalkha, as an Assistant Professor, since July 2012. He has authored over 20 research articles in various international journals and conferences. He has also published his articles in the IEEE conferences and Scopus/SCI Journals. His current research interests include signal and image processing, the Internet of Things, artificial intelligence, and machine learning. He is an Associate Member of All India Institutions of Engineers. He serves as a reviewer for several journals and international conferences.

CHINMAY CHAKRABORTY worked at the Faculty of Science and Technology, ICFAI University, Agartala, India, as a Sr. Lecturer. He worked as a Research Consultant with the Coal India Project at Industrial Engineering and Management, IIT Kharagpur. He worked as a Project Coordinator of the Telecommunication Convergence Switch Project under the Indo-U.S. joint initiative. He also worked as a Network Engineer in system administration with MISPL, India. He is currently an Assistant Professor (Sr.) with the Electronics and Communication Engineering Department, Birla Institute of Technology, Mesra, India. He has published more than 100 articles at reputed international journals, conferences, book chapters, and books. His research interests include the Internet of Medical Things, wireless body sensor networks, wireless networks, telemedicine, m-health/e-health, and medical imaging. He is an editorial board member of different journals and conferences. He is a member of the Internet Society, the Machine Intelligence Research Laboratory, and the Institute for Engineering Research and Publication. He received the Best Session Runner-up Award, the Young Research Excellence Award, the Global Peer Review Award, the Young Faculty Award, and the Outstanding Researcher Award. He was a Speaker of AICTE, DST sponsored FDP, and CEP Short Term Course. He is co-editing several books on smart IoMT, healthcare technology, and sensor data analytics with Elsevier, CRC Press, IET, Pan Stanford, and Springer. He has conducted a session of SoCTA-19, ICICC-2019, Springer CIS 2020, SoCTA-20, and SoCPaR 2020, and he is also a Reviewer of international journals, including IEEE Access, IEEE Sensors Journal, IEEE Internet of Things Journal, Elsevier, Springer, Taylor & Francis, IGI, IET, Telecommunication Computing Electronics and Control (TELKOMNIKA), and Wiley. He has served as the Publicity Chair Member of renowned international conferences, including the IEEE Healthcom and IEEE SP-DLT. He is serving as a Guest Editor for *Future Internet* journal (MDPI), *Internet Technology Letters* (Wiley), *Annals of Telecommunications* (Springer), *International Journal of System Assurance Engineering and Management* (Springer), *Environment, Development and Sustainability* (Springer), and *Business and Society Review* (Wiley); a Lead Guest Editors for IEEE Journal of Biomedical and Health Informatics, *Journal of Health Engineering* (Hindawi), *Big Data* journal (Mary Ann Liebert), *International Journal of E-Health and Medical Communications* (IGI), *Multimedia Tools and Applications* (Springer), *CMC* (TechScience), *Interdisciplinary Sciences: Computational Life Sciences* (Springer), *International Journal of Nanotechnology* (Inderscience), *Current Medical Imaging* (BenthamScience), and *Journal of Medical Imaging and Health Informatics*; a Lead Series Editor for *Advances in Smart Healthcare Technologies* (CRC); and an Associate Editor for *International Journal of End-User Computing and Development*, *Journal of Science and Engineering*, and *Internatonal Journal of Strategic Engineering*.

JAROSLAV FRNDA (Senior Member, IEEE) was born in Martin, Slovakia, in 1989. He received the M.Sc. and Ph.D. degrees from the Department of Telecommunications, VSB–Technical University of Ostrava, in 2013 and 2018, respectively. He is currently an Assistant Professor at the University of Žilina, Slovakia. He has authored and coauthored 12 SCI-E and nine ESCI articles in WoS. His research interests include quality of multimedia services in IP networks, data analysis, and machine learning algorithms.

RASHMI GUPTA received the M.E. and Ph.D. degrees in electronics and communication engineering from the Delhi College of Engineering, Delhi University. She is also holding the position of Founder Director of the Incubation Center AIACTR-IRF funded by the Delhi Government. Prior to this, she has rich experience in industry and various academic institutes. She is currently working as a Professor with the Electronics and Communication Engineering Department, Ambedkar Institute of Advanced Communication Technologies and Research under the Government of NCT of Delhi. She has authored over 90 research articles in various renowned international journals and conferences. She has published patents and DST funded project. She is associated with many international research organizations as an editorial board member and a reviewer. Her research interests include machine learning, computer vision, and signal and image processing.

ARUN KUMAR RANA received the B.Tech. degree from Kurukshetra University and the M.Tech. degree from Maharishi Markandeshwar (Deemed to be University), Mullana, India, where he is currently pursuing the Ph.D. degree. He is currently working as an Assistant Professor at the Panipat Institute of Engineering and Technology, Samalkha, with more than 14 years of experience. He has published around 65 articles in national and international journals and conferences. He has also published four books and two patents. He has also published many other patents. He has attended nine workshops and nine FDP. He has guided six M.Tech. candidates. He serves as a reviewer for several journals and international conferences. His research interests include image processing, wireless sensor networks, the Internet of Things, AI, and machine learning and embedded systems. He is a member of the Asia Society of Research, the International Association of Engineers (IAENG), and the Editorial Board of the *International Innovative Research Journal of Engineering and Technology (IIRJET)*. He was a member of the Sci Scopus indexed international conference/symposium, relentlessly. He received many national and international awards. He is an editor of many edited books and an Associate Editor of one reputed journal.

SUBHENDU KUMAR PANI received the Ph.D. degree from Utkal University, Bhubaneswar, India, in 2013. He is currently working as the Principal of Krupajal Computer Academy (KCA), Bhubaneswar. He has published 51 international journal articles (25 Scopus index). His professional activities include roles as a Book Series Editor with CRC Press, Apple Academic Press, and Wiley-Scrivener, an associate editor, an editorial board member, and/or a reviewer of various international journals. He is an associate with a number of conference societies. He has authored/coauthored more than 150 international publications, five books, 15 edited and upcoming books; and 20 book chapters. He has more than 17 years of teaching and research experience. In addition to research, he has guided 31 M.Tech. students and two Ph.D. students. His research interests include datamining, bigdata analysis, web data analytics, fuzzy decision making, and computational intelligence. He is a Fellow of SSARSC and a Life Member of IE, ISTE, ISCA, OBA.OMS, SMIACSIT, SMUACEE, and CSI. He was a recipient of five researcher awards.

• • •