International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 694~705
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp694-705

Security and imperceptibility improving of image steganography using pixel allocation and random function techniques

Noor Alhuda F. Abbas[1], Nida Abdulredha[1], Raed Khalid Ibrahim[2], Adnan Hussein Ali[3]
[1]Department of Technique Computer Engineering, Al-Esraa University College, Baghdad, Iraq
[2]Department of Medical Instruments Engineering Techniques, Al-Farahidi University, Baghdad, Iraq
[3]Department of Information Communication and Technology, Institute of Technology Baghdad, Middle Technical University, Baghdad, Iraq

Article Info

Article history:

Received Sep 6, 2020
Revised Jul 15, 2021
Accepted Jul 28, 2021

Keywords:

Digital image-steganographic
Huffman coding
Odd/even pixels' allocation
PSNR
Random map function

ABSTRACT

Information security is one of the main aspects of processes and methodologies in the technical age of information and communication. The security of information should be a key priority in the secret exchange of information between two parties. In order to ensure the security of information, there are some strategies that are used, and they include steganography and cryptography. An effective digital image-steganographic method based on odd/even pixel allocation and random function to increase the security and imperceptibility has been improved. This lately developed outline has been verified for increasing the security and imperceptibility to determine the existent problems. Huffman coding has been used to modify secret data prior embedding stage; this modified equivalent secret data that prevent the secret data from attackers to increase the secret data capacities. The main objective of our scheme is to boost the peak-signal-to-noise-ratio (PSNR) of the stego cover and stop against any attack. The size of the secret data also increases. The results confirm good PSNR values in addition of these findings confirmed the proposed method eligibility.

Corresponding Author:

Adnan Hussein Ali
Department of Information Communication and Technology, Institute of Technology Baghdad Middle Technical University
Baghdad, Iraq
Email: dr.adnan@mtu.edu.iq

1. INTRODUCTION

The mention of steganography for the science that converts a message into a form that certifies a complete inability to discover any information hidden in the carrier. A system of steganography warrants each secret information can be kept undetectable [1]. The word of steganographic originates from a Greek term that means as a protected writing. It is regarded as a unique area of data concealment, also considered as an art of science for transmission that is not visible. The aim of making the communication invisible in order to secret data hiding inside the cover image (CI), thereby enhancing its imperceptibility. The existence of the secret information (SI) is often recognized by just the sender's and receiver's [2].

The steganography elements, basically included an information, cover object, a stego key for improved security and embedding mechanism. The carrier object in which the SI is hidden in could be a video, an audio, text or image. Steganography is being utilized in various applications effectively, but it often can be very dangerous so it could be used by attackers for sending trojans and viruses in order to manipulate sensitive

systems. More so, with the use of this information-hiding technology, criminals or terrorists may be enabled to exchange secrete information [3]. The payload is described as the size of secret data which can be hidden within the cover object successfully without creating visible artifacts in stego images. In order to measure payload, bits per pixel (bpp) is used. If each pixel is used in hiding 1 bit of data, then the payload of a steganography algorithm will be 1 bpp or 12.5%.

The word robustness refers to the steganography algorithm's durability against different forms of statistical and basic attacks in steganography. If it is not possible to easily alter or retrieve the data that is concealed in a cover image using image processing operations, the steganography algorithm used is considered robust. Scaling, cropping, image rotation, and noise are some of the image processing activities that can be used in the alteration or retrieval of concealed messages. The issue of robustness is crucial in when watermarking techniques are used because of copyright protection [4]. The notion of imperceptibility is synonymous with undectability, which can be calculated using various image quality measurement metrics, such as peak-signal-to-noise-ratio (PSNR) [5], [6].

The correlation between hiding payload capacity (PC) and quality of stego media (SM) is purely described via a balance which authors attempt to achieve. Most often, the quality of stego medium is reduced by concealment of huge amounts of data within a cover medium. Consequently, hiding capacities have continued to remain comparatively low because of this negative effect on the quality of stego [7]. With respect to mechanism for embedding, the techniques of steganography are partitioned to two important classes, which are spatial-domain (SD) and transform-domain (TD). Regardless of the advantages provided by current methods, problems such as: i) the use of inadequate embedding algorithms may generate visually distorted stego images (SI), which in turn increases the likelihood of human visual system detection, and ii) imbalance between image quality, computational complexity, capacity for payload and security; thus, making them inappropriate. This study, the use of our mechanism alongside with chaotic method is employed in developing an efficient scheme in spatial domain, with the aim of addressing the aforementioned problems. This paper makes the following key contributions: i) introduce an effective digital image steganography with achieving a good quality of image, payload and security; ii) identify the random pixel used to embed hidden information, while the random function is used to boost the system's resilience against trackers' attempts to discover which pixel to embed; iii) the embedding of the secret information is done in a random region within an image through the use of the spatial-domain (SD) of the cover-image (CI) using the odd/even pixel allocation. This way, the quality of the stego-images is boosted while an extraction of the secret data is made difficult

2. PRELIMINARIES

2.1. Least-significant-bit LSB substitution

The representation of least-significant-bit (LSB) considers easy and conventional process applied for inserting secret data enclosed by covered image [8]. Though this process continues, it is thinkable to overwrite the depiction of binary secret data. Concerning to the grayscale images that pixels have values just single ranging (0 to 255) with an 8 bits depth, these secret information bits do not convert into binary bits due to their directly using to substitute the cover image of the objects. With referring to color images which hold 3 routes red, green, and blue (RGB) besides 24 bits depth, then a cover object (image) can be originally partitioning into 3 channels just a secret data is embedded early in each channel. Then, these three paths will be merged in order to create the SI. The LSB bits modification may not be allowed the human visual system (HVS) for detecting the stego-image. Owing to the fact of LSB substitution method as discrete kind is employed in the suggested system, the mathematical expression for this method can be prepared with acceptable details. A mathematical expression aims for providing deeper perception on the focal thought of the scheme in the next section. The assorted LSB embedding percentage (EP) contains 6.25%, 12.5%, 18.75% in addition to 25%, that intends 0.5, 1.0, 1.5, and 2 bpp respectively may be utilized depend on the embedded. By using a simple instance, an inclusive description of the fundamental concept of the LSB steganography basis can be providing. If a 12.5% EP example is considered, that is mean 1 bpp in each LSB, and can be extended to another EP. With such implementation, a stego image imperceptibility is decreased, thus making it simple for the HVS for noticing the stego-image. At this time, image quality will be compromising for data capacity. When data with larger amount is covered, an image quality degradation is arising. By using LSB methods, the capacity with high data can be achieved. Figure 1 shows various stego images of Lena in different embedding percentages [9]-[11].

Through the random addition of 1 to the gray levels on the CI, the pixels of the image are slightly modified using the LSB-matching. This is done if there is no correspondence between the secret bit and the LSB of a given pixel, with the values of the pixels maintained within the range of 0-255. There is no difference between the process of extraction in LSB and LSB-M, this means to use a shared secret key to obtain a traversing route, as well as to extract the LSB of each pixel for obtaining real embedded bits. A pair of pixels

$(P_i,\ P_i + 1)$ is used by least significant bit matching revisited (LSB-MR) [12] as an embedding unit that is manipulated to $(P'_i, P'_i + 1)$ in a way to make criteria is satisfied.

$$\left\{ LSB\ (P'_i) = S_i \qquad LSB\left(\left|\frac{P'_i}{2}\right| + P'_{i+1}\right) = S_{i+1} \right\} \tag{1}$$

Where P_i and $P_i + 1$ denotes the embedding unit while the two secret bits are represented by S_i and S_{i+1}. With this correlation, the LSB and LSB-M such as irregular artifacts art does not formed in stego images. More so, with the use of LSB-MR, the rate at which the pixels are modified in can be minimized in variance method with LSB and LSB-M. The procedure of extraction involves the generation of a traversing path utilizing a secret key (SK) as well as a quasi-random-number-generator, and afterwards the extraction of two bits from each of the units of embedding is performed.

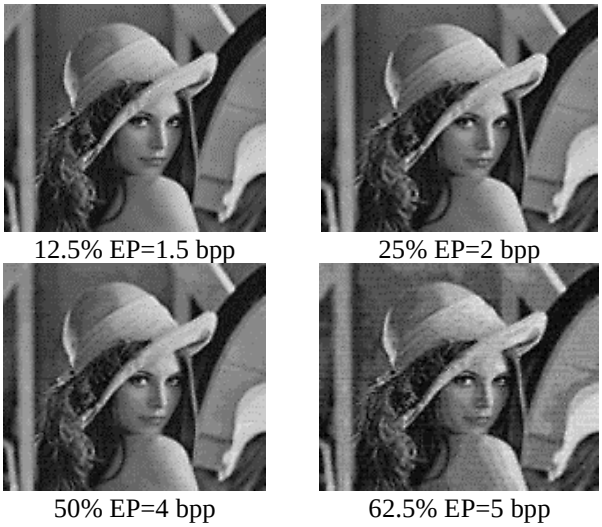


Figure 1. The imperceptibility of Lena stego-image (SI) using different EP [12]

In a study carried out by Bhardwaj and Sharmab [13], attempts were made to improve the security and distribute the message within the entire host image. To achieve this, these researchers investigated the simulation of images through the use of text, and they used LSB to hide information. According to them, the aim of their study is to provide three level security in which the secret message is complemented, the complemented secret message is hidden within a cover image pixel that are selected randomly through the use of a pseudo random number of generator and inverted bit LSB method. Based on the results of their study, their proposed approach outperforms the conventional LSB as well as the inverse LSB with lower mean square error (MSE) and higher PSNR.

Hashim *et al.* [14] in their study, proposed a secure image steganography created by Huffman coding, distribution of odd/even, and Henon map. The implementation of the proposed framework has been found to be less complex in contrast to other current methods. Using the Henon map algorithm, the imperceptibility of the stego-image is increased by using pixel distribution in order to get a better protection method. Prior to the process of embedding, the secret message is embedded using Huffman coding. Two main reasons that this method has always been seen efficient: the first is that during the embedding process it is able to check the correspondence between secret bits with LSB in order to determine 1 and 0, and the second is the segmentation of the secret message in order to track and map every bit within the stego image. The performance of their suggested protocol is better than comparing to [15], [16] in terms of PSNR, based on the findings.

Singh and Datar [17] presented an image steganography created with wavelet transformation and RC4 algorithms. A proposed method with cover image is apportioned into 64 blocks of (8×8) with useful wavelet transform. The secret message here encrypted earlier by embedding with RC4 algorithm is used for enhancing the security levels. The Stego image now is difficult for detect by HVS attack. Patel and Cheeran [18] had employed and investigated the steganography technique and advanced encryption standard (AES) algorithm in order to produce an assessment and comparison into various images format and allows most appropriate information with this procedure. LSB substitution algorithms were used for implementing this Steganography

method. An investigation and evaluation were completed with different parameters like delay, PSNR, MSE, in addition to absolute mean square error (AMSE).

A new reversible method of data hiding utilizing pixel-value-difference (PVD) with differential expansion (DE) were presented by Jana *et al.* (2016). The secret message initially separated into sub-stream with n bits size in projected method. PVD can be applied for embedding n-1 bits in addition to embed 1 bit by applying difference-expansion (DE). Lastly, based on the sharing secret key bit stream, a pair of two-stego pixels will be distributed among dual image. An extracting technique considers a same embed technique to that of reverse sensing [19].

The securing color image steganography based on LSB was recommended by Al-Tamimi *et al.* [20]. They used asymmetric key in the image steganography for LSB scheme which contains 32 integers array. Inserting of data hiding is random in related to hiding message and pixel selection generator, the applying of transposition is done for each 24-bits block. A security has been improved with LSB substitution technique. According to the literature review, the majority of current steganography technologies are incapable of generating high-quality stego-images, leaving the subject vulnerable to identification by human vision systems. Consequently, the hidden secret can be easily accessed by the attackers, and therefore, cannot be used as an authentic information in top-secret security systems.

2.2. Random map function

One of the major reasons' steganography is developed is to afford an environment which is secured, where data can be transmitted over the network by secret messages in stego-images type. The increasing concern about the security of data is one of the main motivations of this research. Many studies were executed in the steganography field with a purpose of developed novel approaches through which by steganography a message can be secured [21]. With respect to enhance data particularity, various studies deal with random technique due to their higher efficiency and simple using. Advantages of randomizing algorithms can be summarized as: i) quick and comfort, or may be both in assorted problems, ii) easy employment, and iii) fast and likely.

Many authors were found in the literature have leveraged random map function compensations, with each bosses its limitations and strengths. Depending on behavior, various kinds of random maps are existing, such as, nubasi [22], Arnold scrambles [23], in addition to knight tour [24]. Concerning normal random maps, the selection numbers can be completed by one parameter at original conditions [25]. Two random maps can be utilized for the pixels allocations with the aiming of preserving the proposed method. Also, an overlap between these two ways that guarantee for data which is introduced can be entirely concealed and discovered the pixels' path is so hard or almost impossible [23], [24], so that, our method security is guaranteed.

2.3. Huffman coding

The main objective of the Huffman coding algorithm is to reduce the size of text before embedding to the image. As shown in Figure 2 the Huffman algorithm depends on reducing the frequent letters and gives them priority code or short path in the Huffman tree. The capacity is an important concept in steganography method to make the method more robust, such as better method that can hold high amounts of data inside hosting image while maintaining the quality of the image represented by PSNR. For the concept of data management and transfer protocol compression of data transferred from sender to receiver is very useful beside other techniques used in this research. Figure 3 shows a simple flowchart of Huffman coding applied in this research. High frequency in this case will get less path of visiting to reduce going deep every time and let less frequency in the deep of the tree, then will gain many clocks in digital word as 0,1.

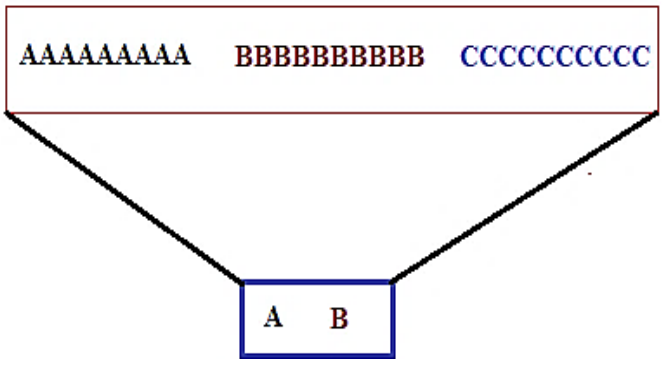


Figure 2. Reduce text frequency in Huffman coding

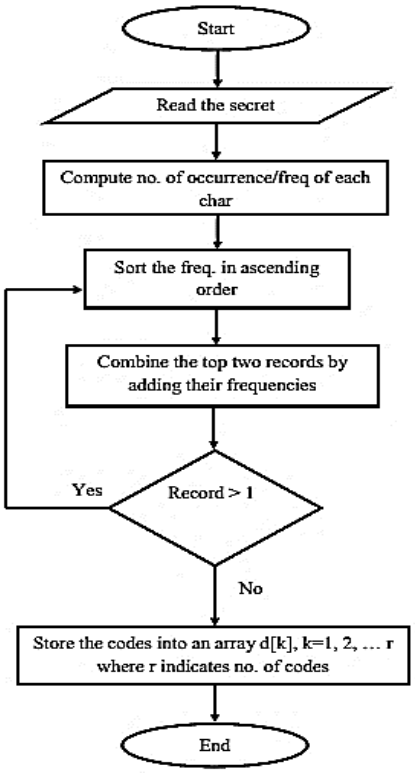


Figure 3. Flowchart of Huffman coding

3. THE PROPOSED METHOD

This section provides a graphic description of the proposed method which is proposed in this study alongside its key modules. The invention of the methodology is further clarified by this graphic representation of the framework, as then readers can get a better image and a greater understanding of our process. The suggested method-based steganography varies from other steganography approaches in that it can have high protection while retaining image quality at a low cost and with a fair payload. The presented work is ideal for secured transmission application of various secret bits, like electronic-patient-records (EPR) transmission to the health care centers, and private communication that requests privacy. Figure 4 shows a graphic explanation for the planned outline.

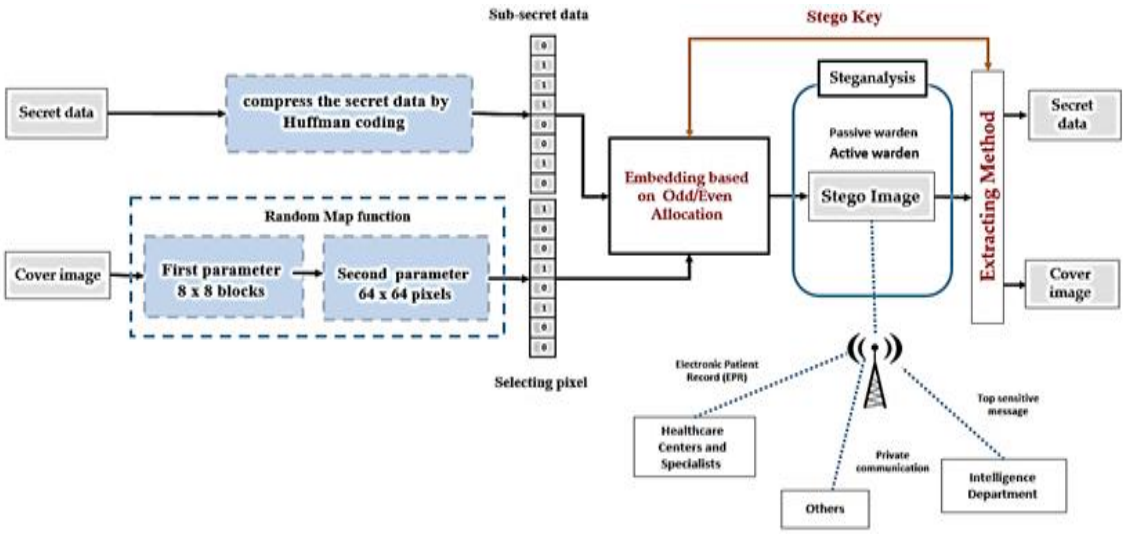


Figure 4. Overall flow of the proposed scheme

This method is made up of four major sub-section which consist: i) image preparation, involving two parts, first part responsible for partitioning of an image and the second part, responsible for pixel selection, ii) preparation of secret data, involving the compression (Huffman coding) of secret data prior to the embedding stage, iii) stage three includes the adaptive hiding of hidden data inside cover images using a data embedding algorithm, which allows the stego-image to be generated, iv) finally, the secret-data is retrieved from the stego-image that has been distributed at the receiving terminal using the extraction algorithm. The data could also be used as appropriate. All of four major stages are summarizing description as follows.

3.1. Image preparation

Image preparation consists of two parts, first part responsible for partitioning of an image and the second part, responsible for pixel selection. These two parts at image preparation stage are executed simultaneously before introducing or can hiding text into an image. The cover image consists of 512×512 pixels come from standard dataset and the pixels arranged as a matrix of two dimensions (2D), grouping these pixels into the blocks for easy management. Selecting one block or group of pixels for embedding, then selecting pixels inside the block that normally occur in this stage. Steganography system normally used one parameter random function or other algorithm like knight tour for a random process. Two control parameters used in random process to achieve the objective of security. Two phases of image division will perform; first, partitioning the cover image to 64 sub-small images called a block. Select the pixels inside this block this selection is the most important process to keep the stego image same original as possible.

3.2. Huffman coding

The objective of the Huffman coding algorithm is to decrease the size of text before embedding to the image. The Huffman algorithm depends on reducing the frequent letters and gives them priority code or short path in the Huffman tree. High frequency in this case will get less path of visiting to reduce going deep every time and let less frequency in deep of the tree, then will gain many clocks in digital word as 0,1. Simply can summarize the procedures of compression text in Huffman coding used with proposed system as Algorithm 1.

Algorithm 1. Huffman coding

```
Input: array f [1…n] of numerical frequencies or probabilities
Output: binary coding tree with n leaves that has minimum expected code length for f.
Huffman (f[1….n])
T=empty binary tree
Q=priority queue of pairs (i, f[i], i=1….n, with f as comparison key
For each k=1…n-1
i=extract Min(Q)
j=extract Min(Q)
f [n+k]=f[i]+f[j]
insert Node (T, n+k) with children I, j
insert Rear (Q, (n+k), f [n+k]))
Return T
```

3.3. Embedding algorithm (EA)

The EA is the responsibility for hiding the secrete message within a CI. By supporting of the secret-key, the embedding algorithm can be able for concealing the encrypted message adaptively inside the LSB layer. In Algorithm 1, the key steps involved in the presented embedding operation are illustrated. Here, marking every pixel into block map is the most crucial procedure. This procedure is referred to as embedding block. The mechanism shown in Figures 5 provides a better view of the core concept of the suggested embedding algorithm.

Algorithm 2. Embedding algorithm

```
Input: Cover image (I^C), Stego Key (K^S), Secret data (SD).
initialize I^C=cover image, SD=secret data , K^S=stego key
Apply Huffman using Algorithm 1 coding on on DS to get the compression bit stream M^CBS)
Segment the M^CBS into groups, each with 16 or 32 bits
Select an appropriate cover image I^C from dataset of cover images (DS^CI)
Generate random number 1 and arrange it according to HMF-a vector
Select one block of (8x8) blocks via HMF-a vector
Generate random number 2 and arrange it according to HMF-b vector
Select the destination pixel via HMF-b vector
Generate EM vector and arrange it related to Odd/Even
Mark each pixel with LSB and M^CBS group
If Bit matched>Bit mismatched so that Embedded directly to pixel from secret by step 15
Otherwise, an Inverting secret message will be embedded with step 15
Iteration (Loop) I=1:N
Fetch M^CBS bits (0 , 1)
```

a. If M^{CBS}=0 and Pixel is even, Do no change in 1-LSB layers.
b. If M^{CBS}=0 and pixel is odd, Do Changes in 2-LSB layer via replace 0 to LSB layer
   Else if the 2-LSB layer is full, Do Changes in 1-LSB layers.
c. If M^{CBS}=1 and pixel is odd, Do no change in 1-LSB layers.
d. If M^{CBS}=1 and pixel is even, Do changes in 2-LSB layer via replace 1 to LSB layer
   Else if the 2-LSB layer is full, Do Changes in 1-LSB layer
   I=I+1
Iterate procedure 16 till all the secret-bits are hidden, and a stego-image (SI) is acquired
Output: Stego-Image (I^S)

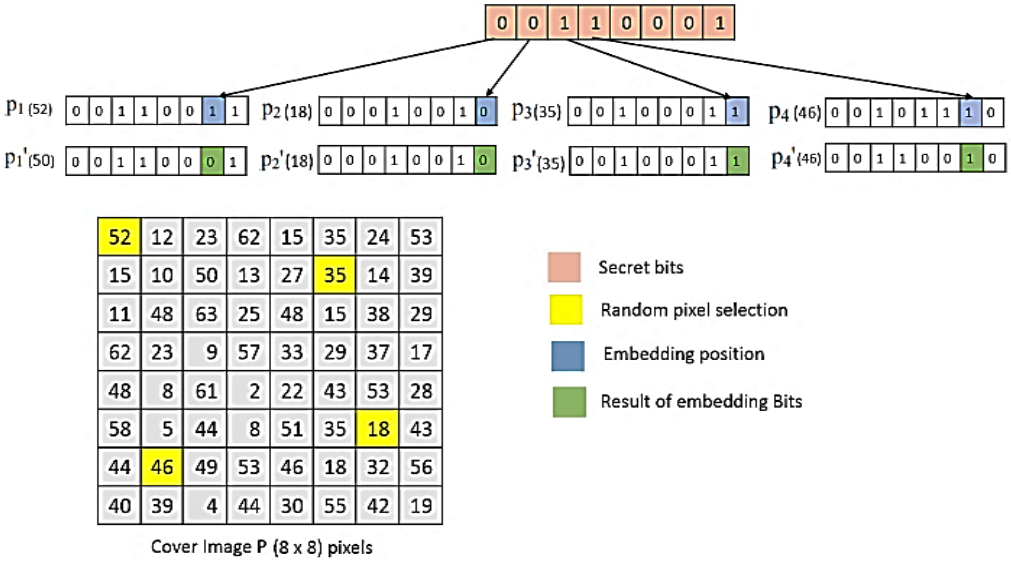


Figure 5. Examples of embedding for the proposed scheme

The second objective which this study seeks to achieve through the proposed scheme, is to hide the secret data within an LSB-layer. This implies that in the LSB, if pixels end with 1, they are odd value pixels, and otherwise, they are even valued pixel. In this case, embedding will involve substituting secret bits based on pixel (the second layer, a secret bit is replaced by odd pixel, while in the first-layer, the even pixel is used to replace the secret bit).

3.4. Retrieving algorithm

The retrieving of the concealed secret information about the stego-image is carried out utilize the retrieving algorithm. For the secret data to be retrieved successfully, different parameters are utilized. Some of these parameters include Huffman coding, Henon map function (HMF), and stego-keys of data embedded scheme. The security feature of a proposing framework is complemented by these parameters, thereby making it difficult for attackers extract secret data. The key steps involved in the proposed mechanism of extraction are presented in Algorithm 3.

Algorithm 3. Retrieving algorithm
Input: stego image (I^S), stego key (K^S)
Begin I^S=Stego-Image, K^S=Secret-Key
Apply random number 1 using HMF-a vector
Select one block of 64 blocks HMF-a vector
Apply random number 2 using HMF-b vector
Select the stego pixel from HMF-b vector
Apply EM vector and arrange it based on odd/even
Mark the LSB of all pixels
Loop start from I=1:N
Reverse the step 15 of embedding process from algorithm 1
Repeat step 9 until extract all secret bits from stego image
Decompression from the resulting bits of step 10 using algorithm1
Re-construct the inventive data from the realized bits
Output: secret message (M)

4. EXPERIMENTAL RESULTS AND DISCUSSION

For performing the experiments at this paper, a MATLAB tool together with eight standard grayscale images which are shown in Figure 6 was utilized for images with (512x512) size were obtained. The different stego-images of our scheme at EP=2 shown in Figure 6. Many parameters were used in the proposed scheme using such as PSNR, bpp, embedding capacity (EC) been evaluated.

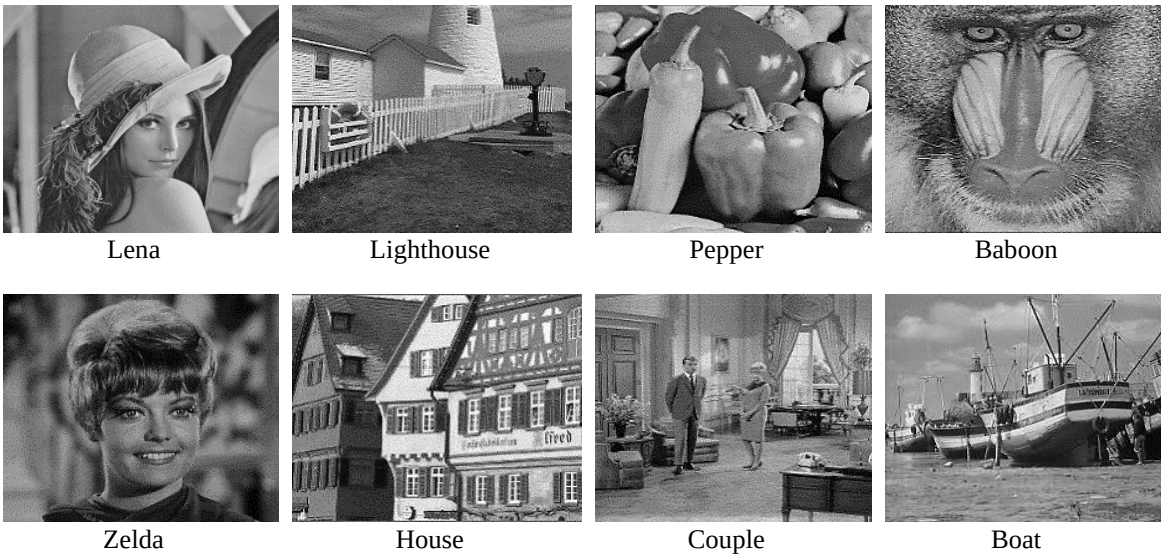


Figure 6. Cover images used in the proposed scheme

4.1. Benchmarking created on EC, PSNR, and bpp

The embedding capacity EC can be considered as the ratio of message bits number to cover pixels number [26], [27], and be directly associated with the pixels number utilized in the suggested scheme here as a various numbers of message bits that can embed by one pixel.

$$EC = \frac{The\ number\ of\ message\ bits}{The\ number\ of\ cover\ images's\ pixels} \quad (2)$$

The diverse payload capacities have been used in this calculation, and offered like percentage with the intention of being in agreement with a most recent study now. Intended for more explanation, some information is given for an image 512x512:

a) At 6.25%, 16384 bytes equal, which means every two pixels=16 bits, thus 1/16=6.25% when 1 bit of two pixels is embedded
b) At 12.5%, 32768 bytes equal, which means every two pixels=8 bits, thus 1/8=12.5% when 1 bit of one pixel is embedded
c) At 18.75%, 49152 bytes equal, which means every two pixels=16 bits, thus 3/16=18.75% when 1.5 bits of one pixel is embedded
d) At 25%, 65536 bytes equal, which means every pixel=8 bits, thus 2/8=25% when 2s bit of one pixel is embedded.

The explanation for using these figures in this analysis is that previous research used different payloads, so a requirement for having uniform tools to get equal results. In Figure 7, the embedding percentages utilized in the proposed scheme are presented. The evaluation of image quality can be specified by PSNR that is evaluated after the embedding process to comparison between original and stego images. A hiding data process can be considered as an unnoticeable to HVS, PSNR calculation result may be equal or may be greater than 30 dB [14]. PSNR are measured with applying these equations:

$$PSNR = 10log_{10}\left(\frac{255}{MSR}\right) \quad (3)$$

where mean square error is MSE, and can be calculated with:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij}) \quad (4)$$

Here, m and n are the images' sizes, while the cover and stego images are represented with x and y respectively. During the implementation of the proposed scheme two important stages were carried out on this study, namely the training and testing stages [27]. In conventional processing of images, the imperceptibility of a SI is measured by PSNR measures [28]. The consistency of the stego-image has been assessed against the existing carrier image using the PSNR measures described above. The results of our scheme, and others methods of Wu and Tsai [29], Wu and Hwang [30], Kumar and Chand [31], Sahu *et al*. [32], Sahu and Swain's [33] and Qui *et al*. [34], are presented in Tables 1-5. More so, Aljuaid and Parah [35] give more results and these schemes and techniques have been compared with term of EC graphically presented in Figure 8.

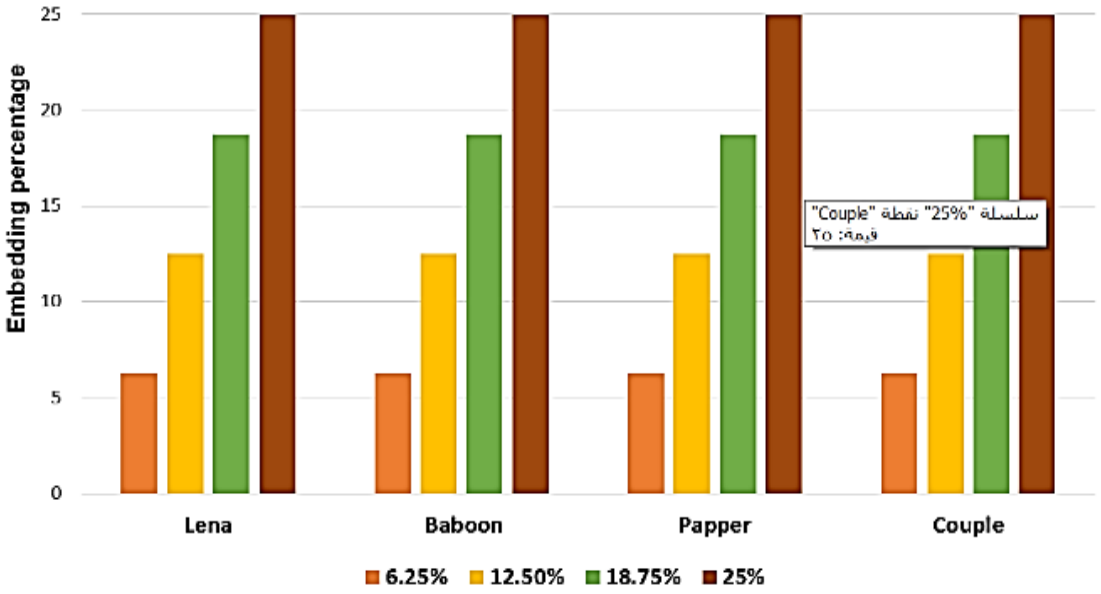


Figure 7. Different embedding percentages (EP)

Table 1. Results of the projected scheme at 6.25% and 12.5% of EP

Image (512x512)	Proposed Scheme (6.25%)			Proposed Scheme (12.5%)		
	PSNR	EC	BPP	PSNR	EC	BPP
Lena	72.01	131.072	0.5	66.44	265.144	10
Lighthouse	72.03	131.072	0.5	66.42	265.144	10
Zelda	72.01	131.072	0.5	66.46	265.144	10
Pepper	72.02	131.072	0.5	66.43	265.144	10
Baboon	72.03	131.072	0.5	66.49	265.144	10
Boat	72.01	131.072	0.5	66.48	265.144	10
House	72.02	131.072	0.5	66.44	265.144	10
Couple	72.02	131.072	0.5	66.43	265.144	10
Average	72.02	131.072	0.5	66.44	265.144	10

Table 2. Results of the scheme at 18.75% and 25%

Image (512x512)	Proposed Scheme (18.75%)			Proposed Scheme (25%)		
	PSNR	EC	BPP	PSNR	EC	BPP
Lena	61.05	393.215	1.5	54.80	542.288	2.0
Lighthouse	61.06	393.215	1.5	54.80	542.288	2.0
Zelda	61.08	393.215	1.5	54.82	542.288	2.0
Pepper	61.18	393.215	1.5	54.10	542.288	2.0
Baboon	61.04	393.215	1.5	54.82	542.288	2.0
Boat	61.05	393.215	1.5	54.80	542.288	2.0
House	61.05	393.215	1.5	54.81	542.288	2.0
Couple	61.09	393.215	1.5	54.82	542.288	2.0
Average	61.07	393.215	1.5	54.85	542.288	2.0

Table 3 Results for [30] and [29] techniques

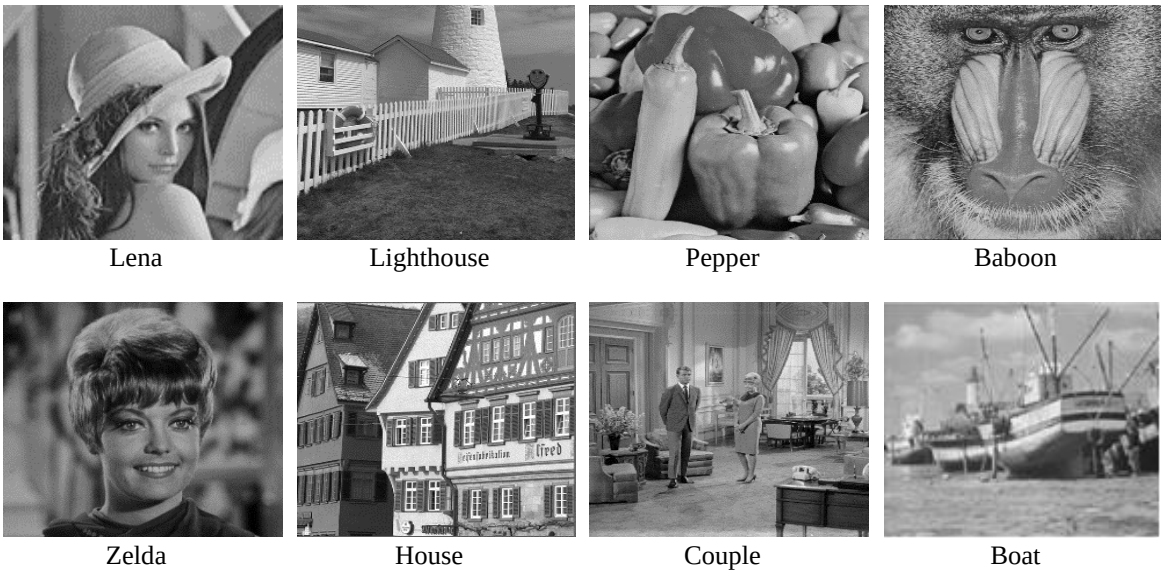
Image (512x512)	Wu [30] (12.5%)			Wu and Tsai [28]		
	PSNR	EC	BPP	PSNR	EC	BPP
Lena	51.05	256.144	1.0	41.45	400.104	1.53
Lighthouse	51.06	256.144	1.0	40.11	411.903	1.57
Zelda	51.08	256.144	1.0	40.01	399.029	1.52
Pepper	51.18	256.144	1.0	40.11	399.140	1.53
Baboon	51.04	256.144	1.0	40.02	419.209	1.60
Boat	51.05	256.144	1.0	39.03	411.674	1.57
House	51.05	256.144	1.0	39.23	401.249	1.53
Couple	51.09	256.144	1.0	39.49	400.670	1.53
Average	51.07	256.144	1.0	39.78	405.238	1.54

Table 4. Results for [31] and [32] techniques

Image (512x512)	Kumar and Chand's (12.5%) [30]			Sahu (18.75%) [32]		
	PSNR	EC	BPP	PSNR	EC	BPP
Lena	51.27	256.144	1.0	47.83	393.126	1.5
Pepper	51.28	256.144	1.0	47.93	393.126	1.5
Baboon	51.27	256.144	1.0	47.73	393.126	1.5
Boat	51.27	256.144	1.0	47.23	393.126	1.5
House	51.28	256.144	1.0	47.73	393.126	1.5
Average	51.27	256.144	1.0	47.43	393.126	1.5

Table 5. Results for [32] and [33] techniques

Image (512x512)	Sahu (18.75%) [32]			Sahu and Swain's (25%) [32]		
	PSNR	EC	BPP	PSNR	EC	BPP
Lena	47.32	542.288	2.0	44.08	542.288	2.0
Pepper	47.33	542.288	2.0	44.07	542.288	2.0
Baboon	47.32	542.288	2.0	44.08	542.288	2.0
Boat	47.18	542.288	2.0	44.07	542.288	2.0
House	47.30	542.288	2.0	44.08	542.288	2.0
Average	47.28	542.288	2.0	44.08	542.288	2.0



Lena Lighthouse Pepper Baboon

Zelda House Couple Boat

Figure 8. Different stego-images with EP=5%

The suggested methodology has PSNR for embedding percentage as: EP=6.25% is 72.80 dB, for EP=12.5% it is 66.60 dB, for EP=18.75 it is 61.20 dB, and for EP=25% it is 54.95 dB. The EC of the proposed scheme is 131, 072, 265, 144, 393, 216, and 524, 288 bits for EP=6.25%, 12.5%, 18.75 and 25% respectively. In the studies carried out by Wu and Hwang [30], and Kumar and Chand [31], PSNR of their techniques were 51.08 dB and 51.27 dB, respectively. As seen from the table of comparison, the proposed technique outperforms that of Wu and Kumar and Chand in terms of PSNR when EP=12.5% with equal EC. The scores

of the PSNR of the proposed scheme when EP=6.25% and 12.5% is presented in Table 3. Based on the results, the marked images of the proposed scheme are of better quality, thereby confirming its effectiveness. Likewise, the PSNR and EC of our scheme for EP=18.75% and 25% is better than that of Sahu *et al*. [32], Sahu and Swain's [33] respectively.

5. CONCLUSION

This study offers an improving image steganography technique related to odd/even pixel allocation and with modified the security of secret-data prior hiding. This developed scheme may be established for enhancing the security level as well as payload capacity for determination the existing complications. A technique of Huffman coding is utilized for compressing the secret data preceding the embedding. Modified secret data before hiding that will support to enhance the security and as will capacity. Different payload capacity has been used with current study and reflected as a percentage to correspond with the researches in recent studies. The goal of the scheme is to increase imperceptibility by utilizing PSNR measurement so it can stand against the attack. A good PSNR value in the results shown and these findings confirmed the eligibility of the proposed scheme. Pixel allocation with high complexities and bits standing by will certify better security as well as robust imperceptibility associated for the existing scheme.

REFERENCES

[1] M. Al-Mualla and H. Al-Ahmad, "Information hiding: steganography and watermarking," *Multimedia Communication and Signal Processing (MCSI)*, 2009.

[2] D. K. Nayak and C. Bhagvati, "A threshold-LSB based information hiding scheme using digital images," *2013 4th International Conference on Computer and Communication Technology (ICCCT)*, 2013, pp. 269-272, doi: 10.1109/ICCCT.2013.6749639.

[3] W. A. Shukur and K. K. Jabbar, "Information hiding using LSB technique based on developed PSO algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 2, pp. 1156-1168, Apr. 2018, doi: 10.11591/ijece.v8i2.pp1156-1168.

[4] M. M. Kareem, M. Ismail, M. A. Altahrawi, N. Arsad, M. F. Mansor, and A. H. Ali, "Grid based clustering technique in wireless sensor network using hierarchical routing protocol," *2018 IEEE 4th International Symposium on Telecommunication Technologies (ISTT)*, 2018, pp. 1-5, doi: 10.1109/ISTT.2018.8701720.

[5] A. H. Ali, M. R. Mokhtar, and L. E. George, "Enhancing the hiding capacity of audio steganography based on block mapping," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 7, pp. 1441-1448, 2017.

[6] B. Wu, M. P. Chang, B. J. Shastri, P. Y. Ma, and P. R. Prucnal, "Dispersion deployment and compensation for optical steganography based on noise," in *IEEE Photonics Technology Letters*, vol. 28, no. 4, pp. 421-424, Feb. 2016, doi: 10.1109/LPT.2015.2496957.

[7] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221-234, Feb. 2016, doi: 10.1109/TIFS.2015.2486744.

[8] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935-946, 2020, doi: 10.11591/ijece.v10i1.pp935-946.

[9] O. Evsutin, A. Kokurina, R. Meshcheryakov, and O. Shumskaya, "The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28567-28599, 2018, doi: 10.1007/s11042-018-6055-9.

[10] A. H. Ali and A. D. Farhood, "Design and performance analysis of the WDM schemes for radio over fiber system with different fiber propagation losses," *Fibers*, vol. 7, no. 3, pp. 19, 2019, doi: 10.3390/fib7030019.

[11] S. Dhargupta, A. Chakraborty, S. K. Ghosal, S. Saha, and R. Sarkar, "Fuzzy edge detection-based steganography using modified Gaussian distribution," *Multimedia Tools and Applications*, vol 78, 2019, doi: 10.1007/s11042-018-7123-x.

[12] J. M. Lopes, P. Marrone, S. L. Pereira, and E.M. Dias, "Health 4.0: Challenges for an Orderly and Inclusive Innovation," *IEEE Technol. Soc. Mag.*, vol. 38, no. 3, pp. 17–19, 2019, doi: 10.1109/MTS.2019.2930265

[13] R. Bhardwaja and V. Sharmab, "Image steganography based on complemented message and inverted bit LSB substitution," *Procedia Computer Science*, vol. 93, pp. 832–838, 2016, doi: 10.1016/j.procs.2016.07.245.

[14] M. M. Hashim and M. S. M. Rahim, "Image steganography based on odd/even pixels distribution scheme and two parameters random function," *Journal of Theoretical & Applied Information Technology*, vol. 95, no. 22, pp. 5977-5986, 2017.

[15] A. Farhood, M. K. Naji, S. H. Rhaif, and A. H. Ali, "Design and analysis of dual band integrated hexagonal haped microstrip UWB antenna," *Indonesian Journal Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 1, pp. 294-299, 2019, doi: 10.11591/ijeecs.v15.i1.pp294-299.

[16] M. M. S. A. Al-Momin, I. A. Abed, and H. A. Leftah, "A new approach for enhancing LSB steganography using bidirectional coding scheme," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5286-5294, 2019, doi: 10.11591/ijece.v9i6.pp5286-5294.

[17] S. Singh and A. Datar, "Improved hash-based approach for secure color image steganography using canny edge detection method," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 14, no. 7, pp. 82-89, 2014.

[18] F. R. Patel and A. N. Cheeran, "Performance evaluation of steganography and AES encryption based on different formats of the image," *International Journal of Advanced Research in Computer and Communications Engineering*, vol. 4, no. 5, 2015, doi: 10.17148/ijarcce.2015.45140.

[19] H. M. Noman, A. A. Abdulrazzaq, M. M. Kareem, and A. H. Ali, "Improvement Investigation of the TCP algorithms with avoiding network congestion based on OPNET," *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, 2019, Art. no. 052025, doi:10.1088/1757-899X/518/5/052025.

[20] P. Thakur, S. Kushwaha, and Y. Rai, "Enhance steganography techniques: A solution for image security," *International Journal of Computer Applications*, vol. 115, no. 3, 2015, doi: 10.5120/20133-2220.

[21] A. A. Hussein and A. H. Ali, "Comprehensive investigation of coherent optical OFDM-RoF employing 16QAM external modulation for long-haul optical communication system," *International Journal Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 2607-2616, 2020, doi: 10.11591/ijece.v10i3.pp2607-2616.
[22] M. Kamath and R. S. Kunte, "Framework for reversible data hiding using cost-effective encoding system for video steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 5487-5496, 2020, doi: 10.11591/ijece.v10i5.pp5487-5496.
[23] S. Roy and A. K. Pal, "A robust reversible image watermarking scheme in DCT domain using Arnold scrambling and histogram modification," *International Journal of Information and Computer Security*, vol. 10, no. 2-3, pp. 216-236, doi: 10.1504/IJICS.2018.091469.
[24] A. Banharnsakun, "Artificial bee colony algorithm for solving the Knight's tour problem," In *International Conference on Intelligent Computing and Optimization*, vol. 866, pp. 129-138, 2018, doi: 10.1007/978-3-030-00979-3_13.
[25] D. Bhattacharyya, T. Kim, and P. Dutta, "A method of data hiding in audio signal," *Journal of the Chinese Institute of Engineers*, vol. 35, no. 5, pp. 523-528, 2010, doi: 10.1080/02533839.2012.679054.
[26] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, B. Balusamy, "Securing data in the internet of things (IoT) using cryptography and steganography techniques," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.
[27] M. J. Mnati, R. F. Chisab, A. M. Al-Rawi, A. H. Ali, and A. V. D. Bossche, "An open-source non-contact thermometer using low-cost electronic components," *HardwareX*, vol. 9, 2021, doi: 10.1016/j.ohx.2021.e00183.
[28] S. A. Lafta, A. H. Ali, M. M. Kareem, Y. A. Hussein, A. H. Ali, "Performance simulation of broadband multimedia wireless networks simulation based on OPNET," *Indonesian Journal Electrical Engineering and Computer Science (IJEECS)*, vol. 17, no. 1, pp. 1-9, 2020, doi: 10.11591/ijeecs.v17.i1.pp1-9.
[29] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613-1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.
[30] N. Wu and M. Hwang, "A novel LSB data hiding scheme with the lowest distortion," *The Imaging Science Journal*, vol. 65, no. 6, pp. 371-378, 2017, doi: 10.1080/13682199.2017.1355089.
[31] R. Kumar and S. Chand, "A reversible data hiding scheme using bit flipping strategy," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 19, no. 2, pp. 331-345, 2016, doi: 10.1080/09720529.2015.1085743.
[32] A. K. Sahu, G. Swain and E. S. Babu, "Digital image steganography using bit flipping," *Cybernetics and Information Technologies*, vol. 18, no. 1, pp. 69-80, 2018, doi: 10.2478/cait-2018-0006.
[33] A. K. Sahu and G. Swain, "A novel n-Rightmost bit replacement image steganography technique," *3D Research* 10, no. 1, 2019, Art. no. 2, doi: 10.1007/s13319-018-0211-x.
[34] H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," in *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2499-2505, Sept. 2020, doi: 10.1109/JBHI.2020.2973467.
[35] H. Aljuaid and S. A. Parah, "Secure patient data transfer using information embedding and hyperchaos," *Sensors*, vol. 21, no. 1, 2021, Art. no. 282, doi: 10.3390/s21010282.