

A pixel contrast based medical image steganography to ensure and secure patient data

Mohammed Mahdi Hashim^{a,*}, Ali A. Mahmood^b, Mohammed Q. Mohammed^{b,c}

^aFaculty of Engineering, Uruk University, Baghdad, Iraq

^bUniversity of information technology and communications, Baghdad, Iraq

^cAl-Esraa University College, Baghdad, Iraq

(Communicated by Madjid Eshaghi Gordji)

Abstract

The information and communications technology time are essential for the security aspect of processes and methodologies. The security of information should be a key priority in the secret exchange of information between two parties. That's to guarantee the information's security, some strategies are used, and they include steganography, watermark, and cryptography. In cryptography, the secret message is converted into unintelligible text, but the existence of the secret message is noticed, on the other hand, watermarking and steganography involve hiding the secret message in a way that its presence cannot be noticed. Presently, the design and development of an effective image steganography system are facing several challenges such as low capacity, poor robustness and imperceptibility. To surmount these challenges, a new secure image steganography work called the Pixels Contrast (PC) method is proposed along with the eight neighbour's method and Huffman coding algorithm to overcome the imperceptibility and capacity issues. In the proposed method, a new image partitioning with a Henon map is used to increase the security part. This method has three main stages (preprocessing, embedding, and extracting) each stage has a different process. In this method, different standard images were used such as medical images and SIPI-dataset. The experimental result was evaluated with different measurement parameters like Histogram Analysis Structural Similarity Index (SSIM), Peak signal-to-noise ratio (PSNR). Compared the proposed method with the previous works then proved to be better than existing methods. In short, the proposed steganography method outperformed the commercially available data hiding schemes, thereby resolving the existing issues.

Keywords: Eight neighbors, Compression method, Image steganography, Security, imperceptibility.

*Corresponding author

Email addresses: comp.mmh@gmail.com (Mohammed Mahdi Hashim), ali_kareem@uoitc.edu.iq (Ali A. Mahmood), dr.mohammed@esraa.edu.iq (Mohammed Q. Mohammed)

Received: August 2021 *Accepted:* November 2021

1. Introduction

Recent advancements in computer technology come with great convenience for information propagation. Information propagation has become so effortless whereby contents may now be easily sent, received, and distributed through the internet. Securing these digital contents become a challenge when they are transmitted over non-secured networks [5, 33]. Therefore, an information hiding mechanism is needed and very important. The techniques of Information hiding can be divided into two broad types including steganography and watermarking [35], wherein both are used to hide secret messages. In addition, these two techniques have a close relation, but each has its own objectives. The watermarking main goal is to protect the secret data integration, either eavesdropper's communication concealing exist or not. The steganography conceals data in contrast for protect the secret data and communicated [11].

Used the steganography technique by non- secured media to concealing secret data or regular data like images. Decades ago, dedicated research efforts have been directed towards developing robust and secured Image Steganography Systems [17]. Popularity of the Image Steganography has gained traction due to effortless transmission by different low-cost devices of the multimedia content (IP digital cameras and smart mobile phones), many social media applications (LinkedIn, Facebook, Twitter and WhatsApp) [14]. Several issues involving image security and hiding secret message still without solutions, furthermore understanding the secret data embedding [10].

Information hiding approaches can be categorized into several types depending on the cover medium. In other words, it is possible to conceal a secret data in different media, which could take the forms of an image, audio, text, video, DNA or even a protocol. Each of these cover media has its advantages and drawbacks [18]. Nevertheless, the image is mostly utilized as a cover object because of its availability, easy usage by customer and large amount of data holding capacity [27]. In general, nowadays steganography mainly used on applications used computer devices through networking channels [28]. Media that carrying data or text is the image that many applications in different fields used this kind of media (image), the most important application which is the subject of this research is used in medical devices such as MRI and CT scanner [3].

In order to make steganography systems effective, developers must emphasize three factors that play an important role in any steganography scheme. These three issues are also the challenges faced by existing steganography approaches. First issue concerns with payload capacity factor, whereby the hosting media needs to be able to accommodate a large volume of data to carry secret information. While, the second issue concerns with security, whereby the approach used needs to be able to secure secret data reliably. Finally, the third issue concerns with imperceptibility factor (embedding approach), which also reflects the success of any steganography scheme [8].

Most of the problem which facing researchers in this regard are to keep the imperceptibility of the image high as possible, that means image containing secret should be innocent during handling and mobility. Psychotherapy is as important as conventional therapy, so hiding medical reports from (patient and companions) which is the facilities of the image is necessary to maintain the privacy of the treating physician is the goal of this study. In the current time, the overseas treatment becomes familiar because the world has become a small village and sending the patient report in advance before making any decision is inevitable [28]. Then with the proposed study can send just a certain image involved inside the whole information regarding the patient case. Many existing methods suggested in literature each has its pros and cons, the challenging here is to find a novel method that gains advantages and go beyond the disadvantages of existing methods [27].

Different medical images are used in this study. These images are used in most of the researches in addition to providing many datasets available on the internet. Some studies in literature and can

say the majority considered diagnosis and detection of cancer diseases [6]. Other studies considered security and privacy in the medical image with two directions first security in term oh hiding information [32], second monitoring and recording [9] or health care for the same reasons [1] this actually do not be effective unless taken in consideration online process and this kind require the high process to keep the results online.

The proposed article intends providing the method (state of the art) called the Pixels Variance (PV) with the eight neighbors method that conceals information reports of the patient inside the different medical images to be available for the second party. The proposed method has three main stages (preprocessing, embedding, and extracting stages) each stage has different steps. The proposed method was evaluated using the statistical and non-structural criteria. The proposed method was resisted by all the common attacks used in the image steganography systems, as well as achieving the required results that were compared with previous works that proved efficient rather than (the state of art). The steganography whole structure with mathematical issues will explain in the next sections.

2. Related Work

2.1. Information hiding History

Information hiding idea is older than the idea of communication and network [8]. Which is consisting of two general terms: first steganography that considered in this proposal and the second concept is watermarking. Steganography itself was very messy, firstly before using transportation like mail, phones, and horses the message was delivered on foot. Thus, hiding the message must have two choices first memorized by messenger or else hidden by messenger [22].

During World War II invisible ink widely used but the extraction was a different method and not easy. Ultraviolet light used to read the invisible ink latterly by using ant counterfeit devices. Monk Johannes Trithemius used cryptography of modern founder, this considered the as the first attempt to conceal secret data in the text [30]. German during World War used a special technique null cipher which considered as an unencrypted message for hiding secret information. Using this technique appeared very innocent outside. Steganography developed rapidly due to the fast progress in internet and communication development. One of the objectives of such a proposal is to keep the pace of development in this area and hide secret messages within a robust system [13].

2.2. Terminologies in Steganography

To understand the basic insight of the steganography, Simmons (1984) narrated a story [31]. That story talked about Alice and Bob two prisoners are tried to interchange discrete messages minus being noticed by their warden named Wendy. As soon as she noticed any interaction linking her two prisoners, she immediately terminated the communication linking to Alice and Bob. This two-prisoners whereabouts were routinely utilized for illustrating the essence of the cryptography within the surroundings of the uncontrolled countries. Specifically, two nations might seek to relay details minus obstruction by a different nation (for instance the “warden”), to eliminate the all suspicion thereby decided to apply steganographic procedures daily conversations.

Figure 1. Framework presents an information-theoretic for steganography that previously applied based on the abovementioned story [20]. The cited framework has two processes, namely the embedding (E) and extraction (D). The left part of the figure exhibits secret message (M) the issuer the embedder (sender side) to the cover image file (C) and relays altered “result image” (S) to receiver on the other side. The windy aims to intersect the messages between the sender and receiver which is placed in the middle of the figure. She continuously attempts to catch the message or detect the

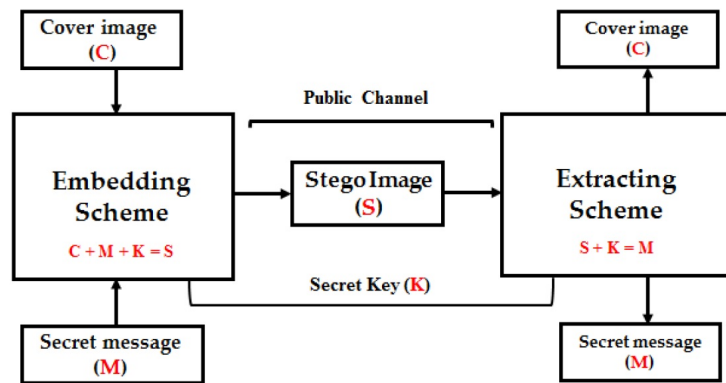


Figure 1: The basic concept of the steganography arrangement in its entirety

information that is exchanged between these parties. This model was structured in a way that only the intended recipient can extricate the message as a result of the distributed secret between the person relaying and recipient. This distributed secret can be an algorithm for obtaining exceptional variables of the algorithm and can be exhibited as a “key.”

Based on this framework, the steganography arrangement can mathematically be explained as a quintuple $\mathfrak{P} = (C, M, K, D_K, E_K)$, where C is the set of cover object used through the public connection, M is the hidden data and K is a key that is used. The steganography plan originates from two functions such as the embedding function $E_K : C \times M \times K \rightarrow S$ and extraction function $D_K(E_K(C, M, K), K) = M$ [11]. The secret message (M) that contained the sensitive details thus necessitates an explicit kind of concealment. The C is the object that hides the data in the interior of their bodies. The operation (E) signifies the procedure of creating a stego file (S) by establishing the details of the information into the cover that is encrypted via a stego key (K). The stego file (S) is an amalgamation in the middle of the cover for the specific secret message is embedded. For the operation (D) signifies the step of getting the embedded details from the stego file. The stego key (K) indicates the factor that inter-relates the procedures of appending the message at the interior of the cover and extracts the same message from the stego file. Holistically, the steganography refers to the pursuit of obscuring sensitive details inside different media (C) to produce a stego file (S) via a key (K). The steganography may be used by the recipient to extract the hidden message (M).

2.3. Image Steganography Domains

Classified the steganography into three types according to different procedures. The main variations among domains are listed in Table 1. [17, 14]. The sections below describe briefly the main functions of these domain-based embedding procedures.

2.4. Related Methods

The maximum payload capacity of a steganography system refers to the highest size of the secret message to be hidden in the media file such as image, video, or audio subjected to a specific condition. Thus, it is desirable to increase the payload capacity of a steganography system for achieving better performance. A significant change in the multimedia file is observed when the maximum data limit is exceeded, causing a failure of the steganography algorithm. The steganography payload is measured utilizing the Data Hiding Ratio (DHR) which is defined as the ratio between the maximum payload capacities to the original media size [25]. In [17] the embedding rate is determined as the payload

Table 1: Comparison among the spatial, transform and adaptive domain-based embedding methods

Characteristics	Properties	Domains		
		Spatial	Frequency	Adaptive
System class	Complexity	Simple	Complex	Depends on adaptive algorithm
Pixel Manipulation	Embedding	Direct	Indirect (transformed coefficient)	Depends on adaptive technique
Embedding Capacity	Payload	High payload	Limited payload	Varied payload
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Robustness	Compression, Noise, Cropping, Rotating, Filtering	Highly prone	Less prone	Depends on adaptive algorithm
Security	Attacks	Vulnerable to attacks	Resistant to attacks	Hard to attacks
Statistical detection Attacks/ analysis	RS, Histogram	Easy to detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful

Table 2: The payload capacity used in various steganography system

Payload capacity	Low capacity	Moderate capacity	High capacity
Bytes	≤ 16384	≤ 49152	> 49152
Bpp	≤ 0.5	≤ 1.5	> 1.5
Percentage (%)	$\leq 6.25\%$	$\leq 18.75\%$	$> 18.75\%$

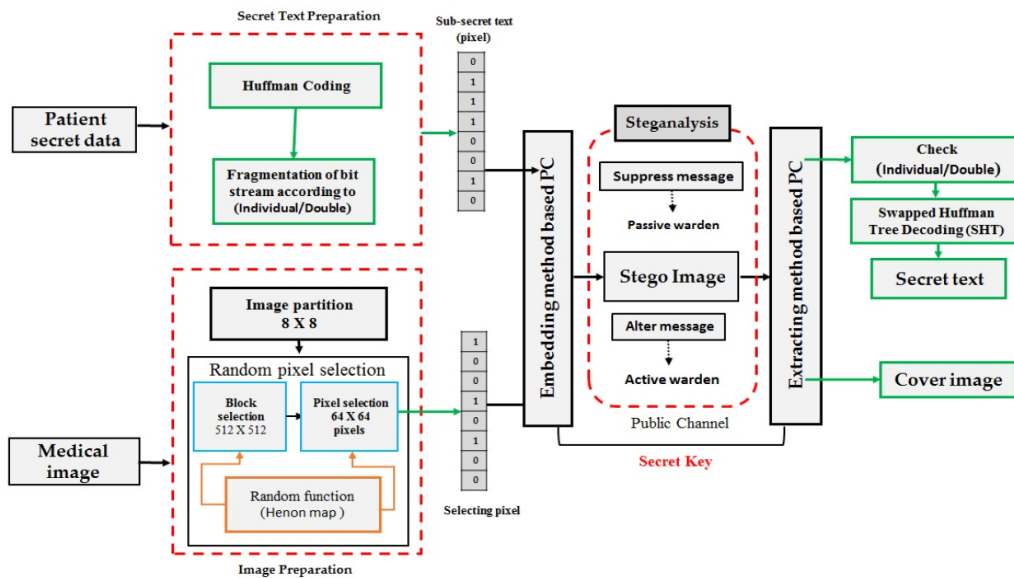


Figure 2: The proposed scheme overall flow

capacity value relative the original image dimension for the data hidden (in bits). Therefore, main challenge is keeping the higher payload capability in a steganography system without sacrificing the security and imperceptibility [15]. The size of the payload capability is characterized in duration of the bits per pixel (Bpp), bytes with percentage (%). Table 1.shows the low, moderate, and high payload capacity used in different steganography systems [17].

Most of the steganography systems employ the compression algorithms to condense the secret data before embedding. The compression algorithms increase the secret data amount inside an image. Huffman coding is the most common approach used in the compression process which can compress the secret data more than 30%. The coding has widely been used to solve the payload capacity problems in the steganography system, wherein the secret data is compressed prior to its insertion into an image [11]. Many recent works related to the image steganography are listed in Table 3.

3. Research methodology

Graphics description has provided in the part for the proposed method which is proposed in this study alongside its key modules. Through this graphic representation of the framework, the innovation of the framework is further explained so that the readers are able to have a clear image and deeper insight of our method. The proposed method based steganography is different from other methods of steganography that are unable to support high security while maintaining a quality of image at a low cost and reasonable payload, in the sense that it is capable of maintaining balance among quality of image, security, payload [13]. Figure 2. below presents a graphic description of the proposed scheme.

Table 3: Recent Works related to the image steganography

References	Method	Performance
(Muhammad et al., 2016) [25]	LSB-MLEA: Applied Multi-level encryption on secret data and stego-key.	$> 45dB$ 1BPP
(Rajendran et al., 2017) [7]	LSB: CM Chaotic map-based ISS has been used in LSB method. The secret bits embedding is based on generated Chaotic sequence while a 1-D logistic map has been used.	44.53 dB 2 BPP
(Nyeem et al., 2018) [26]	Bit plane + Histogram Divided the pixel intensity into 2 values based on the bit-plane values and used the histogram-shifting based embedding through the histogram bins separately.	40 dB 5.0 BPP (High EP)
(Setiadi and Jumanto, 2018) [12]	LSB- Edge Area Combined the Sobel detectors and the Canny to fetch a wider edge area to increase the payload capacity	50.21 dB 1.03 BPP
(Swain et al., 2018) [34]	PVD: 1×2 -pixel blocks through PVD method in overlapped fashion	42.96 dB 2.96 BPP
(Sahu and Swain, 2019) [29]	PVD- MF ISS based on PVD and modulus function (PVD) to enhance the peak signal-to-noise ratio (PSNR), and embedding payload (EP).	42.04 dB 1.5 BPP
(Mukherjee et al., 2020) [24]	PVD: A pixel value difference based text encryption and random pixel section.	41.59 dB 2.94 BPP
(ALabaichi, Al-Dabbas, and Salih, 2020) [4]	LSB: By applying 3D chaotic maps based secret map techniques Least significant bit through that called 3D logistic maps and 3D Chebyshev.	46.15 dB 1.0 BPP
(Seyyedi, Sadau, and Ivanov, 2016) [23]	Wavelet coefficients and RC4 encryption	65.9 dB 0.5 BPP
(Islam, Roy, and Laskar, 2018) [15]	LWT with ANN: decomposed The cover image is into three-levels LWT that indiscriminate in 2×2 non- superposition blocks that embedded on the LWT coefficient component by the encrypted binary data.	43.8 dB 512 bits
(Jude Hemanth et al., 2018) [16]	Genetic Algorithm (GA): Modified GA approach with frequency domain techniques for QR embedding.	50.29 dB 1.0 BPP
(Kadhim, Premaratne, and Vial, 2020) [17]	Edge-based image: Used an adaptive embedding process for the proposed approach with machine learning-based optimization techniques through the Dual-Tree (DT-CWT) subband coefficients.	53.71 dB 1.9 BPP
(Saeed et al., 2021) [21]	Content adaptive steganography: Divided the method to 3 sequential operations: Pixel Complexity Identification (PCI). Image Segmentation (IS).	50.98 dB BPP



Figure 3: The text frequency (redundancy) reduction within the Huffman coding

Table 4: numerical example within the proposed scheme: Five different symbols that yielded

Symbol	S	T	E	G	O
Frequency	22	10	8	6	6

3.1. Data preprocessing

The pre-processing stage is the most vital part of the proposed steganography scheme for achieving an improved security of the secret message and the payload capacity. Thus, two important processes occur simultaneously at this stage including the preparation of the secret message and cover image.

3.1.1. Enhanced Huffman compression coding

The pre-processing of the secret message involves two stages such as the text compression and fragmentation of secret text. In the proposed scheme, enables the pre-processing for the secret message that fund an extra standards of the security on top of increasing the payload capacity of the hidden bits. It is important to mention that any image steganography system have three salient features such as the maximum payload storage into the image, good imperceptibility witch is after embedding the image visual quality [29]. Thus, the enhanced Huffman compression coding assured the attainment of these aspects by the proposed steganography scheme. The main aim of the Huffman coding algorithm embedding after decrees the space of the image from the text. Figure 3 illustrates strategy for the text frequency (redundancy) reduction via the Huffman coding. In this process, the Huffman algorithm depends on the lowering of the frequent letters and offers them the priority code or short path in the Huffman tree.

For more understanding, a numerical example has been provided within the proposed scheme. This example used five different symbols that yielded 4:

The process started with "G" and "O" for the low frequency to build the tree structure of the first branch followed by the "E" and "T" at the same level. These parent nodes had the frequency of 12 and 18, respectively. Each parent node accumulated the frequency of their children in the tree. For instance, the high frequency letter "S" was created in the high level to construct the final tree which finally connected both children in one parent with the frequency 22. Figure 4. illustrates the typical Huffman coding tree structure.

The frequency was reduced and the compression for this example removed the 41% from the original text in case the same frequency of letters occurred as depicted below 5.

In the secret message preparation process, the bit stream must be fragmented. After the Huffman coding process, the produced text was converted into the digital form of 0 and 1. The processing of bits stream depended on the length of the data from the embedding stage. These bits were

Table 5:

Symbol	S	T	E	G	O
Frequency	22	10	8	6	6
Track code	0	100	101	110	111
Length	1	3	3	3	3

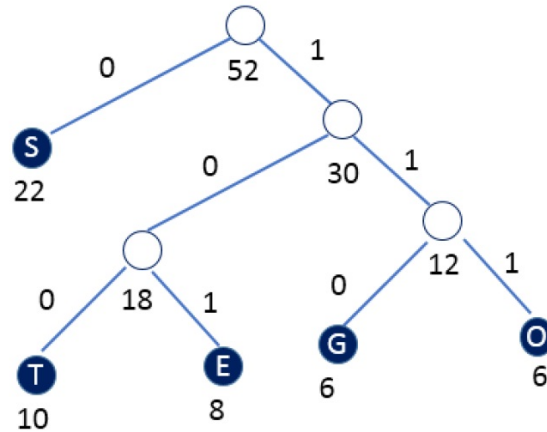


Figure 4: Huffman coding tree

manipulated before embedding to ensure the scheme reliability. In other words, the sample taken from these bits stream was compatible with the process in the embedding stage.

3.1.2. Image Preparation

Another preparation stage is applied to the proposed scheme before the embedding process to achieve an efficient embedding process called image preparation. The following sections explain the detailed process of image normalization technique and image transformation decomposition method.

Image Normalization Technique This preparation phase covered the selection and analysis of the given image before the implementation of any action on it. The image was normalized into a certain range before starting the other processing stages [30, 19]. The cover image has consisted of the 512×512 pixels, where any image used in the proposed steganography scheme followed this range via the expression:

$$I_N = (I - \min) \frac{new\ max - new\ min}{max - min} + new\ min$$

where I is original image, I_N normalized image, max is the maximum range of the selected image, min is the minimum range of the selected image.

Image Partitioning To achieve the objective of security, three phases process of image division with size (512×512) will be performed. First, divide the cover image into 64 sub-images called a block. Then select the pixels inside this block this selection is the most important process to keep the stego image of the same origin as possible. These processes for selection blocks and pixels with the proposed method illustrated in Figure 5. Also, used the random function is to achieve the security objective. Henon map function gets 10^{30} attempt that gives around 2100 this is enough to secure the text inside the image. Normal random used a single parameter to choose the number, the initial condition for this function (single) is 10^{15} , and probability of finding these numbers is 2^{50} . To increase the complexity of randomizing the pixels selection, two control values are used to select the pixels for two stages (block and pixel selection). In the steganography method, security plays an important rule in order to avoid any hacker from discovering our message in a stego image, by this method finding secret message is almost impossible.

The Henon map (HM) is one of important chaotic map. The HM is content two different

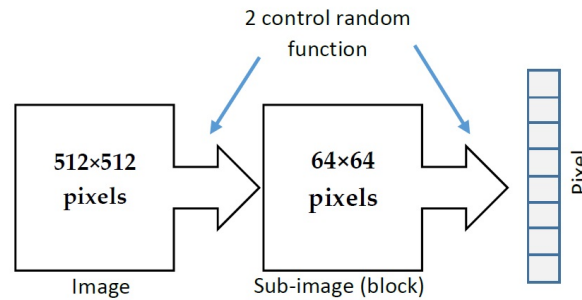


Figure 5: Selection blocks and pixels with the proposed method

parameters $a = 1.4$ and $b = 0.3$ used to be the chaotic. The main idea behind HM is a and b parameters. It can illustrate as coordinate point (X_n, Y_n) in the plane as seen in this equation:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases}$$

As aforementioned, any hiding method has two procedures such as the pixel selection and pixel insertion procedures. The pixel selection is responsible for achieving the enhanced security and imperceptibility of the data hiding system. In this perception, the present study aimed to maintain these two criteria. The pixel selection was accomplished in two stages. The first stage was the movement around the image via a single movement strategy.

3.2. Embedding Method

The new steganography method proposed in this research by hiding from the inside cover image a secret message using a new partitioning random pixel selection with two parameters. The basic essence of the proposed steganography scheme by hiding from the certain image a secret message and transferring it from sender to the authorized receiver side without any suspicion raised by the attackers or intruders. Each pixel in a colour or grayscale image consisted of decimal numbers that represented the contrast of this pixel or illumination. The grey image is consisting the decimal value from 0 - 255. The 0 value reflected black pixel value while the white pixel value reflected by 255 value. The image with the grayscale starting of the white value and ends in black value. The variance area with the corresponding decimal can be represented in an image. Figure 6, can clearly display serval variance and crossover from the low variance to the high variance pixels. In figure 7, the sharp diagonal edge located in the same variance when moved among two adjacent pixels with different large values. Due to the little variation between each pair, the best location to embed the secret message is shown in Figure 7. The maximum of two pixel values variance vary by the insertion like in this space.

The RGB image consisted from three values each pixel such as the (R) refers to the Red, the (G) refers to the Green, and the (B) refers to the Blue. Therefore, 24-bits the consist by the RGB pixels. The hiding in RGB pixels is more flexible due to the ability to jump over these three channels R, G or B. To vary the contrast in the RGB image, for hiding the secret key, per pixel checking three channels for choosing appropriate one. The robust embedding method by critical condition that taking care the condition while thresholding becomes essential.

Checking the embedding condition in the second stage. Operated the two stages simultaneously, each one completing the other. The selected pixels were accumulated in one vector. Upon completing the selection process, based on the new random technique the pixels were at random rearranged while keeping each pixel index. according to one case belong with disparity value, the strategy for the 8



Figure 6: Sub image and pixels variance in boat image in SIP dataset.

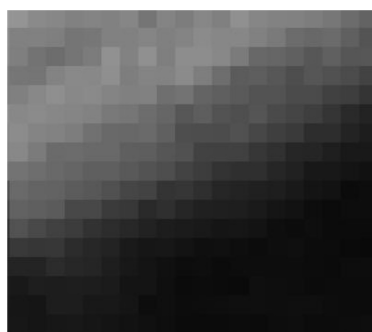


Figure 7: Sub image with edge pixels' variance in boat image in SIP dataset.

neighbour's was used to move through the image. These 8 neighbours covered the image and moving so many directions as horizontal, vertical and diagonally as shown in Figure 8.

The suggested method checked the middle pixels values (x, y) and its neighbours $(\pm x, \pm y)$. When these pixel values differed during to the threshold (T), then the pixel space was saved in vector form while moved accordingly [19, 2]. Otherwise, it was skipped to the other pixel coordinate. Consequently, the pixel was positioned high and low disparity between the two areas; where beside of near brightness was the embedment of the secret bit. Moreover, according to the threshold with the difference value between two pixels was chosen experimentally (the 4 decimal values) then beside a certain pixel the secret bit was embedded in two pixels. Conversely, when the secret bit was 1, then the secret bit was either not embedded with the low value or else (secret bit 0) with the high disparity value shown and explained in Fig 9. The disparity level check of each pixel enabled to scan whole the image for choosing the suitable location (pixel) to hide the secret bit. Subsequently, the proposed method with high security produced high imperceptibility, indicating successful suggested steganography scheme. furthermore the pixel selection strategy the pixel replacement utilized to fur-

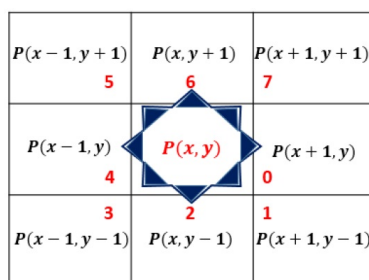


Figure 8: The 8 neighbours' pixel movement strategy

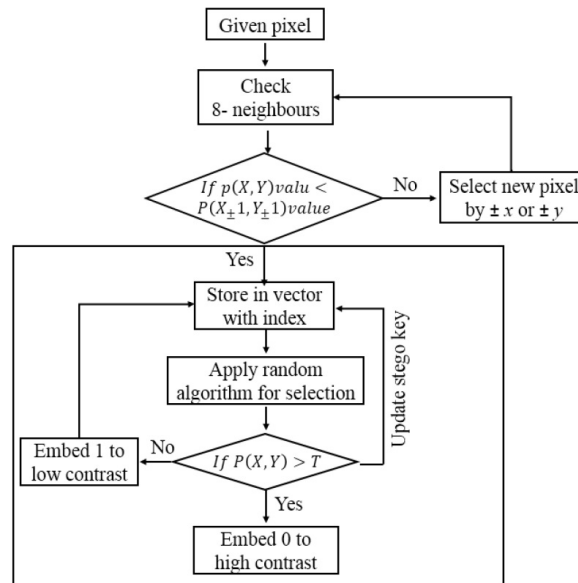


Figure 9: The embedding mechanism with the proposed method

ther enhancement imperceptibility and the security for the data hiding algorithm which is discussed below.

3.3. Extracting Method

Getting the embedded data is the main goal in the extracting stage (secret bits) from the LSB pixels and following the designed procedure in the embedding stage simultaneously. The agreement between the receiver and the sender for the information related by them while controlled by the extracting stage. The remaining information used by the implicit stego key that considered variable information based on image nature and environment. Reflected by image the mostly variable information while besides the fragment of the secret message the block partitioning. Public information called for some of them, moreover considered the private information as method follow up the embedding process. The security and imperceptibility are two main objectives were achieved in the proposed embedding and extracting stages. Figure 10 depicts the extracting and embedding procedure in the suggested ISS.

The embedding and extracting stages were responsible for keeping the image quality (imperceptibility) as high as possible. Meanwhile, the security of the proposed scheme was reflected in the two processes that worked together as one process such as the partitioning of the image and the randomization of both blocks and pixels selection.

4. Experimental Result

Essentially, the steganography methods must consider the appropriate evaluation metrics to make them reliable. Since its inception, good outcomes were achieved in terms of security and imperceptibility, steganography scheme has widely been used. Thus, the suggested steganography scheme considered all these evaluation criteria to improve security, quality, and capacity.

Numerous types of performance evaluation and security attacks face steganography systems such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and Histogram analysis. In this section, the performance for the suggested newly scheme was evaluated with these attacks and evaluations. The proposed work trained by using SIPI-dataset [46] with different medical

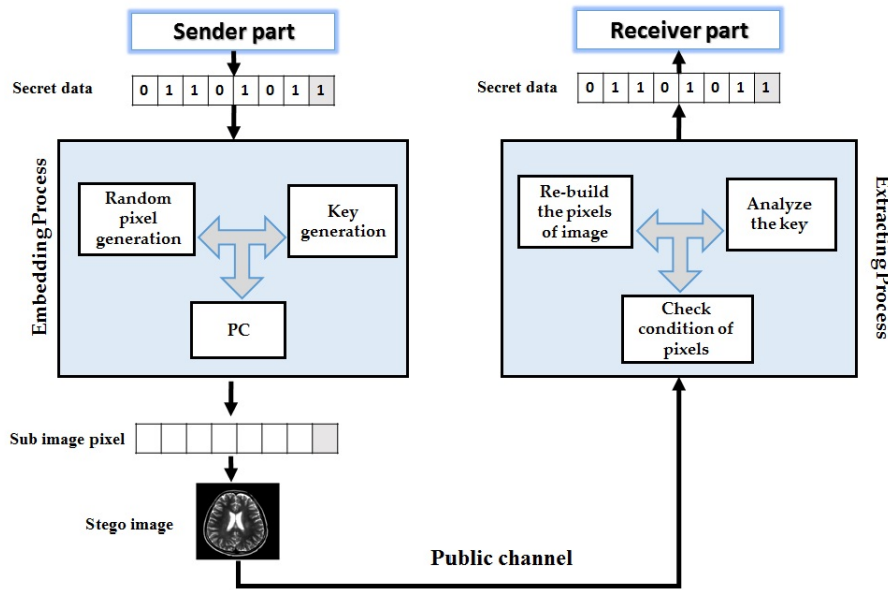


Figure 10: The imperceptibility and security design of the proposed method

images data from U.S. National-Library for Medicine. Image normally comes from scanner device some time become as 2D or 3D image as seen in Figure 10.

The present study considered the standard evaluation measures (objective methods) to validate the proposed ISS including the Embedding Capacity (EC), PSNR, SSIM and Histogram analysis. The EC value can be determining the values for the cover pixels with the message bits' ratio number [17] while the pixel's number that used in the suggested scheme related with them directly. Furthermore, one pixel embedded Different number of message bits as EC is expressed as:

$$EC = \frac{\text{The number of message bits}}{\text{The number of cover images's pixels}}$$

The following parameters were used in the simulation:

- For a given image of dimension (512 × 512) pixels, 16384 bytes corresponded to 6.25%, that means every 16 bits represented by two pixels, thus 1/16 = 6.25% when two pixels from 1 bit was embedded.
- For a given image of dimension (512 × 512) pixels, 32768 bytes were equal to 12.5%, implying that every pixel corresponded to 8 bits, so that 1/8 = 12.5% when one pixel from 1 bit was embedded.
- For a given image of dimension (512 × 512) pixels, 49152 bytes corresponded to 18.75%, signifying that every two pixels were assigned to 16 bits, accordingly 3/16 = 18.75% when one pixel from 1.5 bit was embedded.

Imperceptibility evaluating, PSNR was calculated after the embedding process and a comparison was made between the input image and result image. Human visual System (HVS) was considered to be imperceptibly to the embedding process, when the PSNR outcome was $\geq 30db$ [14]. The value of PSNR was calculated using the expression:

$$PSNR = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right) \tag{4.1}$$

Table 6: The SSIM and PSNR values for the Baboon image obtained using three types of embedding with different EP.

Embedding %	PSNR and SSIM			
	LSB - PSNR	SSIM	PC - PSNR	SSIM
6.25 %	62.910	0.9892	71.080	1
12.5 %	57.919	0.9787	69.402	1
18.75 %	55.999	0.9765	65.849	1

Table 7: The values of PSNR and SSIM for the Lena image obtained using three types of embedding with different EP.

Embedding %	PSNR and SSIM			
	LSB - PSNR	SSIM	PC - PSNR	SSIM
6.25 %	61.001	0.9891	70.425	1
12.5 %	58.998	0.9743	68.520	1
18.75 %	55.889	0.9656	65.211	1

with

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (4.2)$$

where max is the image maximum possible pixel value; and the dimensions of the image represented by m and n ; while the corresponding original and noisy pixel represented I and K . Thus, the similarity measurement between the stego image and the original image the amount of SSIM was used [17]. The value of SSIM (ranged from - 1 to 1, where in 1 specified between the stego image and original image no difference) was calculated via:

$$SSIM = \frac{(2P_O Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2 Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)} \quad (4.3)$$

where P_O, P_O^2 and σ_O^2 corresponding to the original image as well as Q_S, Q_S^2 and σ_S^2 denote the particular mean pixel value for the stego image, standard deviation and variance. Between the stego image and the original image covariance represented by $\sigma_{OS} \cdot C_1 = k_1 L$ and $C_2 = k_2 L$ are constants with $k_1 = 0.01, k_2 = 0.03$, and $L = 255$ for the grayscale image.

Table 6, 7 and 8 illustrates the obtained PSNR values for the three types of embedding (simple LSB, and PC) used execution evaluation for the suggested scheme with different EP for the greyscale standard SIPI images (Lena, Baboon and Paper (512×512)).

Generally, the calculated PSNR values for the color images are lower than the gray scale images through the color pixels image representation with 24-bits for one pixel as opposed to only 8-bits for the gray scale. In addition to implementing the proposed scheme on the SIPI standard image dataset, different medical images were taken from [36, 25] through the system test performance. A histogram graphical representation of intensity frequency in an image. In cover images histograms are considered an image property or as information related to the image. The histogram of the stego image similar to the histogram of the cover image because the hiding information was embedded based on our method which makes pixels less change the image. Finally, the stego image looks like

Table 8: The values of PSNR for the Paper image obtained using three types of embedding with different EP.

Embedding %	PSNR and SSIM			
	LSB - PSNR	SSIM	PC - PSNR	SSIM
6.25 %	62.999	0.9889	71.276	1
12.5 %	58.998	0.9765	68.464	1
18.75 %	56.339	0.9732	65.909	1

the cover image which is the main goal for the image steganography histogram as shown in Figure 11 and 12 for colour and grayscale images.

The evaluated test images with different evaluation parameters system performance shown in Table9.

5. Conclusion

An advanced image steganography method in this research based on Pixels Contrast (PC) with the method of eight neighbors and the Henon map algorithm to conceals information reports of the patient inside the different medical images to be available for the second party. Demonstrated our proposed method to enhance the security level with payload capacity to resolve the existing problems which mentioned in related work. Ccompressed the secret data prior embedding used the enhanced Huffman coding method. The Huffman coding method is used to 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 security and imperceptibility are solved based on proposed image partitioning with Henon map (HM) and PC with the eight neighbors method. Goal of the method is to increase imperceptibility by utilizing PSNR and SSIM measurements to check the stego image quality. The experimental results for the proposed method verified the worthiness terms of SSIM, PSNR and Histogram analysis.

References

- [1] B. Abd-El-Atty, A.M. Iiyasu, H. Alaskar, A. El-Latif and A. Ahmed, *A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms*, Sensors 20(11) (2020) 3108.
- [2] A. Abdulbaqi, M. Younis, Y. Younus and A. Obaid, *A hybrid technique for EEG signals evaluation and classification as a step towards to neurological and cerebral disorders diagnosis*, Int. J. Nonlinear Anal. Appl. 13(1) (2022) 773–781.
- [3] M.N. Abdulwahedand, S.T. Mustafa and M.S.M. Rahim, *Image spatial domain steganography: A study of performance evaluation parameters*, IEEE 9th Int. Conf. Syst. Engine. Technol. (2019) 309–314.
- [4] A. Alabaichi, M.A.A.K. Al-Dabbas, A. Salih, *Image steganography using least significant bit and secret map techniques*, Int. J. Elect. Comput. Engin. 10(1) (2020) 935–946.
- [5] T. AlKhodaiddi A. Gutub, *Refining image steganography distribution for higher security multimedia counting-based secret-sharing*, Multimedia Tools and Appl. (2020) 1–31.
- [6] S. Chatterjee, M. Biswas, D. Maji, B.K. Ghosh and R.K. Mandal, *Logarithm similarity measure based automatic esophageal cancer detection using discrete wavelet transform*, Recent Trends and Advances in Artificial Intelligence and Internet of Things (2020) 427–453.
- [7] Q.S. Hamad, M.Q. Mohammed and S.Q. Muhamed, *Surface water pollution monitoring system based on IOT*, Plant Arch. 20(2) (2020) 630–634.
- [8] M.M. Hashim, A.K. Mohsin and M.S.M. Rahim, *All-encompassing review of biometric information protection in fingerprints based steganography*, Proc. 3rd Int. Symp. Computer Sci. Intell. Control (2019) 1–8.

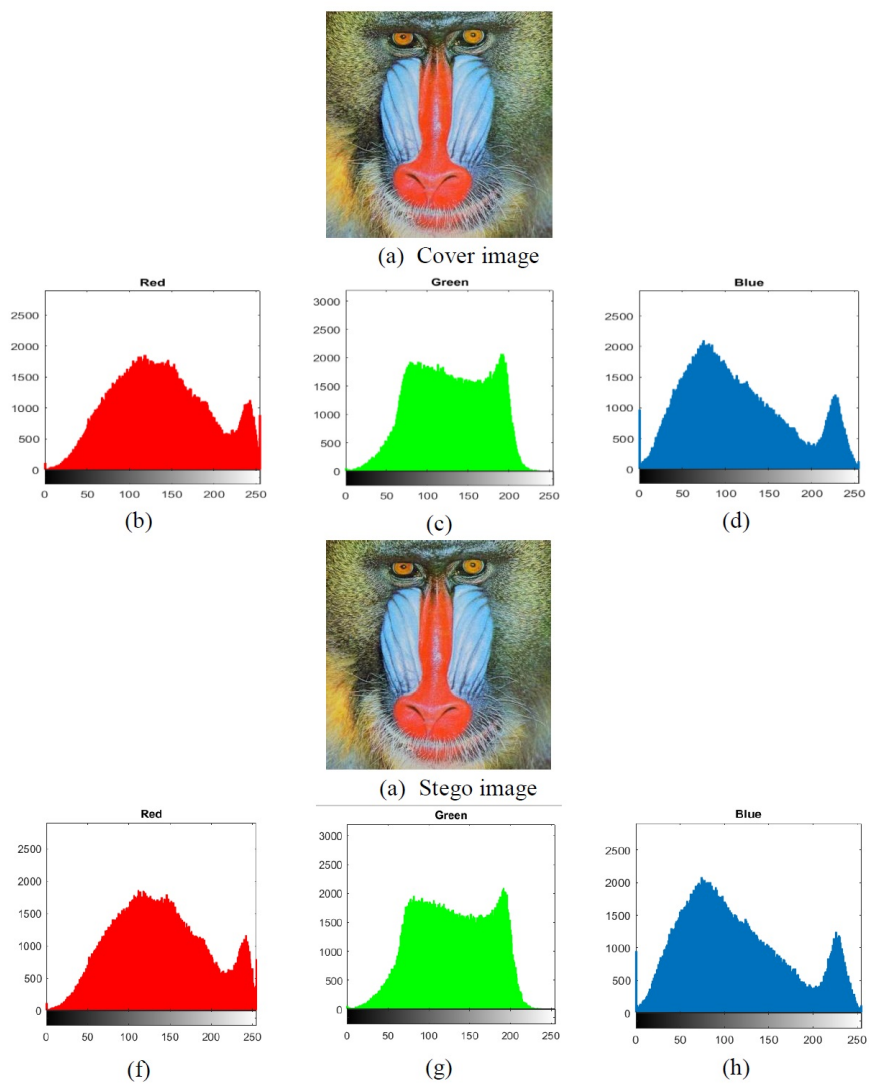
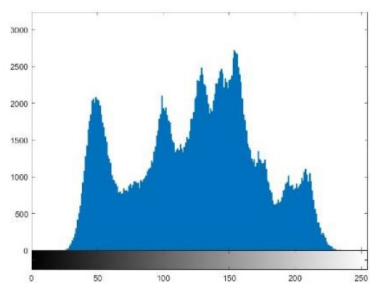
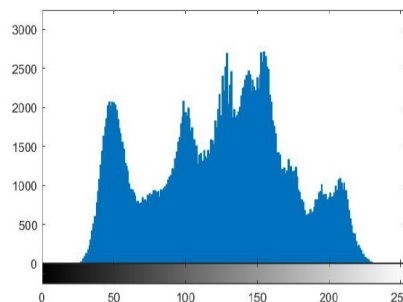


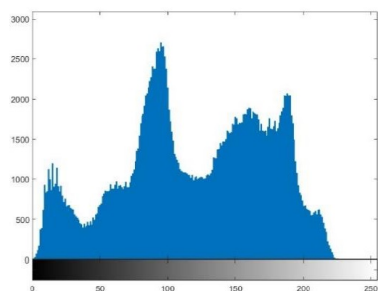
Figure 11: Histogram analyses with payload 6.25% for (a) refers for the cover image, (b) refers to the red channel of cover image, (c) refers to the green channel of cover image, (d) refers to the blue channel of cover image, (e) refers to the stego image, (f) refers to the red channel of cover image, (g) refers to the green channel of cover image and (h) refers to the blue channel of cover image



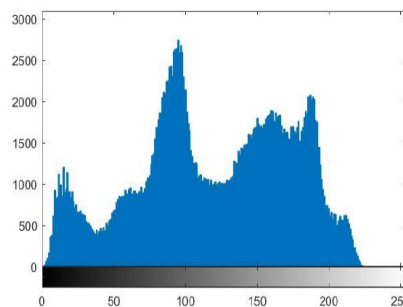
(a) The Original- carrier -image- Lena



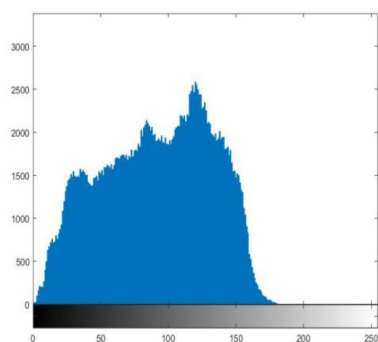
(d) The identical -stego -image- Lena



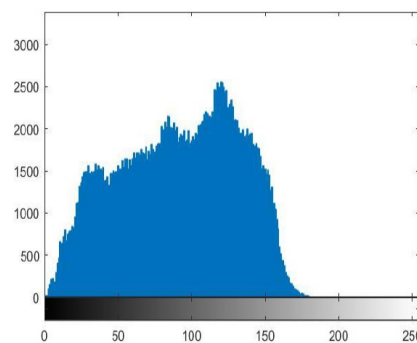
(b) The identical- carrier- image - Papper



(e) The identical -stego- image- Papper



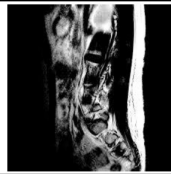
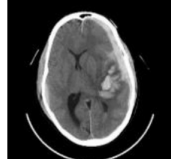

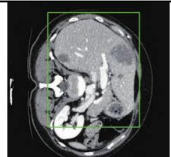
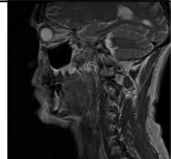
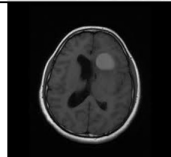
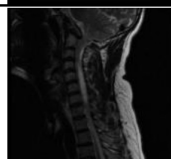


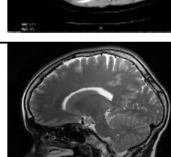
(c) The Original carrier -image- Zelda



(f) The identical stego- image -Zelda

Figure 12: The corresponding stego images and the Histograms for the original carrier images and the payload 6.25%.

Table 9: Used Test medical images to evaluate the system performance

Medical image	EP %	PSNR (dB)	SSIM
	6.25%	66.21	0.9999
	6.25%	65.11	0.9999
	6.25%	67.13	1
	6.25%	66.23	0.9999
	6.25%	66.87	1
	6.25%	64.14	0.9999
	6.25%	65.12	0.9999
	6.25%	63.45	0.9999
	6.25%	66.20	0.9999
	6.25%	66.52	0.9999

- [9] M.M. Hashim and M. Rahim, *Image steganography based on odd/even pixels distribution scheme and two parameters random function*, J. Theore. Appl. Inf. Technol. 95(22) (2017).
- [10] M.M. Hashim, S.H. Rhaif, A.A. Abdulrazzaq, A.H. Ali, M.S. Taha, *Based on IoT healthcare application for medical data authentication: Towards a new secure framework using steganography*, IOP Conf.Ser.: Materials Sci. Engin. 881(1) (2020) 012120.
- [11] M. Hassaballah, M.A. Hameed and M.H. Alkinani, *Introduction to digital image steganography*, Digital Media Stegan. (2020) 1–15.
- [12] R.K. Hussein, A. Alenezi, H.F. Atlam, M.Q. Mohammed, R.J. Walters and G.B. Wills, *Toward confirming a framework for securing the virtual machine image in cloud computing*, Adv. Sci. Technol. Eng. Syst. J. 2(4) (2017) 44–50.
- [13] M. Hussain and M. Hussain, *A survey of image steganography techniques*, Int. J. Adv. Sci. Tech. 54 (2013).
- [14] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T. Ho and K.H. Jung, *Image steganography in spatial domain: A survey*, Signal Processing: Image Communication, Signal Processing-Image Commun., 65 (2018) 46–66.
- [15] M. Islam, R. Amarjit and R.H. Laskar, *Neural network based robust image watermarking technique in LWT domain*, J. Intell. Fuzzy Syst., 34(3) (2018) 1691–1700.
- [16] D. Jude Hemanth, J. Anitha, D.E. Popescu and L.H. Son, *A modified genetic algorithm for performance improvement of transform based image steganography systems*, J. Intell. Fuzzy Syst. 35(1) (2018) 197–209.
- [17] I.J. Kadhim, P. Premaratne, P.J. Vial and B. Halloran, *Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research*, Neurocomput. 335 (2019) 299–326.
- [18] B. Karthikeyan, P. Nishmitha, B. Poojasree and S. Asha, *Authentication of secret message using Rabin-Karp in image steganography*, Int. Conf. Intell. Comput. Control Syst. (2019) 388–391.
- [19] G. Lakshmi, M. Ghonge and A.J. Obaid, *Cloud based IoT smart healthcare system for remote patient monitoring*, EAI Endorsed Trans. Pervasive Health Technol. (2021) 1–11.
- [20] N. Manohar and P.V. Kumar, *Data encryption and decryption using steganography*, 4th Int. Conf. Intell. Comput. Control Syst. (2020) 697–702.
- [21] M.Q. Mohammed, S.Q. Muhamed, M. Ievlanov and Z. Gazetdinova, *Improvement of the method of scenario analysis of functional requirements to an information system*, Eastern-European J. Enterprise Technol. 3(2(99)) (2019) 25–35.
- [22] B.S. Mohan, A.A. Mahmood, M.Q. Mohammed and N.D. Zaki, *Replicating the MAP kinase cascade in membrane computing*, J. Phys.: Conf. Ser. 1963(1) (2021) 012156.
- [23] S.Q. Muhamed, M.Q. Mohammed, M. Evlanov and H. Kliuchko, *The ADALINE neuron modification for solving the problem on searching for the reusable functions of the information system*, Eastern-European J. Enterprise Technol. 3(2(93)) (2018) 25–32.
- [24] S.Q. Muhamed, M.Q. Mohammed, T. Nayl, D. Mikhnov and A. Mikhnova, *Technology of structural optimization for subsidiary in enterprise information systems*, Int. J. Adv. Trends Comput. Sci. Engin. 8(1) (2019) 544–549.
- [25] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S.W. Baik, *A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image*, Multimedia Tool. Appl. 75 (2016) 14867–14893.
- [26] H. Nyeem, *Reversible data hiding with image bit-plane slicing*, 20th Int. Conf. Comput. Inf. Technol. (2018) 1–6.
- [27] J. Qin, Y. Luo, X. Xiang, Y. Tan H. Huang, *Coverless image steganography: A survey*, IEEE Access 7 (2019) 171372–171394.
- [28] A.K. Sahu and G. Swain, *A novel n-rightmost bit replacement image steganography technique*, 3D Res. 10(1) (2019).
- [29] A.K. Sahu and G. Swain, *An optimal information hiding approach based on pixel value differencing and modulus function*, Wireless Personal Commun. 108(1) (2019) 159–74.
- [30] P. Shah, P. Choudhari and S. Sivaraman, *Adaptive wavelet packet based audio steganography using data history*, IEEE Region 10 and the Third Int. Conf. Indust. Inf. Syst. (2008) 1–5.
- [31] G.J. Simmons, *The prisoners' problem and the subliminal channel*, Adv. Crypt. (1984) 51–67.
- [32] B. Stoyanov and B. Stoyanov, *Boost: Medical image steganography using nuclear spin generator*, Entropy 22(5) (2020) 501.
- [33] W. Su, J. Ni, X. Hu J. Fridrich, *Image steganography with symmetric embedding using gaussian Markov random field model*, IEEE Trans. Circuit.Syst. Video Technol. 5 (2020).
- [34] G. Swain, *Adaptive and non-adaptive PVD steganography using overlapped pixel blocks*, Arab. J. Sci. Engin. 43(12) (2018) 7549–7562.
- [35] M.S. Taha, M.S.M. Rahim, M.M. Hashim and H.N. Khalid, *Information hiding: A tools for securing biometric information*, Technol. Rep. Kansai Univ. 62(04) (2020) 1383–1394.

[36] <https://www.nlm.nih.gov/>.