International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 6, December 2022, pp. 6545~6558
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i6.pp6545-6558

Digital watermarking by utilizing the properties of self-organization map based on least significant bit and most significant bit

Khalid Kadhim Jabbar[1], Munthir Bahir Tuieb[1], Salam A. Thajeel[2]
[1]Department of Computer Sciences, College of Education, Mustansiriyah University, Baghdad, Iraq
[2]Department of Petroleum Technology, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Jul 2, 2021
Revised Jul 27, 2022
Accepted Aug 14, 2022

Keywords:

Digital watermarking
Information security
Least significant bit
Most significant bit
Self-organization map

ABSTRACT

Information security is one of the most important branches concerned with maintaining the confidentiality and reliability of data and the medium for which it is transmitted. Digital watermarking is one of the common techniques in this field and it is developing greatly and rapidly due to the great importance it represents in the field of reliability and security. Most modern watermarking systems, however, use the self-organization map (SOM), which is safer than other algorithms because an unauthorized user cannot see the result of the SOM's training. Our method presents a semi-fragile watermark under spatial domain using least significant bit (LSB) and by relying on most significant bit (MSB) when the taken values equal to (2 or 4 bits) depending on the characteristics of SOM through developing the so-called best matching unit (BMU) which working to determine the best location for concealment. As a result, it shows us the ability of the proposed method to maintain the quality of the host with the ability to retrieve data, whether it is a binary image or a secret message.

Corresponding Author:

Khalid Kadhim Jabbar
Computer Science Department, College of Education, Mustansiriyah University
Baghdad, Iraq
Email: khalid_jabbar@yahoo.com, khalidk.jabbar@uomustansiriyah.edu.iq

1. INTRODUCTION

However, steganography is an antiquated art, the beginning of personal computer (PC) innovation has given it new life. PC based steganography methods acquaint changes with computerized covers to install data unfamiliar to the local covers. Such data might be conveyed as text, parallel records, or give extra data about the cover. The requirements for information embedding within another cover, copyright protection and steganography are important work [1].

Computerized picture watermarking should meet prerequisites, for example keep up with image quality, hard to eliminate the watermark, nature of watermark extraction, and appropriate [2]. The accompanying variables are considered in planning an ideal information concealing framework [3]; the following properties must be met by the digital watermark technology in general. To begin, the embedded watermark should not affect the image visually and should be perceptually unnoticeable:

– Imperceptibility: the features of human visual or auditory systems are the basis for this idea. If the average human person is unable to distinguish between carriers that carry hidden information and those that do not, the embedded information is unnoticeable. One of the most important criteria in this field is that the cover is included without significant deterioration, deformation or loss in the quality of cover.

- Security: the criterion of a secure embed algorithm lies in a successful and robust embedding process where the embed information remains undetectable after its discovery, and this depends on the total amount of information about the embedding algorithm and the secret.
- Capacity: the thought of limit in information stowing away demonstrates the absolute number of bits stowed away and effectively recuperated by the steganography scheme.
- Robustness: Durability of the inserted information must remain unblemished if the stego-image goes through change, for example, linear and non-linear filtering; addition of random noise, scaling, rotations and loss compression.
- Embedding intricacy: if the image with the embedded message matches the source model from which the cover images were drawn, the information included is undetectable by intruders. For example, if the steganography approach includes a secret message in the noise component of the image, the steganography must take place without causing any statistically significant changes in the carrier noise. On the other hand, the size of the secret message and the nature of the cover image content have an impact on the inability to detect.

The technique of embedding a hidden information (i.e., a watermark) into digital data (such as audio, video, or digital images) in order to establish ownership or identify a buyer is known as digital watermarking. A logo, a label, or a random sequence can be used as a digital watermark. In general, visible and invisible watermarks are the two forms of digital watermarks. For authentication or identification, the embedded watermarks can be retrieved or recognized from the watermarked medium. Watermarks that are not visible can be divided into two categories: robust and fragile watermarks, because they are resistant to practically all types of image processing procedures, strong watermarks are commonly employed for copyright protection and ownership verification. Fragile watermarks, on the other hand, are mostly used for content authentication and integrity attestation because they are fully vulnerable to any changes.

2. BACKGROUND

The stego durability is improved by inserting it within lower-middle-significant bits. For good perception quality and watermark recovery, Kutter and Petitcolas [4] recommend inserting 80 bits of watermark data in the host image. This is enough to recover more than 80% of the watermark.

Parah *et al.* [5] devise a watermarking approach that uses a random vector address to embed the logo in the intermediate significant bits of the three host images at precise geographical places. In [6], a strategy for numerous watermarks is suggested that utilizes a square plan based on the human visual elements. An edge is utilized to decide the watermark esteems by altering first section of the symmetrical U framework acquired from singular value decomposition (SVD) [7]. In this investigation, picture steganography utilizing least huge piece and mystery map strategies is performed by applying 3D tumultuous guides, in particular, 3D Chebyshev and 3D calculated guides, to acquire high security. This method depends on the idea of performing arbitrary inclusion and choosing a pixel from a host picture.

According to Peng *et al.* [8], embedding two bits in each pixel increases the payload, and processing the two images for image integrity makes the work very difficult [9]. Create a watermark from most significant bit (MSB) by inserting them as standard bits and authentication bits, but according to Kutter and Petitcolas' [4] benchmark methodology, the watermark must be independent of the host image, which was violated. The proposed method that presented in [10] involved proposing a model based on the specified pixel values (first and last) from least significant bit (LSB), MSB based on the spatial domain for information masking and retrieval as the pixel values of the image would be a mixture of those bits. While [11] proposed a method that based on including the secret message in the small part of the host depending on the LSB, as well as hiding the confidential information in the host within the same field in the most important part of the digital image MSB by relying on the new hybrid technique (NHB).

The results showed a big difference when hiding information using LSB and MSB, noting that the proposed method has the ability to deal with information with different extensions such as DOX, XLSX, and PDF in [12], the research contributed to shedding light on the most important methods and mechanisms adopted in the field of embedding and retrieval of the binary watermark, and how to determine tampering area(s). While [13] present a block-wise and pixel-wise techniques, it depend on the false positive rate false positive rate (FPR) parameter, if the size of the block wise is small then the FPR will be decrease, otherwise it will be lower than that of the block-wise detection.

The proposed method that presented in [14] was embedded the gray image in the color image under transform domain. This is done by analyzing the gray image into a binary image by arranging the bit numbers from LSB to MSB by combining those binary bits with the corresponding blocks by using a quantization technique. In [15], it aimed to hide the secret data in the encrypted image by relying on what is called the reverse method of masking, this method determines the embedded pixels depending on the prediction errors

with the neighboring pixels in terms of strong correlation with them, and then the encoded image is created resulting from the rearrangement of those embedded pixels by taking advantage of the MSB properties. Another attempt presented in [16], the differences between LSB technology and MSB technology in hiding with color or gray image after including the secret message in the digital image was highlighted, specifically when embedded the secret information in small parts of LSB, as well as using MSB technology to hide that confidential information in the most important part of the digital image within spatial domain.

While study [17] present a method based on computing the security authentication code/watermark bit for each pixel based on MSB and subsequently the watermark bit will be embedded in LSB for each pixel based on a secret sequence obtained from an approved logistic map in the proposed method. In this method that presented in [18], eight bits are included in each of the two LSBs for the whole image in order to obtain the validation bit from the image summaries that are recovered from every 2×2 non-overlapping blocks based on the two techniques of wavelet and halftone after two summaries are generated from the host image.

3. SELF-ORGANIZATION MAP

self-organization map (SOM) or self-organizing feature mapping (SOFM) is a kind of artificial neural network (ANN) that utilizations prepared solo figuring out how to create low-dimensional (normally two-dimensional), discrete portrayal preparing tests. The info space, called the guide, is an approach to lessen the quantity of measurements. Self-sorting out maps are not quite the same as other counterfeit neural systems in that they apply contending adapting instead of blunder adjusting learning (for instance, back engendering with slope plummet), as in they use neighborhood capacities to safeguard the topology of the info space.

A SOM arrange normally comprises of two layers, the input layer and the output layer, see Figure 1. Not quite the same as the vast majority of the other neural systems, in SOM the input layer of source hubs is legitimately associated with the output layer of calculation hubs with no concealed layer. The hubs in the information layer indicate the characteristics (highlights) or, all the more for a most part, the factors contained in the information. Each bit of information is spoken to by a m-dimensional info vector, $x = (x_1, x_2, \ldots, x_m)$, whose components show the trait estimations of a specific dataset. In the event that there are enormous contrasts among the characteristic qualities in the informational collection, standardization of the information is required so as to keep away from the strength of a specific trait or subset of properties. This will give equivalent opportunities to all the traits and improve the numerical precision.

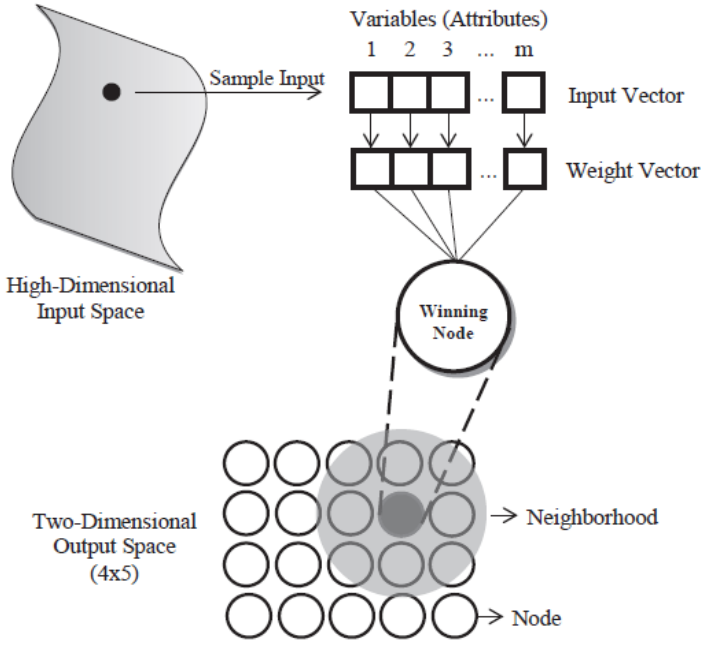

Figure 1. Self-organization map

Best matching unit (BMU) is reached by figuring the separation between completely input vectors and the example vector, at that point getting the weight going through every one of them. The victor weight

is the one with the most limited separation. There are numerous approaches to figure the separation. The weight vectors are instated to begin SOM mapping. An example vector is chosen arbitrarily and looking through the guide of weight vectors to discover which test is best spoken to by the weight, remunerating the weight that is picked by having the option to turn out to be progressively like the example vector that was haphazardly chosen. Neighboring loads are accessible for each weight vector and are near it, compensating the neighbors of that weight likewise by having the option to turn out to be increasingly like the picked test vector. Now the quantity of neighbors diminishes additionally weight learning rate diminishes after some time. This entire procedure is rehashed countless occasions [19].

4. LEAST SIGNIFICANT BIT AND MOST SIGNIFICANT BIT

LSB is the lowest bit in a sequence of numbers in the binary form e.g. in the binary number: (10110001), is the least significant bit is far right 1. The LSB used to embed the secret data in to the least significant bits of the pixel values in a cover image. While MSB represent the highest bit in a sequence of numbers in the binary form e.g. in the binary number of: (11001100), the most significant bit is far left 1 [20], [21].

5. THE PROPOSED METHOD

5.1. Statement of the problem

Images are considered one of the most important media, fastest and easiest media used to hide confidential information in them under spatial domain or frequency domain whether they were binary image or secret messages or gray image. The watermarked image content could be deliberately tampered with the presence of professional and easy-to-use of friendly programs, in addition may be destroyed unintentionally; for this reason, many attempts were made to maintain the secrecy of watermarked image by preserving the confidentiality of the method used for inclusion in the host. The main challenge of this diversity is allowed the proposed method to be able to deal with different media, while preserving the quality of the color image that used as a host for those media during the embedding stage with ability to recover the logo after extraction stage with preserving the quality of the host. The proposed method includes the process of hiding a binary image in the color image, as well as the ability to embedded the secret message in the color image under spatial domain by utilizing the properties of both LSB and the value that provided by MSB to determine the best hiding site in a manner that differs in subtraction and results from previous attempts by controlling the values of each.

In order to achieve the best results and observe the effectiveness of the proposed method and the quality of watermarked images after embedding stage when embedded the text/binary image in the color image, the proposed method depends on the mechanism that provided by SOM to determining the BMU value that was developed in the proposed method that used to determine the optimal hiding site to achieve the embedding stage and it is our contribution. Our proposed method embedded the binary image inside the color image under spatial domain based on LSB. The colors of image are classified into set of clusters or regions based on SOM, the regions have different sizes relied on color distribution in cover image. The varied distribution of colors is allocating randomly within the cover image. This randomization is exploited in the proposed approach, because this feature complicates finding a proper position of embedding information in the cover. The proposed method consists of following main stages:

5.2. Self-organization map stage

Considered one of the most important steps in the process of learning self-organizing maps, note the following algorithm:

Algorithm 1. Learning process.

```
Input: Weight, information vector.
Output: SOM Learning
Begin
    1. Weight instatement.
    2. The information vector is browsed the dataset.
    3. BMU is processed.
    4. The range of neighbors that will be refreshed is registered.
    5. Each load of the neurons inside the range will be changed in accordance with make
       them increasingly like the information vector.
    6. Steps from 2 to 5 are rehashed for each information vector of the dataset.
    7. END; END.
```

The training sample is supplied to the network SOM, the distance is computed based on Euclidean to all weight values which arranged as vectors, the most similar neuron to the input sample in term of weight vector is named the BMU. The BMU weights and nearest neurons in the SOM lattice are regulated concerning to the input vector. The changing degree of distance reduces with time according to BMU. The following formula for a weight vector *(Wv (t))* with neuron:

$$\mathrm{Wv}(\mathrm{t}+1) = \mathrm{Wv}(\mathrm{t}) + \Theta(\mathrm{v}.\mathrm{t})\alpha(\mathrm{t})\big(\mathrm{D}(\mathrm{t}) - \mathrm{Wv}(\mathrm{t})\big) \quad (1)$$

where $\alpha(t)$ is a learning coefficient which is decreasing monotonically and $D(t)$ is denote to the input vector. The $\Theta(v, t)$ indicates a neighborhood function relies on the distance of lattice. The complete memory of SOM is kept inside of the weighted links between the output and input layer. The weights are modified in apiece epoch. An epoch takes place as soon as training data is offered to the SOM and the weights are attuned based on the outcomes of the training data sample.

Algorithm 2. Self-organization map.

Input: O, SOM. (Where O: original image)
Output: BMU.
Begin
1. Read the original image O.
2. Apply SOM over the whole O to produce the nodes O_n.
3. Initialize a weight for each O_n (O_{n0}, O_{n1},…, O_{nm}) to produce the weighted victor as O_w.
4. For each O_n find the Euclidean distance between O_n and O_w to produce O_E'. (where O_E': Euclidean distance)
5. Compute Best Matching Unite (BMU) during the iteration process for each pixel of the whole O by using O_w'.
6. Updates the neighbors of BMU and BMU itself by engage them to input.
7. IF iteration reached THEN
   GOTO step 8
   ELSE
   GOTO step 4: END.

5.3. Choose the optimal embedding site stage

The regions of colors are arranged from larger to smaller distance or verse versa. Then choosing half of center region for embedding start depending on comparison between two most significant bit (MSB) of the pixel be for embedding and two MSB of random number, if the (2 MSB of pixel < 2 MSB) of random then embedding will start from small to large else it will start from large too small. The binary image will be read either column or row; the method depends on the difference between center byte of secret message and first eight bits of center pixel.

Algorithm 3. Choose the optimal hiding site.

Input: BMU, R_n. (Where R_n: random number)
Output: H_S, H_L.
Begin
1. Measure the regions of BMU to produce the BMU'.
2. Generate the random numbers R_{ni}.
3. Choose the W, where W represent the value of (MSB =2 bits/ 4 bits) for each R_n to produce R_n'.
4. Choose the W form MSB of each BMU' to produce BMU''.
5. IF R_n < BMU'' THEN
   Start form smallest region to largest region for hidden (hiding site is H_S).
   ELSE
   Start form largest to smallest region for hidden (hiding site is H_L).
6. END; END.

5.4. Embedding stage

After the process of calculating the weights from the original image and configuring the SOM to get the BMU through which adding to R_n we will get the best concealment areas, which are *HL\Hs*, and as shown in the Figure 2. After obtaining the concealment sites, the basic embedding stage will take place, that need the original image, LSB, and binary data (image/Message). Figure 2 illustrate our proposed embedding stage, while algorithm 4 illustrates the embedding process:

Algorithm 4. Embedding stage.

Input: O, B_i, BMU'', R_n. (where B_i: binary image).
Output: W_i.
Begin
1. Read O, and B_i.

2. Apply SOM to the whole O to arrange color and produce O'.
3. Read BMU''.
4. Read R_n.
5. Perform embedding process between B_i and O' inside (H_S\H_L) according W based on LSB, to produce watermarked image as W_i.
6. END; END.

During the embedding stage, our proposed method computes the LSB and MSB from the algorithm 5:

Algorithm 5. Compute LSB.

Input: Cove image, Binary (message\logo)
Output: Stego Image.

1. Read the host image.
2. Read the logo in the binary form.
3. Calculate LSB of each pixel of host image.
4. Replace the LSB of the host image with the corresponding bit of binary sequence one by one.
5. **END; END.**

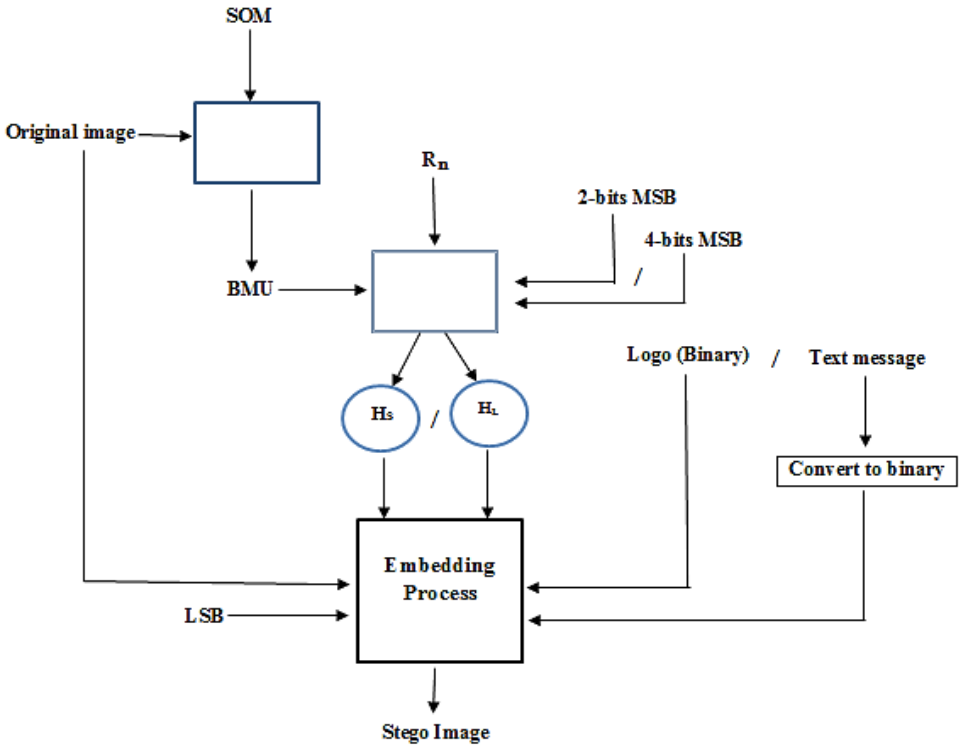

Figure 2. The general diagram of our proposed method

5.5. Extraction stage

The extraction watermark is one of the important stages. Especially in the process of verifying reliability (image authentication), in addition to illustrate the most important results through which the extent of integration in the proposed embedding algorithm is known. The extraction stage illustrated in the algorithm 6:

Algorithm 6. Compute MSB.

Input: Cove image, Binary (message\logo)
Output: Stego Image

1. Read the host image.
2. Read the logo in the binary form.
3. Calculate MSB of each pixel of host image.
4. Replace the LSB of the host image with the corresponding bits of binary sequence one by one.
5. END; END.

Algorithm 7. Extraction stage.

Input: W_i, B_i, BMU'', R_n.
Output: O', W'.
Begin
1. Read W_i.
2. Calculate LSB of each pixel of stego image.
3. Retrieve bits and convert each 8 bit into character.
4. Perform extraction process over W_i from ($H_S \backslash H_L$) to produce the recovered image O' and extracted watermark W'.
5. END; END.

6. EXPERIMENTAL RESULT

The evaluation of our proposed method is labeled for improving the hiding fastness, the evaluation implemented in various characteristics to improve the performance of hiding process. It also improves the fastness of hiding and extraction process of images. A group of different samples was dealt with in the results paragraph in order to obtain different results according to the type of image used by take into consideration image texture such: high texture, low texture, standard, and painted, all of them with size of 256×256 and with different image file format such as: (BMP, PNG, and JPG); Table 1 shows our approved samples, while Figure 3 shows the original samples that used in our proposed method, furthermore; Figure 4 shows the original watermark (binary logo with size of 128×128); Our proposed method was tested with several hosts such as: i) color image with binary logo and ii) color image with text message.

Table 1. The samples

Name	Texture
Lena	Smooth
Baboon	High texture
Peppers	Low texture
Prush	Painted

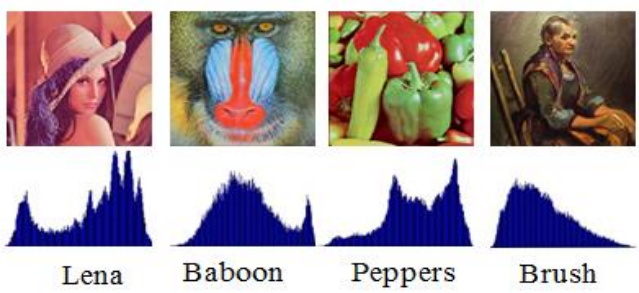

Figure 3. The different samples with histogram

Figure 4. The original watermark

6.1. Color image with binary logo

The most important results that obtained after applying the proposed method between the color image and the binary watermark will be reviewed. In this regard, two types of basic criteria were relied upon. It is shown in the following two sections:

6.1.1. Objective side

Figure 5 shows the watermarked image (2 bits MSB), while Figure 6 presents the extracted watermark, and Figure 7 shows the watermarked images with histograms (4 bits MSB), and the extracted watermark illustrated in Figure 8. Our proposed method survives the host quality after completing the embedding process when the value of (MSB=2 bits) with the possibility of retrieving the binary watermark after the embedding process without any distortion, but when the value of (MSB=4 bits) became lost in the color image, in addition to the inability to retrieve the watermark. The reason for this is due to two things: the first is that the embedding process in order to be foolproof and with a good result, the best domain for embedding process is frequency domain, but this does not mean that the spatial domain does not perform the desired goal or it is incompetent, but in such a case it is possible that the results are best in the case of four bits if the embedding process field is frequency domain. The second reason is because the amount of additional data added per pixel is due to the use of LSB and then the use of MSB again.

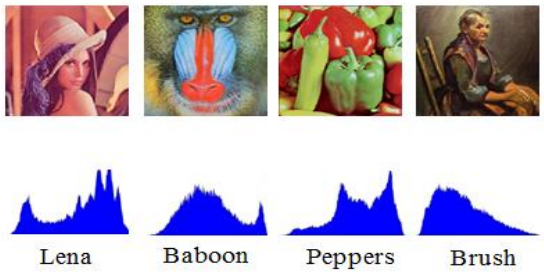

Figure 5. The watermarked image (2 bits MSB) with histogram

Figure 6. The recovered watermark from the watermarked image (2 bits MSB)

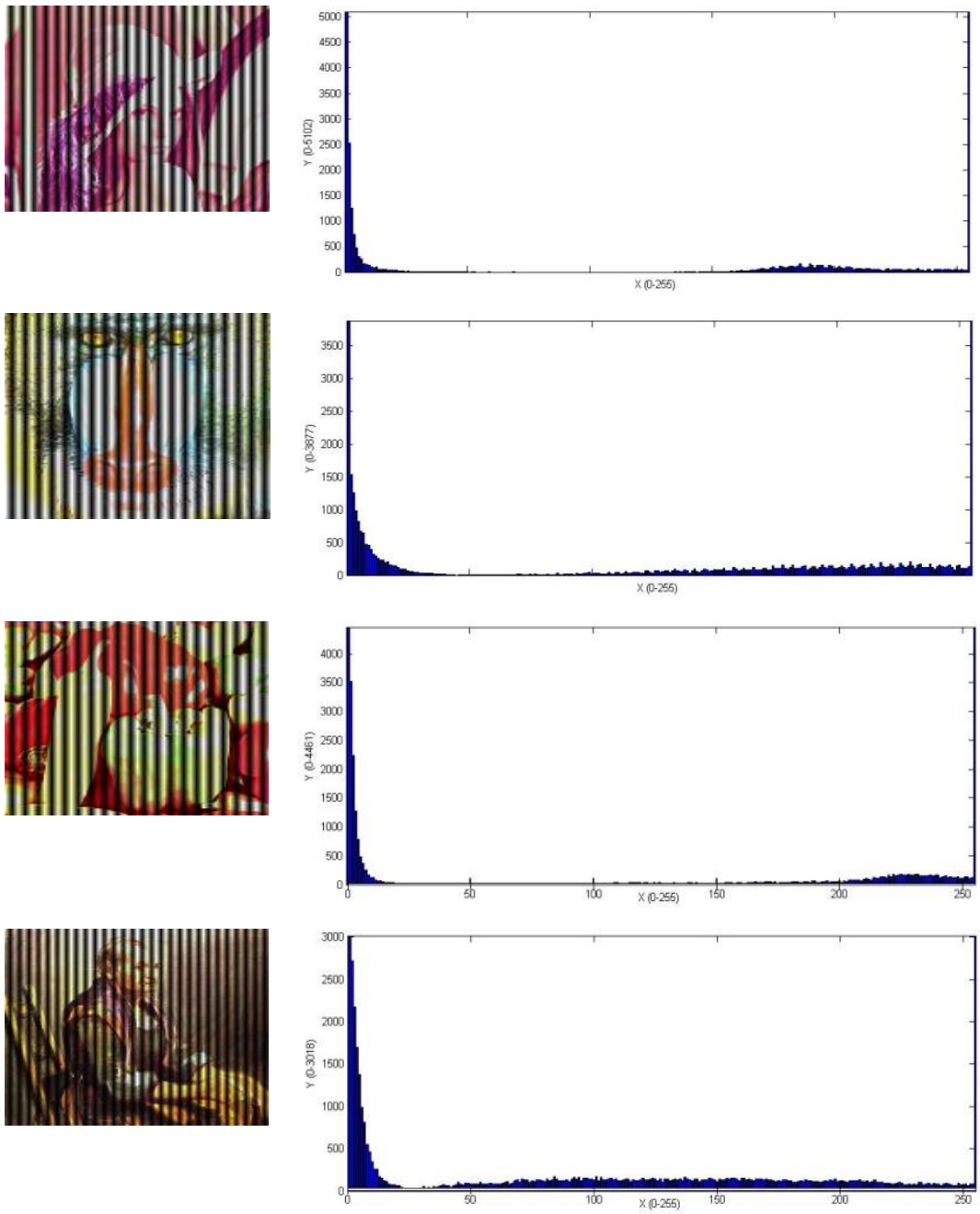

Figure 7. The watermarked image (4 bits MSB) with histogram

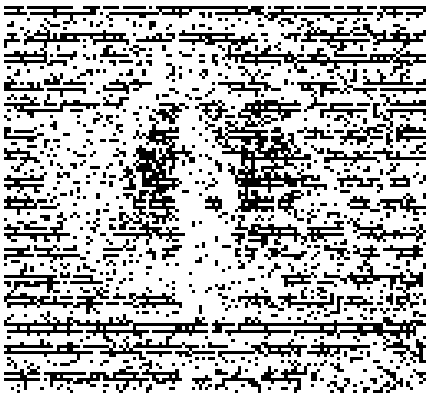

Figure 8. The recovered watermark (4 bits MSB)

6.1.2. Subjective side

Through the use of a set of well-known measurement tools such as: mean square error (MSE), peak signal to noise ratio (PSNR), normalized cross-correlation (NK), accuracy rate (AR), maximum difference (MD), normalized absolute error (NAE), runtime (MS), and bit error rate (BER), that used to illustrate the difference between the original image and watermarked image after embedding stage when: (MSB=2 bit, and MSB=4 bit), furthermore; to obtain the ability of our proposed method to recovered the watermark form the watermarked image after embedding stage when: (MSB=2 bit, and MSB=4 bit). These measures are described as:

a. Mean square error (MSE)

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

Where I(i, j) represent the original image and $K(i,j)$ is an encrypted image. A low value of MSE gives the optimal difference between original image and its encryption image [17].

b. Peak signal to noise ratio (PSNR)

The fundamental presentation of any stenographic calculation is the stego-picture quality and the implanting limit that the calculation gives to convey privileged information. The stego quality is measured utilizing the picture metric pinnacle sign to clamor proportion PSNR:

$$\text{PSNR}=10\times\log\left(\frac{255^2}{MSE}\right) \quad (3)$$

The value of MSE is calculated from (2). A high value of PSNR gives the better result of difference between original image and its encryption image [22].

c. Normalized cross-correlation (NK)

$$\text{NK}=\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j).K(i,j)]}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j).I(i,j)]} \quad (4)$$

Where I(i, j) represent the original plain image and K(i, j) is an encryption image, low values of NK measure the differences between the original watermark and extracted watermark.

d. Accuracy rate (AR)

It computes from (6) between original watermark and recover watermark, AR is used to measure the difference ratio between the original watermark and the recovered one [23], its defined as (5).

$$AR = CP/NP \quad (5)$$

e. Maximum difference (MD)

$$\text{MD}=Max(Max\big(I(i,j) - K(i,j)\big)) \quad (6)$$

Where I(i, j) represent the original plain image and $K(i,j)$ is an encryption image. A large value of (MSE, MD) gives the difference between original image and its encryption image [24].

f. Normalized absolute error (NAE)

$$NAE=\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[|I(i,j)-K(i,j)|]}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)]} \quad (7)$$

Where I(i, j) represent the original plain image and K(i, j) is an encryption image. A large value of NAE gives the difference between original image and its encryption image [25]. The experimental results of our proposed method after embedding process that computed between the original image and the watermarked image when (MSB=2 bits) illustrated in Table 2, while the results when (MSB=2/4 bits) illustrated in Table 3 and the value of MSE and AR are computed between the original watermark and the extracted watermark.

Table 2. The value of quality measurement after embedding process, (LSB=2 bits)

WI	MSE	PSNR	NK	AR	NAE
Lena	0.0000	51.1115	0.0202	0.9985	0.0099
Baboon	0.0040	51.1138	0.8566	0.99792	0.1070
Pepear	0.0006	50.4347	0.6576	0.99963	0.1006
Brush	0.0963	50.2450	0.3585	0.67520	0.2108

Table 3. The value of quality measurement after embedding process, (MSB=2/ 4 bits)

WI	MSE	PSNR	NK	AR	NAE
Lena	1.2300	14.2564	1.9936	1.9987	1.2543
Baboon	1.9931	14.0012	1.9854	1.3147	2.6487
Pepear	1.1458	13.5478	1.9993	2.2975	2.4878
Brush	1.9851	13.0010	2.9852	2.0852	2.1132

From the results reached and shown in Tables 2 and 3, it was found that the proposed method has the ability to maintain the quality of watermarked image with the possibility of retrieving the watermark after the embedding process, in addition to the possibility of achieving good results with the scales used in this aspect when the value of (MSB=2 bits), as shown in Table 2 based on the nature of the measures that used to measure the quality of watermarked image after embedding process, in addition to that the variation is clear in the results that shown in Table 3, where it was found that the watermark cannot be recovered after embedding process in addition to the quality of the resulting image is not acceptable; because of the increase in the amount of extra data per pixel when (MSB=4 bits), it distorted the watermarked image after embedding process.

6.2. Color image with text message

As we reviewed the results obtained after applying the proposed method between the color image and the binary watermark, we would like to highlight the most important results that were obtained after the embedding stage between the host and the text message. So, the two types of computational criteria were used. It is described in the following two sections:

6.2.1. Runtime analysis based on stego message size

Runtime is the measure of time occupied to retrieve the embedded data with respect to their size. Millisecond (MS) is the unit to measure runtime, the following mathematical equation to calculate the runtime as (8).

$$Runtime\ (MS) = Retrieval\ Time * Data\ Size \quad (8)$$

Secret text messages with size of (3.5 k) were used in order to discover the difference in the results between the different pictures according to the differences in image texture. It is possible to use other sizes of text messages and the results are close as they were predetermined. The process of embedding was applied between the color image and the secret message (in text form), after converting the message to the binary form then the binary bits are embedded in the host under spatial domain based on LSB when (MSB=2 bits) the results shown in Table 4, while the result that obtain after embedding process when (MSB=4 bits) illustrated in Table 5.

In the Tables 4 and 5, text messages of different sizes were used, after converting the secret message to the binary form, it was embedded in the color image under spatial domain by utilize the properties of LSB,

and by controlling the value of MSB, the following results obtained: i) when (MSB=2 bits) then the run time values are higher and ii) when (MSB=4 bits) then the run time values are lower.

Table 4. Runtime analysis (MSB=2 bits)

Host Name	Size/ K	Runtime/sec
Lena	62.7	0.700472
Baboon	87.4	2.035349
Pepear	39.4	0.664984
Brush	90.2	1.985545

Table 5. Runtime analysis (MSB=4 bits)

Host Name	Size/ K	Runtime/sec
Lena	62.7	1.986514
Baboon	87.4	3.123560
Pepear	39.4	2.112477
Brush	90.2	3.786212

This discrepancy in the results led us to a new result that differs from the results that reached after embedded the watermark in the color image, due to the difference in the size of the data between the two cases. Our result is the possibility of achieving better run time in the case of (MSB=4 bits) and conversely in the case of (MSB=2 bits). So, the runtime is relied on the data Size and retrieval time, the method is more efficient when lower runtime is obtained.

6.2.2. Bit error rate on image steganography

The performance of image-based information hiding is measured relying on the rate of bit error. The rate of bit error indicates to the number of bit errors (in the terms of KB) divided by the overall number of conveyed bits (in the terms of KB) at a certain period of time. The performance of embedded the secret message inside the host is measured based on the rate of bit error and is formulated as given (9).

$$Bit\ Error\ Rate\ (BER) = Bit\ Errors\ SMS * 100 \quad (9)$$

According to (3) the lower the rate of bit error, the performance is thought to be higher, Table 6 presents rate of bit error with respect to images in different sizes when (MSB=2 bits), while Table 7 illustrate the value that obtained when (MSB=4 bits) that measured in terms of KB. The growing size of hidden message leads to increase the bit error rate.

Table 6. Bit error rate (MSB=2 bits)

Host Name	Size/K	Bit Error Rate
Village	3.7	13.23
Lena	4.5	19.33
Peppers	3.1	11.14

Table 7. Bit error rate (MSB=4 bits)

Host Name	Size/K	Bit Error Rate
Village	62.7	53.0023
Lena	87.4	57.0031
Peppers	39.4	51.0114

The increase in the size of secret message leads to an increase in the bit error rate, on the other hand; the bit error rate has been reduced in the proposed method when the value of (MSB=4 bits) in order to accommodate the largest amount of data and distribute it over the host area and thus the bit error rate has become less, and this explained in the previous tables. A different methodology used to present our proposed method and the results that applied, this difference in the method of presentation is what distinguishes our proposed method

Our proposed method has the ability to deal with different images texture regardless of their color nature due to the mechanism that used in the embedding stage while ensuring good results with each image, on the other hand; there is a convergence between our proposed method with [7], and the results are close in terms of the quality of the watermarked image after the embedding stage, but the first depends on the gray image as a basic part of the embedding process after converting it to the binary form, and this represents a weakness in this method if it is applied to color images. As for the method [10], it gave good results with MSB depending on the reverse method that aimed to embed the secret data in the encrypted image which is generated from the same image depending on the error coefficient. It in turn makes the proposed method good with MSB technology but it does not deal with LSB while our method had good results with the use of LSB and also with MSB in including confidential data in the color image in terms of execution time.

On the other hand, the comparison between our proposed method and [13] resulted in close results with the standards used to measure the quality of the watermarked image with the adoption of the same LSB technique in the embedding process. In this state, if the embedding process is based on MSB then the watermarked image will be subject to distortion after embedding stage and watermark bits cannot be retrieved from it. As for the other methods mentioned in the previous studies, the proposed method was compared from a group of previous methods, and the results were analyzed according to Table 8 represents the results that were reached during that comparison.

From Table 8, it is noted that our proposed method has the ability to survive image quality after the embedding stage when using LSB technique, as well as with using MSB; on the other hand, the execution time spent is better with using MSB to hide the secret message inside the color image. Especially when (MSB=4 bits), and these results were different from what the methods that were compared with other methods that mentioned, and the reason for that is due to our use of SOM technique which allowed us to determine the optimal hiding site after utilizing a BMU which it developed in our proposed method to work on determining the best hiding site according to the nature of the media (color image, text).

Table 8. Comparison between the proposed methods with others

Proposed Method	Embedding Technique	Time (millisecond)		MSE (dB)		PSNR (dB)		Survive	
		LSB	MSB	LSB	MSB	LSB	MSB	LSB	MSB
[2]	LSB/MSB	159	262	0.307	0.114	53.263	15.492	Strong	Middle
[9]	LSB/MSB/NHB	160	280	0.371	52.481	52.480	10.380	Strong	Middle
[6]	LSB/MSB	232	319	0.581	21.380	50.910	21.381	Strong	Middle
[11]	LSB/MSB	178	290	0.410	110.977	51.320	18.331	Strong	Weak
[12]	LSB/MSB	266	385	0.031	22.378	49.592	22.917	Middle	Middle
[14]	LSB/MSB	301	395	0.007	97.044	46.010	42.401	Middle	Weak
Our proposed method	LSB/MSB/SOM	1.986	0.700	0.000	1.230	51.111	14.256	Strong	Strong

7. DISCUSSION

The main challenge that illustrated in the proposed method is who to make the method able to deal text and binary image in same time with survive the quality of the host under spatial domain by utilizing the properties of SOM by using LSB, and MSB. The scientific contribution in this paper is through comparison in the results that are obtained after hiding the binary image in the color image, taking into account the variation of images texture that used in the proposed method, on the other hand, the secret message data that is hidden in the color image, all within the time domain with different sizes for confidential message files. The embedding stage is accomplished by taking advantage of SOM properties depending on LSB, MSB, and we also controlled the MSB values and observed the variance in the results obtained and explained that.

On the other hand; The methodology used in the proposed method differs from the others through the use of the same embedding and retrieval algorithm in the case of including a binary image with the color image, as well as including the secret message in the same color images that were dealt with in the first case, the proposed method relied on three techniques: LSB, MSB, and SOM in order to determine the best location for concealment by relying on BMU, which determines that location depending on the type of host and the type of medium, the proposed method deals with all types of color images regardless of the color nature of that image and it also deals with media of the type text, binary image and this in turn, the proposed method provided the ability to determine the feasibility of the embedding and retrieval algorithms according to the used technique LSB and MSB depending on the values of each.

8. CONCLUSION

The results obtained proved that the proposed method preserved the image quality after the embedding process with the possibility of retrieving the watermark successfully when the value of (LSB, MSB=2 bits), and when we changed the values for (LSB, MSB=4 bits), it is noticed that the difference in that the resulting image was of lower quality with (LSB, MSB=4 bits). The possibility of retrieving the binary image is due to the increase in the value of the last bit that was hidden, and the aim of this experiment is to ensure the possibility of the technology according to the values specified for it in maintaining the quality of the host image after the embedding process. On the other hand, the quality of the host image was not affected after the inclusion process when the values of (LSB, MSB=4 bits), on the contrary, gave better results at the time of implementation, and the reason is due to the color nature of the host image and on the other hand, the embedding time was short and the ability to retrieve the secret message. May be a group of known techniques were used in the proposed method, such as: (SOM, LSB, and MSB), which rely on BMU, R_n to determine the best location for concealment.

After the proposed method was compared with a set of previous methods, the results were converging in several aspects, including the values that were reached using the known standards that are used to measure the quality of the image in this aspect, and it was also found that the proposed method has the ability to provide a safe environment for the inclusion of confidential messages in true images as well as the inclusion of binary images in color images so that we can later achieve a higher level of security for these media. From the obtained results, our proposed method presents a semi-fragile watermark scheme with

ability to survive the watermarked image after mild-processing. The methodology used in the proposed method is different and it is almost a new attempt in the aspect of using different media in the same proposed algorithm, as images and texts were dealt with simultaneously, and this is considered a good contribution to this topic.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq for its support in the present work.

REFERENCES

[1] Akhi and S. Gawande, "A review on steganography methods," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 10, pp. 4635–4638, 2013.

[2] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1850–1860, Jun. 2019, doi: 10.11591/ijece.v9i3.pp1850-1860.

[3] V. A. Kumar, C. Dharmaraj, and C. S. Rao, "A hybrid digital watermarking approach using wavelets and LSB," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 5, pp. 2483–2495, Oct. 2017, doi: 10.11591/ijece.v7i5.pp2483-2495.

[4] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking system," in *Proceedings of SPIE - The International Society for Optical Engineering*, Apr. 1999, pp. 226–239, doi: 10.1117/12.344672.

[5] S. A. Parah, J. A. Sheikh, U. I. Assad, and G. M. Bhat, "Realisation and robustness evaluation of a blind spatial domain watermarking technique," *International Journal of Electronics*, vol. 104, no. 4, pp. 659–672, Apr. 2017, doi: 10.1080/00207217.2016.1242162.

[6] F. Ernawan, S.-C. Liew, Z. Mustaffa, and K. Moorthy, "A blind multiple watermarks based on human visual characteristics," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 4, pp. 2578–2587, Aug. 2018, doi: 10.11591/ijece.v8i4.pp2578-2587.

[7] A. Alabaichi, M. A. Ali 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, Feb. 2020, doi: 10.11591/ijece.v10i1.pp935-946.

[8] Y. Peng, X. Niu, L. Fu, and Z. Yin, "Image authentication scheme based on reversible fragile watermarking with two images," *Journal of Information Security and Applications*, vol. 40, pp. 236–246, Jun. 2018, doi: 10.1016/j.jisa.2018.04.007.

[9] C. Qin, H. Wang, X. Zhang, and X. Sun, "Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode," *Information Sciences*, vol. 373, pp. 233–250, Dec. 2016, doi: 10.1016/j.ins.2016.09.001.

[10] S. O.Akinola and A. A.Olatidoye, "On the image quality and encoding times of LSB, MSB and combined LSB-MSB steganography algorithms using digital images," *International Journal of Computer Science and Information Technology*, vol. 7, no. 4, pp. 79–91, Aug. 2015, doi: 10.5121/ijcsit.2015.7407.

[11] Y. Y. Wai and E. E. Myat, "Comparison of LSB, MSB and new hybrid (NHB) of steganography in digital image," *International Journal of Engineering Trends and Applications (IJETA)*, vol. 5, no. 4, pp. 16–19, 2018.

[12] L. Rakhmawati, W. Wirawan, and S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13640-019-0462-3.

[13] C.-F. Lee, J.-J. Shen, Z.-R. Chen, and S. Agrawal, "Self-embedding authentication watermarking with effective tampered lotcation detection and high-quality image recovery," *Sensors*, vol. 19, no. 10, May 2019, doi: 10.3390/s19102267.

[14] T. Huynh-The and S. Lee, "Color image watermarking using selective MSB-LSB embedding and 2D Otsu thresholding," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2017, pp. 1333–1338, doi: 10.1109/SMC.2017.8122798.

[15] D. Wang, X. Zhang, C. Yu, and Z. Tang, "Reversible data hiding in encrypted image based on multi-MSB embedding strategy," *Applied Sciences*, vol. 10, no. 6, Mar. 2020, doi: 10.3390/app10062058.

[16] A. Khurana and B. M. Mehta, "Comparison of LSB and MSB based image steganograph," *International Journal of Computer Science And Technology*, vol. 3, no. 3, pp. 870–871, 2012.

[17] S. Prasad and A. K. Pal, "A secure fragile watermarking scheme for Protecting integrity of digital images," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 44, no. 2, pp. 703–727, Jun. 2020, doi: 10.1007/s40998-019-00275-7.

[18] B. Bolourian Haghighi, A. H. Taherinia, and A. Harati, "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique," *Journal of Visual Communication and Image Representation*, vol. 50, pp. 49–64, Jan. 2018, doi: 10.1016/j.jvcir.2017.09.017.

[19] U. Asan and S. Ercan, "An introduction to self-organizing maps," in *Computational Intelligence Systems in Industrial Engineering*, 2012, pp. 295–315.

[20] M. Alia and K. Suwais, "Improved steganography scheme based on fractal set," *The International Arab Journal of Information Technology*, vol. 17, no. 1, pp. 128–136, Jan. 2020, doi: 10.34028/iajit/17/1/15.

[21] V. L. Reddy, "Novel chaos based steganography for images using matrix encoding and cat mapping techniques," *Information Security and Computer Fraud*, vol. 3, no. 1, pp. 8–14, 2015, doi: 10.12691/iscf-3-1-2.

[22] S. A. Mehdi, K. K. Jabbar, and F. H. Abbood, "Image encryption based on the novel 5d hyper-chaotic system via improved AES algorithm," *International Journal of Civil Engineering and Technology (IJCIET)*, vol. 9, no. 10, pp. 1841–1855, 2018.

[23] K. S. Rawat and D. S. Tomar, "Digital watermarking schemes for authorization against copying or piracy of color images," *Indian Journal of Computer Science and Engineering*, vol. 1, no. 4, pp. 295–300, 2010.

[24] F. Memon, M. A. Unar, and S. Memon, "Image quality assessment for performance evaluation of focus measure operators," *Mehran University Research Journal of Engineering and Technology*, vol. 34, no. 4, pp. 379–386, 2015.

[25] K. V. Thakur, O. H. Damodare, and A. M. Sapkal, "Identification of suited quality metrics for natural and medical images," *Signal & Image Processing: An International Journal*, vol. 7, no. 3, pp. 29–43, Jun. 2016, doi: 10.5121/sipij.2016.7303.

BIOGRAPHIES OF AUTHORS

Khalid Kadhim Jabbar Baghdad-Iraq, B.Sc. in Computer Science, Baghdad University, Baghdad, Iraq, 2001. HI-DUP in Data Security, ICCI, Baghdad, Iraq, 2002. M.Sc. in The Science of Software Engineering, ICCI, 2012. Asst. Pro. In Computer Science Department, Collage of Education, Mustansiriyah University. Scientific reviewer, Designated Reviewer, Editorial Board Member, and member of the Technical Program Committee in local and international journals (Scopus). My scientific interests include the majors of: information/ data security, image processing, chaotic system, steganography, AI, software engineering, digital watermarking, data structure, and digital forensic. He can be contacted at email: khalid_jabbar@yahoo.com, khalidk.jabbar@uomustansiriyah.edu.iq.

Munthir Bahir Tuieb Baghdad-Iraq, date of Birth 29\4\1987, BSc. In Software Engineering, Imam Ja'afar Al-Sadiq University, Baghdad-Iraq, 2009. MSc in Software Engineering Science, ICCI, Baghdad, Iraq, 2012. PhD in Computer Science, ICCI, Baghdad, Iraq, 2021. The major field of study is: Network and Communication, Driven and Maintenance and Information Security. He can be contacted at email: munthir87@yahoo.com.

Salam A. Thajeel received the BSc degree in computer science from Mustansiriyah University, Baghdad-Iraq, in 2000. His M.Sc. degree in computer science (pattern recognition) from Iraqi Commission for Computer and Informatics, Informatics Institute for Postgraduate studies, in 2003; and his Ph.D. degree in computer science (digital forensic) from University Technology Malaysia (UTM), Malaysia, in 2016. He is currently an assistant professor at University of Technology-Iraq. His research interest includes digital forensic, computer vision, multimedia information security. He can be contacted at email: sath72@gmail.com.