

# Evolutionary programming approach for securing medical images using genetic algorithm and standard deviation

Shihab A. Shawkat<sup>1,4</sup>, Najiba Tagougui<sup>2</sup>, Monji Kherallah<sup>3</sup>

<sup>1</sup>National School of Electronics and Telecommunications of Sfax, University of Sfax, Sfax, Tunisia

<sup>2</sup>Department of Computer Science Engineering, Higher Institute of Computer Science and Multimedia, University of Sfax, Sfax, Tunisia

<sup>3</sup>Department of Physics, Faculty of Science, University of Sfax, Sfax, Tunisia

<sup>4</sup>Department of Quality Assurance and Academic Performance, University of Samarra, Samarra, Iraq

## Article Info

### Article history:

Received Apr 1, 2023

Revised Jul 17, 2023

Accepted Jul 30, 2023

### Keywords:

Data hiding

Genetic algorithm

Information security

Mean square error

Medical image

Peak signal to noise ratio

Standard deviation

## ABSTRACT

The integrity and security of medical data have become a big challenge for healthcare services applications. Images of hidden text represent steganography forms in which the image is exploited as an object to cover information and data. So, the data masking ability and image quality of the cover object are significant elements in image masking. In this study, the patient's personal information and message generated by the doctor's comment are stored in the images. Image pixels and message bits are exchanged sequentially. The best cluster is randomly selected using the genetic algorithm (GA) and standard deviation (STD) methods. The method, depending on optimizing and taking benefits of the similarities between pixels, has been proposed. High image quality can be achieved by using stego-image and increasing the data amount to be hidden. Analysis metrics of visual quality such as peak signal to noise ratio (PSNR), mean square error (MSE), structural similarity index measure (SSIM) and bit error rate (BER) are adopted to assess the performance of the method proposed. The suggested and proposed model has proven its capability to mask the secret data of patients into a cover image transmitted with high ability, imperceptibility, and minimal future degradation.

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



## Corresponding Author:

Shihab A. Shawkat

National School of Electronics and Telecommunications of Sfax, University of Sfax

Sfax, Tunisia

Email: shahab84ahmed@gmail.com

## 1. INTRODUCTION

The modern era is going through a rapid technological evolution, and we are witnessing the production of a huge amount of information that can be worthily enhanced with appropriate management and analysis. This advancement in digital technology also raises certain concerns about the illicit access to and dissemination of multimedia information. The genetic algorithm (GA) has been introduced as a solution to these problems [1]. Therefore, we work to definitively represent the applications of GA in medical sciences, we note that the genetic algorithm finds its way in various fields of medical sciences such as image segmentation, personalized healthcare, and radiology, and discusses how to successfully apply the principle of the genetic algorithm in these applications. also try to have a comparative discussion of selected apps on different criteria. In general, inserting of hidden text causes degradation of image quality. This degradation is not visible to the human eye. Furthermore, the images are affected with distortions caused by active or passive attacks.

The hidden text procedure must be robust against all the attacks. According to the visibility, domain and permanency, data hiding procedures are classified in to different types. Medical information is the

prerequisite for any medical treatment nowadays. To obtain the optimal outcome for any diagnosis, several tests have been proposed in a manner that is cost and time effective and that preserves the confidentiality of diagnostic data [2]. Therefore, we work to definitively represent the applications of GA in medical sciences, we note that the genetic algorithm finds its way in various fields of medical sciences such as image segmentation, personalized healthcare, and radiology, and discusses how to successfully apply the principle of the genetic algorithm in these applications. also try to have a comparative discussion of selected apps on different criteria.

According to the findings of the literature review, information security is a key factor in determining the success or failure of future progress. There has been a significant growth in the number of information preservation techniques [3], due to the fast advancement of technology. However, security has also become a serious problem as a result of the increasing number of security risks. As a result of widespread digitization, huge amounts of data are transferred from one network to another. An attacker or intruder uses a variety of methods to monitor the network to obtain important information [4]. Now with the development of communication and information, information access has become easier, and establishing secure communication has become an essential requirement [5]. To ensure secure communication, different methods have been developed. Information steganography is one of the methods exploited in covering data. It is defined as a science or a technique that helps in transmitting information discreetly on a carrier of multimedia (audio, image, text, and video) [6].

Steganography represents a technique used for masking information and data into a cover object to create what is so-called a stego-image. The stego-image is sent by the sender to the recipient by a common object (medium). This prevents the outsiders (interlopers) from noticing the shrouded message in the image. The secret message in the image can be easily extracted with or without a stego-key by the recipient, with the help of an embedding algorithm. The concept of steganography of images is explained in Figure 1. The embedding algorithm requires a cover (image) with a secret (message) [7].

Data hiding aims at delivering data reliably from sender to receiver without any degradation, alteration, or any third-persons (hackers). Nowadays, steganography has changed the way we look at the development of technologies [8]. To prevent hackers or others from seeing or knowing the secret information is not the only purpose of steganography; it also tries to remove any suspicion about the hidden message or information. The information or the message represents credentials sent and disguised in the medium so that it is hard to detect. Any steganography has two main aspects, the ability to hide information and the inability to recognize hidden content [9]. However, these two characteristics confuse each other, as it is hard to raise the capacity while the steganography system is maintaining its imperceptibility. Besides, limited information cloaking methods are still there with protocols of data transmission communication. Such protocols can be unusual, yet, their future is promising [10].

A GA refers to a developmental and computational model influenced by the method of biological evolution. GA is usually used as a function enhancer. GA represents a model employs operators like recombination and selection to create new individuals in the search space, and to improve objective functions. Typically, a genetic algorithm includes two principal problem-based constituents the coding and evaluation functions. Some variables are optimized by either maximizing certain objectives or the error function [11]. Optimizing objective function is supposed to be a black box of a control dial series characterizing various criterion. The output of the black box refers to the extent to which the evaluation function returns on the optimization problem through a set of parameters. Standard deviation (STD) refers to image contrast change the bigger the value, the clearer the edge contour. To determine both the extreme value and the average value, it is advantageous to figure out the population STD. Calculating STD makes it simple to determine the frequency distribution. As the STD of AC increases, the image becomes more obvious [12].

The integrity and security of medical data have become a big challenge for healthcare services applications. Digital healthcare requires the process of transferring medical data, and has become a daily routine [13]. It provides an incorporated communication environment of interdependent platforms and devices by connecting both physical and virtual aspects. Thus, it is important to improve an efficient model to achieve the integrity and security of the transmission and reception of patients' diagnostic data [14]. This goal is achieved by employing algorithms of system encryption and techniques of steganography together to mask digital data in an image [15].

The proposed technique has important benefits where it requires no static cover image. Moreover, high quality and resolution are achieved in the pilot study conducted using texts and JPG images. With the basis of the integration of steganography technology and cryptography scheme for a high security system of healthcare, the technique aims at improving the security of transmitting medical data. The study is divided into five sections in addition to the current section. Section 2 explains the previous works related to the subject studied; section 3 illustrates the proposed and suggested model and the algorithms used; section 4 deals with the discussion of the results of the experimental findings. Finally, section 5 is concerned with the main conclusions.

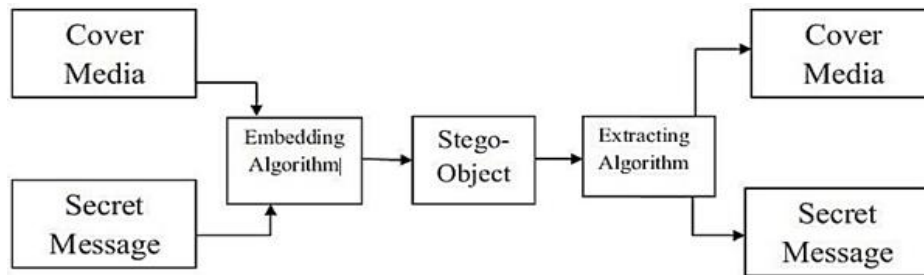


Figure 1. Conceptual diagram of embedding algorithm

## 2. RELATED WORKS

There are many uses for digital images, and sometimes they are used in some applications and important areas. Data should be safeguarded against unauthorized access, where the attackers should not be able attack throughout transmission. The outcomes of such works have, nonetheless, slightly improved. This section discusses a few of previous studies conducted by some authors. A very important research direction was introduced by Arsalan *et al.* [16]. It presented genetic programming (GP) depending on a reversible watermarking technique. To inset the optimum level of a watermark in the chosen pixels and to choose a domain of coefficients in integer wavelet transform, the researchers use GP in their technique. In its coefficients, the least significant bit (LSB) embeds watermarks. A trade off between imperceptibility and payload is gained by using the sub band category of wavelet coefficients and amplitude information. In this case, GP introduces GA, depending on the reversible integer wavelet transformed commanding technique. To obtain payload and a higher level of imperceptibility, GA is employed for the coefficient selection.

Anwar *et al.* [17] proposes an algorithm which depends on an artificial immune system and image segmentation. A block has been chosen following the algorithm proposed and after the cover medium (image) is segmented. Then, the artificial system of immune is used to cover the bits of the message in the best available place. In a domain of frequency, a data hiding approach is presented by employing a genetic algorithm. First, the cover medium (image) is mapped to a suitable domain with the use of a genetic algorithm and adaptive wavelet transform. The data and information to be covered are hidden and encrypted in frequency coefficients characterizing the edges of the image in the spatial domain. A hybrid model for securing data of the diagnosis text in medical images is suggested [18]. The model suggested is improved via integrating one of the following techniques: 2-D discrete wavelet transform 1 level (2D-DWT-1L) or 2-D discrete wavelet transform 2 level (2D-DWT-2L). However, either one is done with a proposed hybrid scheme of encryption. To start with, it encrypts the hidden data; then it conceals the output in a cover image. To conceal various sizes of text, images of both color and grayscale are employed as cover images.

Ahmadi and Sajedi [19] an approach which uses picture segmentation and a system of artificial immunity is suggested. According to the suggested approach, the system of artificial immunity is used to cover the bits of the message in the most suitable location. This is done after the cover picture has been split into blocks. The cover picture is firstly transferred to the proper frequency domain using a genetic algorithm and adaptive wavelet transform. Then, a method for concealing data in the frequency domain is described. The information is encoded and concealed in frequency coefficients that represent the spatial edges of the picture. Elhoseny *et al.* [20] presents a model of hybrid security as a suggestion for protecting the textual diagnostic information in medical pictures. The suggested model is made by combining a suggested strategy of hybrid encryption with one of the following steganography approaches: the 2D-DWT-1L or 2D-DWT-2L. First, the secret data is encrypted; after that, a cover picture is used to conceal the outcome. To hide various text sizes, cover graphics in both color and grayscale are employed.

Karakus and Avci [21] states that using stego-images and increasing the amount of data to be concealed are to guarantee high image quality by making use of pixels similarities. As a cover medium, medical images of different sizes are used. The doctor's comments on the situation of the patient are covered in medical images of 256×256 size without utilizing any technique of data compression. A robust and reversible framework of watermarking and a secure multiparty computation are used to achieve encrypted images [22]. To embed a watermark, the protected multi-party computation method is used where the scheme is not assessed for hybrid attacks and the system computational complexity is greater.

In the open environment, in Shawkat *et al.* [23] argues, the cloud infrastructure resources are shared via cloud computing on the internet. This maximizes the problems of security such as data integrity, confidentiality, and availability. Therefore, such problems can be solved by adopting data encryption, which is important to secure users' data. A comparative study is conducted between the two algorithms of security in

a cloud platform known as eyeOS. The study concludes that the algorithm of Rivest Shamir Adlemen (3kRSA) outperforms the algorithm of the triple data encryption standard (3DES) in terms of output bytes and complexity.

A fusion method for multimodal medical images is proposed in Arif and Wang [24] based on the curvelet transform. The GA method depends on the curvelet transform to solve the wavelet transform drawback in processing curvy forms and contours of objects that often appear in medical images. Any diffuses and suspicions existing in the input image can be solved by the method, which can further improve the characteristics of image fusion. The method proposed has been verified and tested in various places of medical pictures. Also, it is compared with new techniques of medical image fusion.

### 3. THE PROPOSED MODEL

This method ensures that the ciphertext and the stego-image (image after embedding) maintain the highest level of image authenticity and quality. By utilizing the potent qualities of crossover and mutation GA operations, the suggested approach employs a GA twice, for producing an approach for encoding the text and picking the optimum region to mask. STD for each section is then finding value of a standard deviation, (i.e., be adopted as locations to hide) and that by including all bit of message. The algorithm was applied to more than one image, where the standard deviation value is measured, as the lower the dispersion value of the image data, which indicates better results, as the peak signal to noise ratio (PSNR) value was high, which indicates that there is no visible change in the image after masking compared to the cover image. On the basis of the GA and STD, a novel scheme of text encryption and embedding is suggested to maintain the security of medical image files. On a few random texts and well-known images, the encoding technique suggested in this paper is tested, and promising results are noted.

#### 3.1. Encryption and embedding text

The GA is used, in the process of optimization, to optimize (1). To find the value of (1), let's suppose the count of 0s is shown by  $x$  and the count of 1s is by  $y$ . Besides, we have  $n$  which shows a threshold value. Next,  $f_1$ ,  $f_2$  and  $f_3$  are calculated and are added as in (1) to conclude the objective function of the key of the input. Thus, the value of 1 s and 0 s in the key is calculated and that of  $f_1$  is returned to either one in the condition of equality and zero in inequality. Whereas, the second function begins when the significance of  $n$  is entered. It refers to the required value of block units, where  $n = 8$ . The value of  $n$  in the key string is searched for and the value is returned to either one in the case of a size block  $n$  or zero in the absence of a block of size  $n$ . Besides, it is returned to either one in the case of a measure gap  $n - 1$  or zero in the absence of the presence of a gap of measure  $n - 1$ .

The GA main section is the fitness function, and it is used to evaluate whether a member is useful or not. A new fitness function, in this study, is presented for GA. It can maximize the true positive rate and lessen the rate of error in choosing useful features. In various images such as medical images, the represented features of the image are only the ones used to make better and more accurate detection. Thus, it is important to extract suitable features of the image rate in addition to improving quality. They are used:

$$f(x) = \sum_{i=1}^m f_i, m = 1,2,3 \quad (1)$$

$$f_1 = f(x) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases} \quad (2)$$

$$f_2 = f(x) = \begin{cases} 1, & x \geq n \\ 0, & x < n \end{cases} \quad (3)$$

$$f_3 = f(x) = \begin{cases} 1, & y \geq n - 1 \\ 0, & otherwise \end{cases} \quad (4)$$

Here, to create a stronger key other than the one resulted from the previous process, evolutionary optimization is applied. The same standards followed in the previous step are used here in the process of development in (4) as an objective function. Anyhow, it is conducted iteratively. Four new arbitrary solutions are generated at the beginning of this process. Thus, they represent the solutions of the population, (4). Using (4), each one of the four proposed solutions is simultaneously evaluated till we find the best or better solutions after some generations. The process of optimization continues till sufficient merit of the fitness function is achieved for any of these candidate solutions. During the successive generations, it is expected that the solutions that have high ranks will be exploited for the encryption of the message.

Figure 2 shows the key generation process with the use of GA in encryption. Firstly, the length of the key must be identified to determine the working parameters of the GA before starting the process of optimization. The proposed GA parameters are as:

- Generations: determined by reaching the best solution according to the fitness function
- Initial population: 4
- Selection: roulette-wheel
- Crossover: one-cut point crossover
- Mutation: uniform with 0.001 probability [25]

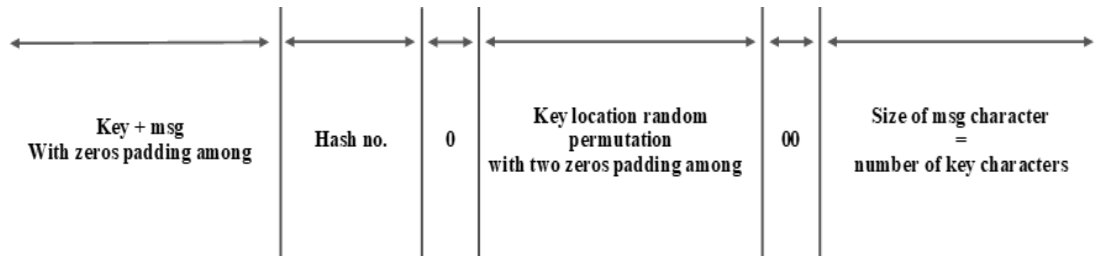


Figure 2. Encrypted message frame

The plain or data text will be transformed into a certain format of image as an outcome of this action. The text to be encrypted will be hidden in that image. To view the text by the receiver, the image must be segmented first into blocks. The concealed key will be exploited to make some adjustments to each color component. Hackers will face a big problem in breaking the encryption and stealing the information will be impossible. Figure 3 explains the general framework for concealing the secret data by the proposed systems. These figures represent the main steps performed on both sides by the sender and receiver.

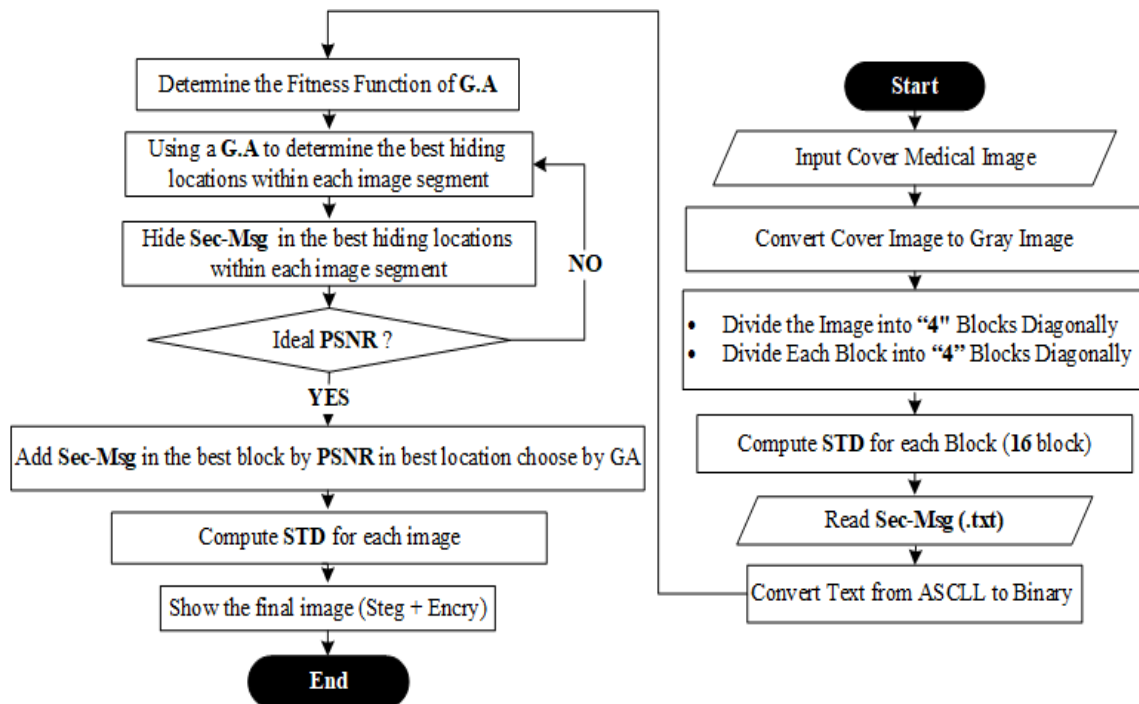


Figure 3. Embedding the secret data into the source image

### 3.2. Extraction and decryption text

The encoded image will be loaded onto the ciphertext along with the underlying in-formation for that text. The image will then be converted to a grayscale image to facilitate further processing of the image. This is to extract sensitive information en-coded within the image. It is more efficient than using the native RGB image format. While, the grayscale image contains less information than the RGB image. Thus, this transformation is a

way to extract features that only relate to valuable information about the encrypted data. In the context of our proposed method, the decoding process represents the extracting operation of the original message. The decoding first starts by splitting the 1-D element matrix frame and retrieving the final element representing the message length. Next, the location of the key is extracted with two of the removing the appended zeros. After that, all the added zeros of the hidden information are deleted. Here, the location of the message must be discovered by the extraction of the key and the secret information via its location. Eventually, it can be extracted by the frame hash number. To transform the binary array of the key of the information to decimal numbers is so important.

Later, the image is passed to another major step, which is the process of dividing only the image specific parts, where the secret message or information is stored. This image is then parsed into two components. The image index is the typical block identifier, where the hidden text fragments will be extracted. At this moment, the information required for the hidden text is returned and the cover image from which the text is extracted is compared with the original image, so that we can evaluate the image accuracy. The method proposed is subject to standard evaluation measures in the field to avoid possible attacks on the ciphertext. Figure 4 shows the mechanism for extracting the text from the cover image using the proposed method.

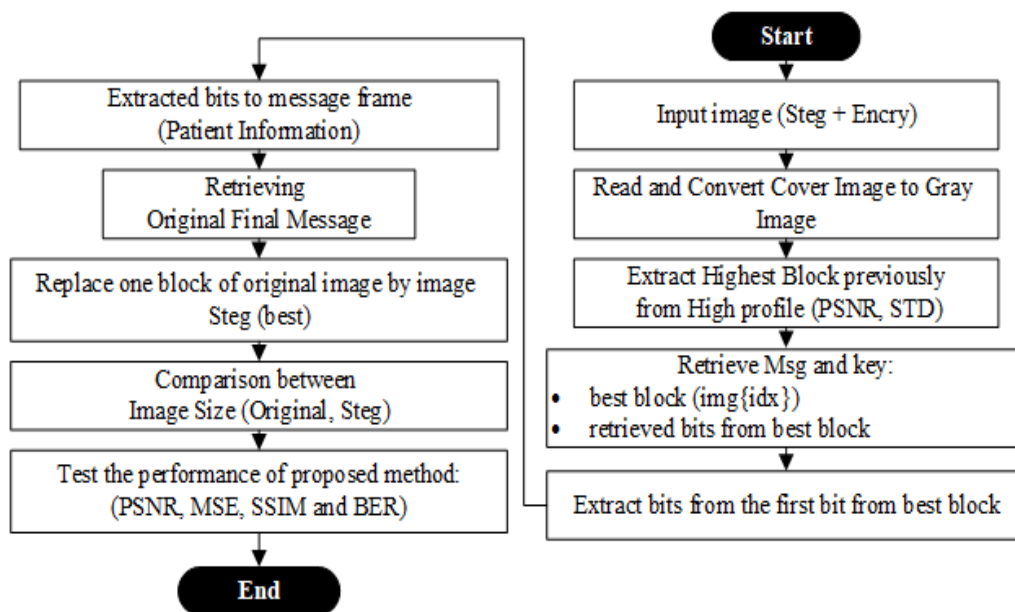


Figure 4. Extraction the secret data into the source image

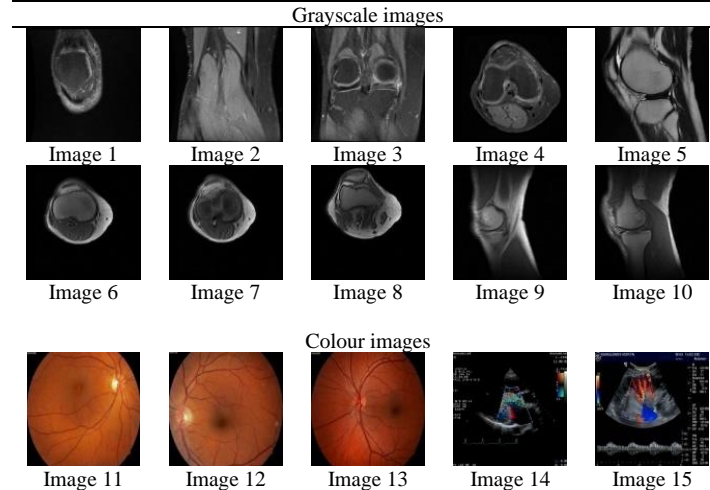
## 4. EVALUATION OF THE PROPOSED METHOD

### 4.1. Dataset and used parameters

The illegal obtaining or changing the personal data of the patient may result in the violation of the patient's personal rights and change the course of the treatment process. The way patients' personal information and data are stored and transferred must be preserved because they are vulnerable to illegal appropriation or violation. This may cause harm to the patients. In this study, been used cover objects, 15 images of (512×512) size type of computed tomography (CT) and magnetic resonance (MR), chosen randomly from the library of digital imaging and communications in medicine (DICOM) [26]. The integrity and security of medical data have become a big chthe patient's personal information and message generated by the doctor's comment are stored in the images. Our aim with this work to mask the secreta data of patients into a cover image transmitted with high ability, imperceptibility and in order to get new dataset (grayscale and colour) images of chosen randomly (15 images), The used images of the test are as shown in Table 1. It shows the gray and color datasets versions.

Our suggested model is implemented with MATLAB R2021b software operating on a PC with 8 GB of RAM, a 2.27 GHz Intel® Core™ i5 CPU, and Windows 10. The computation of selected statistical values specifies the proposed-model quality of security. These scales compute the comparison between the stego-image and the original image (cover). The achieved results will be assessed on images of both color and grayscale with various text sizes. Here, the evaluation of performance depends on four statistical parameters structural similarity index measure (SSIM), mean square error (MSE), peak signal to noise ratio (PSNR), and bit error rate (BER) [27].

Table 1. Test images with color and grayscale formatting of the dataset (15 Images)



#### 4.1.1. PSNR

PSNR is typically employed to calculate the proportion between the maximum potential power of signs and the power of corrupting distortion that influences image accuracy. Mainly, the ratio is used to differentiate between the quality of a stego-image containing hidden data to that of an empty cover image. In (5) is used to determine the PSNR value.

$$PSNR = 10 \log(\max(I_{mn}^2)/MSE) \quad (5)$$

#### 4.1.2. MSE

MSE is simply the average squared disparity between a cover image and a stego-image. A lower MSE value means fewer variations between both images. In (6) is used to determine the MSE value.

$$MSE = \frac{1}{MN} \times \sum_{m,n} (I_{1mn} - I_{2mn})^2 \quad (6)$$

#### 4.1.3. SSIM

It is an index that gauges how structurally similar two images are. Its range of values is from -1 to 1. The SSIM of two almost similar photographs is close to 1. As a result, it is employed as a technique for determining how similar two images are. To calculate the SSIM between (1) and (2) at a certain pixel  $P$ . The SSIM value is calculated using the in (7).

$$SSIM = \frac{2 \times \mu_1(p) \mu_2(p) + c_1}{\mu_1(p)^2 + \mu_2(p)^2 + c_1} \times \frac{2 \times cov(p) + c_2}{s_1(p)^2 + s_2(p)^2 + c_2} \quad (7)$$

#### 4.1.4. BER

The number of errors made concerning the total sum of signals sent is known as BER. The performance of the system improves when the percentage of errors decreases and vice versa. Multiple disturbances during transmission have an impact on the signal, and this could be immediately translated into the number of errors in a string of a transmitted number of bits. With the use of (8), the definition regarding BER could be reduced to the following straightforward formula.

$$BER = \text{number of bit errors} / \text{number of bit transferred} \quad (8)$$

## 4.2. Experimental results

The technique presented in the section 3 was put to use in analysis metrics of used visual quality, where creating a simulation environment is essential to validate the performance of the proposed algorithms. In this study, the patient's personal information and message generated by the doctor's comment are stored in the images. The GA is used twice, in text encryption and in choosing the ideal block for hiding. Also, the STD chooses the ideal block for hiding. Whereas, working on the main goal of obfuscating images is to preserve the privacy of the contents of the image, which is highly desirable in the privacy request. It specifies the match index of the original block (before hiding) to the selected best block. Image pixels and message bits are

exchanged sequentially. The best cluster is randomly selected using the GA and STD methods. The method, depending on optimizing and taking benefits of the similarities between pixels, has been proposed. High image quality can be achieved by using stego-image and increasing the data amount to be hidden. Analysis metrics of visual quality such as PSNR, MSE, SSIM, and BER are adopted to assess the performance of the method proposed. Figure 5(a), and Figure 5(b) shows the algorithm’s operation and experimental implementation.

Experimental results of the three proposed techniques are presented with the images from various sources utilized for evaluating our suggested techniques. With both conventional and medical images, we use the recommended method. Thus, we observe the performance of the proposed smart technologies. The similarity-based method proposed by Elhoseny *et al.* [20], which saves the diagnosis text data in a medical image using a hybrid security paradigm. The suggested methodology encrypts sensitive data first, then conceals the outcome in a cover image. To conceal the various text sizes, a color image is utilized as cover images (128,256) bytes. It is different from the one that proposed by Karakus and Avci [21], Anand and Singh [28]. The method we proposed is of different capacities of texts, (1000 characters between 142 words and 250) and (5000 characters between 714 and 1250 words). It uses words to mask the secrete data in medical images. The model proposed demonstrates its efficiency to mask the confidential data of the patient in the cover image sent with high non-perceiving ability, amplitude, and minimal degradation in the received groove image. The comparison results are shown in Table 2, Table 3, Table 4, and Table 5.

Table 2 shows the comparative performance of the outcomes of the four obtained statistical parameters after applying the suggested technique with Elhoseny *et al.* [20] on color images for (128,256) bytes. In these cases, the results are quite close to each other. The data are concealed, and efficient outcomes are obtained.

The suggested approach offers greater flexibility than the existing schemes, when the new system is compared to several well-known contemporary designs. As previously mentioned, evaluation criteria like SSIM, MSE, PSNR, and BER are exploited to assess the optical robustness and efficiency of the suggested technology. The highest PSNR of the scheme proposed is found in comparative studies, where no attack is louder than 75.7678 dB in Table 3, 68.6890 dB in Table 4, and 70.3197 in Table 5. The greatest MSE values are closer to one and are 0.0012331 and 0.0042543 in Table 3 and Table 4. The SSIM merits are nearer to one, as shown in the tables, ensuring that the proposed framework is not perceived.

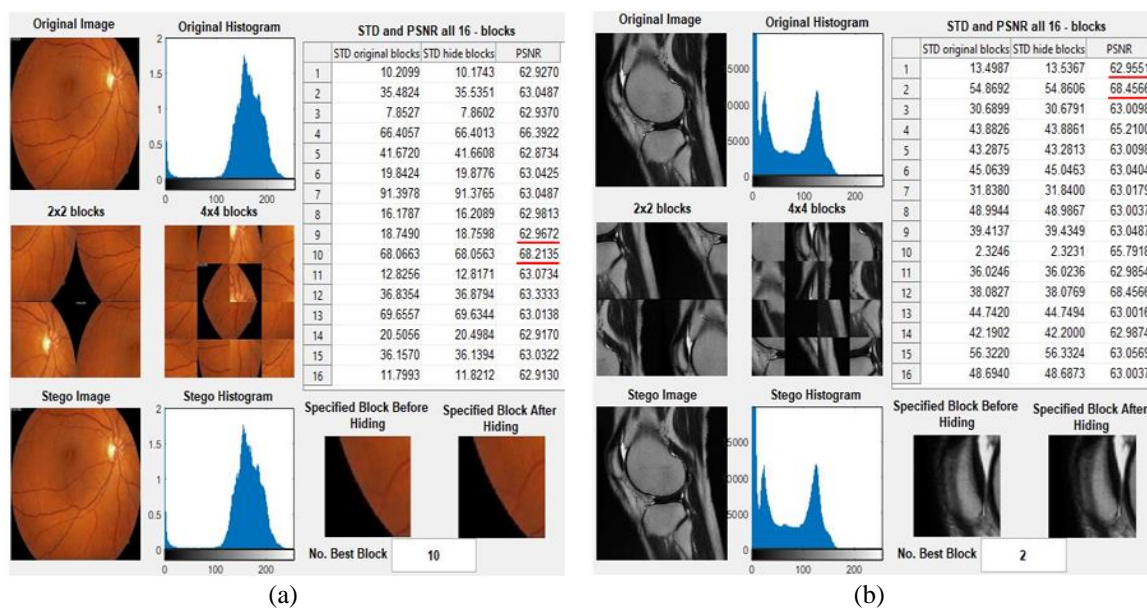


Figure 5. Comparisons between the previous and posterior predictors visually (before hiding) the best-chosen block’s matching index in dataset (a) color images and (b) grayscale images

Table 6 will show how the proposed technique compares in terms of speed while encrypting and decrypting color pictures (Lena image size: 512×512). Our suggested approach exhibits rather acceptable efficiency when compared to algorithms for similar environments, despite the fact that the prior environments were different. It demonstrates that because of how quickly it can encrypt and decrypt data, the technique we’ve shown is recommended for real-time applications.



An important element in picture steganography is the quality of the image and data concealing capabilities. The primary merit of the technique suggested is that it requires no static cover image and high resolution. Quality is achieved using texts and images. An advantage of this method is that the output file (image) must be the same as the result of the included input file (image). Table 7 shows the images used before and after embedding. It is noted that the size of the images is fixed and there has been no change. So, the proposed model demonstrates its capacity to transmit a cover image containing sensitive patient information while maintaining high levels of imperceptibility, capacity, and stability of the received stego-image.

Table 2. Comparative performance of results of four parameters obtained from an implementation of proposed method on color images for (128,256) bytes

Test images	Elhoseny <i>et al.</i> [20]				Proposed algorithm			
	PSNR	MSE	SSIM	BER	PSNR	MSE	SSIM	BER
Image11	50.70	0.55	1	0	74.347	0.0016	1	0
	51.66	0.44	1	0	71.312	0.0027	1	0
Image12	50.65	0.56	1	0	73.896	0.0018	1	0
	51.60	0.45	1	0	71.095	0.0026	1	0
Image13	50.59	0.57	1	0	74.345	0.0015	1	0
	51.49	0.46	1	0	71.090	0.0026	1	0
Image14	51.79	0.48	1	0	75.630	0.0017	1	0
	51.27	0.43	1	0	73.190	0.0031	1	0
Image15	52.66	0.49	1	0	71.059	0.0020	1	0
	50.58	0.41	1	0	68.650	0.0032	1	0

Table 3. Comparative performance of results of three parameters obtained from an implementation of method on grayscale images for (1000-character) [21]

Test images	Karakus and Avci E [21]			Proposed algorithm		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Image1	66.5574	0.014366	0.154574	75.7678	0.0017237	0.99993
Image2	66.5047	0.014542	0.153886	75.7675	0.0017233	0.99993
Image3	66.5413	0.014420	0.153906	75.7672	0.0017233	0.99993
Image4	66.5298	0.014458	0.154413	75.6673	0.0017243	0.99993
Image5	66.5344	0.014442	0.153924	75.6572	0.0017223	0.99993
Image6	60.4693	0.058365	0.154820	75.3636	0.0016909	0.99992
Image7	60.4772	0.058258	0.154926	75.3157	0.0016851	0.99992
Image8	60.5299	0.057556	0.154799	74.2425	0.0016127	0.99989
Image9	60.4286	0.058914	0.154232	72.3697	0.0012331	0.99984
Image10	60.4230	0.058990	0.154302	72.5287	0.0013180	0.99981

Table 4. Comparative performance of results of three parameters obtained from an implementation of method on grayscale images for (5000-characters) [21]

Test images	Karakus and Avci [21]			Proposed algorithm		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Image1	59.4460	0.073872	0.154572	68.6890	0.0058575	0.99960
Image2	59.4159	0.074387	0.153885	68.6459	0.0058422	0.99961
Image3	59.3950	0.074745	0.153904	67.2091	0.0050306	0.99970
Image4	59.4676	0.073505	0.154411	67.2468	0.0050936	0.99948
Image5	59.3784	0.075031	0.153924	67.3307	0.0051041	0.99927
Image6	53.3657	0.299576	0.154817	66.9320	0.0046463	0.99935
Image7	53.3799	0.298599	0.154922	66.7789	0.0045509	0.99935
Image8	53.3646	0.299652	0.154795	66.4851	0.0044260	0.99963
Image9	53.3637	0.299713	0.154229	66.3615	0.0043602	0.99968
Image10	53.3483	0.300781	0.154298	66.2848	0.0042543	0.99973

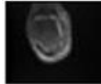


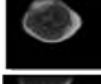

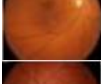



Table 5. Comparative performance of results of three parameters obtained from an implementation of method on grayscale images for (5000 characters) [28]

Test images	Anand and Singh [28]		Proposed algorithm	
	PSNR	SSIM	PSNR	SSIM
Image1	59.4460	0.154572	65.5639	0.99984
Image2	59.4159	0.153885	68.6506	0.99954
Image3	59.3950	0.153904	68.0977	0.99964
Image4	59.4676	0.154411	70.1197	0.99973
Image5	59.3784	0.153924	70.3197	0.99977

Table 2. As compared to other methods for execution time (in seconds)

Methods	Encryption time	Decryption time	Experiment environment
Xiong <i>et al.</i> [29]	20.915818	18.802360	1.90 GHz CPU, 4.0 G RAM
Li <i>et al.</i> [30]	0.3239	–	2.4 GHz CPU, 2.0 G RAM
Xuejing and Zihui. [31]	9.0016	9.1095	2.7 GHz CPU, 8.0 G RAM
Teng <i>et al.</i> [32]	1.769703	0.837978	2.30 GHz CPU, 4.0 G RAM
Proposed algorithm	0.1656	0.1341	2.7 GHz CPU, 8.0 G RAM

Table 3. Size of the images used before and after embedding (1000-5000) character data hiding

No.	Image before embedding (original)	Image after embedding (stego)
1	 <b>image original.jpg</b> JPG File 44.5 KB	 <b>image stegano.jpg</b> JPG File 44.5 KB
2	 <b>image original.jpg</b> JPG File 67.2 KB	 <b>image stegano.jpg</b> JPG File 67.2 KB
3	 <b>image original.jpg</b> JPG File 65.0 KB	 <b>image stegano.jpg</b> JPG File 65.0 KB
4	 <b>image original.jpg</b> JPG File 29.4 KB	 <b>image stegano.jpg</b> JPG File 29.4 KB
5	 <b>image original.jpg</b> JPG File 32.0 KB	 <b>image stegano.jpg</b> JPG File 32.0 KB
6	 <b>image original.JPG</b> JPG File 50.0 KB	 <b>image stegano.JPG</b> JPG File 50.0 KB
7	 <b>image original.JPG</b> JPG File 47.5 KB	 <b>image stegano.JPG</b> JPG File 47.5 KB
8	 <b>image original.JPG</b> JPG File 50.4 KB	 <b>image stegano.JPG</b> JPG File 50.4 KB

## 5. CONCLUSION

The security and integrity of medical data has become a major challenge for healthcare services applications. It is challenging to find out the color component in the cover image for embedding in order to meet research objectives and withstand different kind of attacks. So, the main challenge faced while implementing secure, robust and imperceptible technique is combining cryptography and hidden text. Any illegal user is easily able to access important data and change their original owners in the current Internet domination scenario. As compared to others, our proposed and suggested technique outperforms many security models of recent techniques in protecting diagnosis data in terms of imperceptibility and robustness. This is done to improve the embedding steganography and obtain high similarity between the cover image and the secret bit stream in a medical image with text. A robust GA and STD based scheme have been developed that provide better noncognition and potency. Investigations into the effectiveness of our plan for various image-processing activities reveals that the suggested method is resilient to simultaneous assaults. The suggested model is created to make sure that the stego-image (image after embedding) keeps as much of its original quality and distinctiveness as possible. In order to test the performance of the proposed method, visual quality analysis metrics such as PSNR, MSE, SSIM and BER have been used. Proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal degradation. The results show that the recommended strategy yields the best results in terms of nonvisual perception and solves the problems of classification confusion and improves the quality of the image. In future, although, we believe that the research and contributions conducted in this paper are essential. It is possible to rely on other intelligent techniques to generate the key, such as the use of neural networks. In addition to the possibility of integrating more than one encryption algorithm and benefiting from the GA by generating the key to it, and the use of the well-known camouflaging function that achieves the required specifications. With encrypting images of various sorts and sizes, making it suitable for dependable and feasible cryptographic usage.

## ACKNOWLEDGEMENTS

The authors would like to thank National School of Electronics and Telecommunications of Sfax (www.enetcom.rnu.tn) Sfax-Tunisia and University of Samarra (www.uosamarra.edu.iq) Samarra-Iraq for its support in the present work.




## REFERENCES

- [1] T. M. Deserno, "Fundamentals of Biomedical Image Processing," *Biomedical Image Processing*, Berlin, Heidelberg: Springer, 2010, pp. 1–51, doi: 10.1007/978-3-642-15816-2\_1.
- [2] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities, A Guide to Detection and Prevention*, Apress Access Books, 2016, doi: 10.1007/978-1-4842-2155-6.
- [3] E. Oztemel and S. Gursev, "Literature review of Industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, vol. 31, pp. 127–182, 2020, doi: 10.1007/s10845-018-1433-8.
- [4] A. Sestino, M. I. Prete, L. Piper, and G. Guido, "Internet of Things and Big Data as enablers for business digitalization strategies," *Technovation*, vol. 98, 2020, doi: 10.1016/j.technovation.2020.102173.
- [5] G. Aceto, V. Persico, and A. Pescapé, "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges," *Journal of Network and Computer Applications*, vol. 107, pp. 125–154, 2018, doi: 10.1016/j.jnca.2018.02.008.
- [6] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, vol. 80, pp. 21165–21202, 2021, doi: 10.1007/s11042-021-10723-4.
- [7] G. V. K. Murugan and R. U. Subramaniam, "Performance analysis of image steganography using wavelet transform for safe and secured transaction," *Multimedia Tools and Applications*, vol. 79, pp. 9101–9115, 2020, doi: 10.1007/s11042-019-7507-6.
- [8] H. M. Taher, S. Q. A. Al-Rahman, and S. A. Shawkat, "Best S-box amongst differently sized S-boxes based on the avalanche effect in the advance encryption standard algorithm," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6535-6544, 2022, doi: 10.11591/ijece.v12i6.pp6535-6544.
- [9] R. Pavaiyarkarasi, R. Ramu, G. Sahaana, L. Saravanan, R. B. Begam, and R. T. Prabu, "A Hybrid Security Model for the Protection of Diagnostic Text Data in Medical Images over Internet of Things," *2022 Sixth International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*, 2022, pp. 196-203, doi: 10.1109/I-SMAC55078.2022.9987292.
- [10] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, 2023, doi: 10.1016/j.sigpro.2022.108908.
- [11] K. Höschel and V. Lakshminarayanan, "Genetic algorithms for lens design: a review," *Journal of Optics*, vol. 48, pp. 134–144, 2019, doi: 10.1007/s12596-018-0497-3.
- [12] T. Akbarpour, M. Shamsi, S. Daneshvar, and M. Pooreisa, "Medical image fusion based on nonsubsampling shearlet transform and principal component averaging," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 17, no. 04, 2019, doi: 10.1142/s0219691319500231.
- [13] A. K. Sahu and A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," *Multimedia Tools and Applications*, vol. 81, pp. 30663–30683, 2022, doi: 10.1007/s11042-022-13015-7.
- [14] C. Wang and Z. Lu, "Cyber Deception: Overview and the Road Ahead," in *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80-85, 2018, doi: 10.1109/MSP.2018.1870866.
- [15] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in *IEEE Access*, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
- [16] M. Arsalan, S. A. Malik, and A. Khan, "Intelligent threshold selection for reversible watermarking of medical images," *Proceedings of the 12th annual conference companion on Genetic and evolutionary computation*, 2010, pp. 1909–1914, doi: 10.1145/1830761.1830825.
- [17] A. S. Anwar, K. K. A. Ghany, and H. ElMahdy, "Human ear recognition using SIFT features," *2015 Third World Conference on Complex Systems (WCCS)*, 2015, pp. 1-6, doi: 10.1109/ICoCS.2015.7483254.
- [18] K. Karaman and İ. Akgül, "Web based values education application for primary school students," (in Turkish language), *Uşak Üniversitesi Sosyal Bilimler Dergisi*, vol. 8, no. 3, 2015. [Online]. Available: <https://dergipark.org.tr/tr/download/article-file/202550>
- [19] S. D. Ahmadi and H. Sajedi, "Image steganography with Artificial Immune System," *2017 Artificial Intelligence and Robotics (IRANOPEN)*, 2017, pp. 45-50, doi: 10.1109/RIOS.2017.7956442.
- [20] M. Elhoseny, G. R. -González, O. M. A. -Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in *IEEE Access*, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615.
- [21] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," *Medical Hypotheses*, vol. 139, 2020, doi: 10.1016/j.mehy.2020.109691.
- [22] H. Zhang, Z. Li, X. Liu, C. Wang, and X. Wang, "Robust image watermarking algorithm based on QWT and QSVD using 2D Chebyshev-Logistic map," *Journal of the Franklin Institute*, vol. 359, no. 2, pp. 1755–1781, 2022, doi: 10.1016/j.jfranklin.2021.11.027.
- [23] S. A. Shawkat, B. A. Tuama, and I. Al-Barazanchi, "Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adleman," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6496-6505, 2022, doi: 10.11591/ijece.v12i6.pp6496-6505.
- [24] M. Arif and G. Wang, "Fast curvelet transform through genetic algorithm for multimodal medical image fusion," *Soft Computing*, vol. 24, pp. 1815–1836, 2020, doi: 10.1007/s00500-019-04011-5.
- [25] S. A. Shawkat, N. Tagougui, and M. Kherallah, "Optimization-based pseudo random key generation for fast encryption scheme," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 1007–1018, 2023, doi: 10.11591/eei.v12i2.4953.
- [26] "DICOM Tags." DICOM Library-Anonymize, Share, View DICOM Files. [Online]. Available: <https://www.dicomlibrary.com/dicom/dicom-tags/> (accessed Jan. 28, 2023).
- [27] S. A. Shawkat and I. Al-Barazanchi, "A proposed model for text and image encryption using different techniques," *TELKOMNIKA*, vol. 20, no. 4, pp. 858-866, 2022, doi: 10.12928/telkomnika.v20i4.23367.
- [28] A. Anand and A. K. Singh, "SDH: Secure Data Hiding in Fused Medical Image for Smart Healthcare," in *IEEE Transactions on Computational Social Systems*, vol. 9, no. 4, pp. 1265-1273, 2022, doi: 10.1109/TCSS.2021.3125025.




- [29] Z. Xiong, Y. Wu, C. Ye, X. Zhang, and F. Xu, "Color image chaos encryption algorithm combining CRC and nine palace map," *Multimedia Tools and Applications*, vol. 78, pp. 31035–31055, 2019, doi: 10.1007/s11042-018-7081-3.
- [30] Z. Li, C. Peng, W. Tan, and L. Li, "A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation," *Symmetry*, vol. 12, no. 9, 2020, doi: 10.3390/sym12091497.
- [31] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, 2020, doi: 10.1016/j.image.2019.115670.
- [32] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dynamics*, vol. 105, pp. 1859–1876, 2021, doi: 10.1007/s11071-021-06663-1.

## BIOGRAPHIES OF AUTHORS






**Shihab A. Shawkat**    received the B.Sc. degree in Computer Science from University of Tikrit in 2007 and M.Sc. Degree in Computer Science from Mansoura University in 2017, Currently a Ph.D. student in National School of Electronics and Telecommunications of Sfax, University of Sfax, Sfax, Tunisia. He worked as a teacher during the period from 2008 to 2019 in Directorate of Education in Salah Al-Din, Ministry of Education, Iraq. He has recently started working at the University of Samarra at the end of 2019 till now. His research interest lies in computer science, information security, image processing, and AI. He can be contacted at email: shahab84ahmed@gmail.com.



**Najiba Tagougui**    is actually Assistant Professor at the Higher Institute of Computer Sciences and Multimedia of Sfax, Sfax University Tunisia from where she graduated in Computer Sciences in 2005. She obtained a master degree in News technologies of dedicated computer systems in 2007 and a Ph.D. in Computer Systems Engineering in 2014 at the National Engineering School of Sfax. Her research interest includes applications of intelligent methods to pattern recognition. She focuses her research on intelligent pattern recognition, especially online handwriting recognition and image caption generation. She can be contacted at email: najiba.tagougui@isims.usf.tn.



**Monji Kherallah**    received the Ing. Diploma degree, the Ph.D. and HU in electrical engineering, respectively in 1989, 2008 and 2012, from University of Sfax (ENIS). Now he is an associate professor in Faculty of Science of Sfax and member in Research Group of Intelligent Machines: REGIM-Lab. His research interest includes the handwritten documents analysis and recognition. The techniques used are based on intelligent methods, such as neural network, logic fuzzy, and genetic algorithm. He is one of the developers of the ADAB-Database (used by more than 50 research groups from more than 10 countries). He is co-organizer of the online Arabic handwriting recognition competitions at ICDAR 2009 and ICDAR 2011. He has more than 70 papers and book chapters. He is a member of IEEE and IEEE AESS Tunisia. He can be contacted at email: monji.kherallah@fss.usf.tn.