Nonlinear Dyn (2021) 105:2677–2692
https://doi.org/10.1007/s11071-021-06700-z

ORIGINAL PAPER

Steganography-based voice hiding in medical images of COVID-19 patients

Melih Yildirim

Received: 12 April 2021 / Accepted: 2 July 2021 / Published online: 22 July 2021

Abstract A novel image steganography technique in order to hide the ciphered voice data has been suggested in this work. The doctor's voice comments belonging to a coronavirus disease 2019 (COVID-19) patient are hidden in a medical image in order to protect the patient information. The introduced steganography technique is based on chaos theory. Firstly, the voice comments of the doctor are converted to an image and secondly, they are ciphered utilizing the suggested encryption algorithm based on a chaotic system. Then, they are embedded into the cover medical image. A lung angiography dual-energy computed tomography (CT) scan of a COVID-19 patient is used as a cover object. Numerical and security analyses of steganography method have been performed in MATLAB environment. The similarity metrics are calculated for R, G, B components of cover image and stego image as visual quality analysis metrics to examine the performance of the introduced steganography procedure. For a 512×512 pixel cover image, SSIM values are obtained as 0.8337, 0.7926, and 0.9273 for R, G, B components, respectively. Moreover, security analyses which are differential attack, histogram, information entropy, correlation of neighboring pixels and the initial condition sensitivity are carried out. The information entropy is calculated as 7.9993 bits utilizing the suggested steganography scheme. The mean value of the ten UACI and NPCR values are obtained as 33.5688% and 99.8069%, respectively. The results of security analysis have revealed that the presented steganography procedure is able to resist statistical attacks and the chaotic system-based steganography scheme shows the characteristics of the sensitive dependence on the initial condition and the secret key. The proposed steganography method which is based on a chaotic system has superior performance in terms of being robust against differential attack and hiding encrypted voice comments of the doctor. Moreover, the introduced algorithm is also resistant against exhaustive, known plaintext, and chosen plaintext attacks.

Keywords COVID-19 · Steganography · Cryptography · Chaos · Voice hiding · Differential attack · Statistical attacks

1 Introduction

Data security has become a mandatory requirement with ever increasing in the number of internet users for delivering data [1]. Numerous software-based encryption techniques such as DES [2] and RSA [3] can be employed in order to transmit the data and information

M. Yildirim (✉)
The Scientific and Technological Research Council of Turkey (TUBITAK), Ankara, Turkey
e-mail: melih.yildirim@tubitak.gov.tr

in shared channels in a secure way. Optical methods are also used to encrypt images so that original images are not able to be retrieved without keys [4, 5]. The essential objective of the data hiding is to transfer the secret data safely from the transmitter to receiver. One of the methods which is used to ensure a safe data transmission is steganography [6]. Steganography is a technique that provides data and information to be transferred safely on a carrier such as video, audio, text and image [7, 8]. The word steganography is obtained using Greek words steganos and graphie, and it means concealed writing. Cryptography is the art of encrypting data and information and making them hard to understand. In cryptography, the secret message is in scrambled form or encrypted form which is not understandable but the existence of the secret message is visible to everyone unlike steganography. On the other hand, unlike cryptography, in steganography after data hiding, the secret information is not even visible to the eavesdropper or the intruder which causes this method safer and secure to follow [8].

Steganography technique includes components such as cover object, secret data, and stego object. Cover object is utilized as an environment to hide the data. Secret data are hidden as a message in the cover object. After hiding the secret data in the cover object, stego object is obtained. The type of steganography is named according to the medium used as a cover object. When the cover object is an image, it is named image steganography. In a similar way, the technique is named text steganography, video steganography, and sound steganography with respect to the type of media utilized as a cover object [6]. In the introduced study, a lung CT scan is utilized as a cover object. However, the proposed steganography method for voice hiding can be performed in different types of medical images.

Numerous studies based on information and data encryption have been carried out [9–22]. Some of these studies have suggested encryption techniques using chaotic system [9, 12, 13, 16–19, 21, 22]. Apart from encryption methods, steganography-based methods have also been proposed in order to hide the digital information and data [1, 6, 23]. Karakus and Avci [6] have proposed an image steganography method in order to hide doctor's comments into medical image. The comments of the doctor in different capacities such as 1000, 5000 and 10,000 characters are hidden in cover image by applying genetic algorithm–optimum pixel similarity (GA-OPS) technique. They have succeeded to increase the amount of data to be hidden. Vaidyanathan et al. [23] have suggested a chaos-based steganography method. In the steganography application, a 64×64 image is hidden in the audio file using a new 4-D chaotic system. Miri and Faez [1] have suggested a unique method to hide data employing genetic algorithm. The secret data are encrypted and the encrypted data are embedded in frequency domain. Yildirim [24] has presented a RGB image encryption technique using DNA encoding method. A chaotic system including neuron model based on memristor structure is utilized in encryption scheme. The analog circuit of the chaotic system is constructed using operational transconductance amplifier (OTA). An algorithm with the ability of being resistant to differential attack which is based on complement operations and bit swapping is introduced.

In literature, transform domain-based techniques such as discrete cosine transform (DCT) [25], discrete wavelet transform (DWT) [26], and discrete Fourier transform (DFT) [7] have been suggested. In these techniques, transformation processes are performed in order to hide the secure message in the cover object. On the other hand, in this study, a LSB-based method which is carried out in spatial domain has been proposed due to its being a simpler technique compared to the one performed in transform domain [27].

The motivation of carrying out this work is presented as follows. The encrypted voice comment of the doctor is hidden in a medical image. A novel encryption scheme is suggested in order to cipher the voice data. Differently from the previous studies [9–22] on encryption technique, the algorithm of XOR operation for sequential bits of the pixel has been suggested. In addition, the complement and four bits swapping operations dependent on the number of bits equal to one have also been proposed in this work. In previous studies [1, 6, 23] on steganography technique, differential attack has not been taken into consideration. However, in the proposed study, a novel algorithm which is resistant to differential attack has been proposed in order to be utilized in the steganography method.

The rest of the paper is organized as follows. Section 2 presents a novel steganography algorithm scheme including chaotic system to hide the doctor's ciphered voice comment. Security analyses which are

statistical attacks, differential attack and initial condition sensitivity are given to show the functioning of the suggested steganography algorithm in Sect. 3. The study is concluded in Sect. 4.

2 A new steganography algorithm scheme based on chaos to hide encrypted voice comment

An image steganography technique in order to hide the encrypted audio data has been suggested in this study. The proposed steganography technique is based on logistic chaotic map. When the chaotic system is realized on a digital computing device with finite precision, it is called digital chaotic system. The sequence obtained by the digital chaotic system becomes periodic due to finite precision device. This challenge leads the dynamical degradation of digital chaotic system [28]. In this study, a delay-introducing method-based logistic chaotic map presented in [29] has been utilized to counteract the effect of the dynamical degradation in the digitalization of the chaotic system. Logistic chaotic map which is realized on the device with finite precision can be presented as

$$x_{i+1} = \mathrm{FL}(ax_i(1 - x_i)) \tag{1}$$

where FL represents the precision function and the control parameter $a \in (3.5699, 4)$. To counteract the degradation effects, a linear function of delay state x_{i-1} given in Eq. (2) is utilized in place of parameter a.

$$h(x_{i-1}) = bx_{i-1} + 4 - b \tag{2}$$

where parameter $b \in (0, 0.4)$ and function $h(x_{i-1}) \in (3.5699, 4)$. Therefore, Logistic chaotic map utilizing delay-introducing method which is realized on a digital computing device with finite precision can be defined as

$$x_{i+1} = \mathrm{FL}((bx_{i-1} + 4 - b)x_i(1 - x_i)) \tag{3}$$

where the initial values $x_0 = 0.1$ and $x_1 = 0.2$. In the algorithm of steganography method, the secret key sequences with the values between 0 and 255 are required since the density of a pixel is between 0 and 255. In order to obtain the values of x_{i+1} between 0 and 255, the following equation is used.

$$x_{i+1} = \mathrm{floor}\left(\mathrm{mod}\left(x_{i+1} \times 10^5, 256\right)\right) \tag{4}$$

where mod represents modulo operation and floor rounds the element to the nearest integer less than or equal to that element.

Steganography scheme comprises of converting audio data to pixel value, random pixel placement, logical XOR, XOR for sequential bits, complement and swap, XOR operation with next pixel and encrypted audio data hiding into cover image based on LSB (least significant bit) method. To improve security of the proposed steganography method, audio data to be hidden have been encrypted. In an algorithm which is robust against differential attack, a minor change in one bit of any pixel in the plain image should completely change the encrypted image [24]. In the introduced algorithm, XOR operation for sequential bits transfers the value of any bit in the pixel to the other bits of the pixel. This operation is useful for the bits of a pixel. On the other hand, XOR operation with next pixel transfers the value of any pixel in the image to the other pixels of the image. In brief, XOR operation for sequential bits has an impact on bits, while XOR operation with next pixel has an impact on pixels to obtain a robust algorithm. Therefore, these two algorithms convey any slight change in pixel to the other pixels and they are necessary for generating an algorithm resistant to differential attack. It is proved in the analysis part that the encrypted data can be resistant against differential attack. In this paper, a lung angiography dual-energy CT image in [30] is utilized as a cover object. In addition, the bit depth of audio file to be hidden is chosen as 8 bits in this study. In practical implementations, the length of the voice record depends on the size of the cover image and the quality of voice record. When we increase the size of the cover image or decrease the quality of the voice record, the length of the voice data to be hidden in the medical image can be extended. For example, more than 1-h audio record can be hidden utilizing a cover image of size 2048 × 2048 pixels and down sampling the audio record by 8.

(i) Converting audio data to pixel value

(1) Assume that a 8-bit audio file is named A and its size is N and each audio sample value in $A(i)$ ranges from − 128 to 127, $i = 1,2,\ldots,N$. $A(i)$ is converted to $B(i)$ which ranges from 0 to 255. $B(i)$ can be shown as follows

$$B(i) = s_7 \times 2^7 + s_6 \times 2^6 + s_5 \times 2^5 + s_4 \times 2^4 + s_3 \times 2^3 + s_2 \times 2^2 + s_1 \times 2^1 + s_0 \times 2^0 \quad (5)$$

Obviously, s_i, i = 0,1,2,…,7 belongs to {0,1}.

(2) In an image, a pixel value is demonstrated using 8 bits. Using Eq. (5), each element in $B(i)$ presented as an integer value is transformed into 8-bit binary value named C(N,8). C(i) is given as "$s_7s_6s_5s_4s_3s_2s_1s_0$". C(p) ranges from 0 to 255, p = 1,2,…,N. Each sample of audio data can be presented as one pixel by converting the 8-bit audio data value into a pixel value.

(ii) **Pseudorandom pixel placement**

In the literature, random number generators (RNGs) have been utilized in numerous applications [31–34]. There are two kinds of RNGs which are true random number generators (TRNGs) and pseudo random number generators (PRNGs). The TRNGs are utilized to produce random numbers with the help of physical processes which are jitter and thermal noise. Nevertheless, the TRNGs are not able to be used in encryption and decryption processes since two exactly same secret key sequences can not be obtained in these processes, respectively. On the other hand, in the PRNGs, a sequence of unpredictable values can be generated due to its deterministic behavior [31]. This type of random generator is called pseudo since the same unpredictable sequence is produced under the same condition in encryption and decryption processes, respectively. In other word, the pseudorandom pixel placement algorithm makes pixel placement unpredictable, not random.

In the introduced algorithm, a blank image whose all pixel values are zero is generated in order to hide the voice comments of the doctor into a cover medical image. Each value of C(p) is placed in this blank image, not sequentially, utilizing a pseudorandom coordinates array produced by the chaotic system. For a cover image of $m \times m$ pixels, a pseudorandom pixel coordinates array is generated using Algorithm 1. Using coordinates array in terms of row and column produced by Algorithm 1, a pseudorandom placement of voice comments into the blank image has been carried out. X, Y, Z represent the digital values produced by the variable x of logistic chaotic map given in Eq. (4). Parameter b given in Eq. (3) is taken as 0.1, 0.2, 0.3, respectively, to obtain the values of X, Y, Z.

Algorithm 1: Pseudorandom pixel placement

```
s = 0;
XY = xor(X,Y);
YZ = xor(Y,Z);
while (coordinates_array < N) do
s = s + 1;
row = X(s).*Y(s).*XY(s);
row = mod(row,m) + 1;
column = Y(s).*Z(s).*YZ(s);
column = mod(column,m) + 1;
coordinate = [row,column];
coordinates_array = unique([coordinates_array;
  coordinate]);
end while
```

(iii) Logical XOR operation

Logical XOR operation is carried out utilizing Algorithm 2. The key of R(p) is produced using a delay-introducing method-based logistic chaotic map.

Algorithm 2: Logical XOR operation

```
XY = xor(X,Y);
YZ = xor(Y,Z);
XZ = xor(X,Z);
R = [XY;YZ;XZ;X;Y;Z];
C = C ⊕ R;
```

(iv) XOR for sequential bits

XOR operation is performed for sequential

bits of each C(p) using Algorithm 3. Sequential XOR operation is carried out from LSB to MSB. For example, assume that C(p) is [10010110]. After performing Algorithm 3, new C(p) becomes [01110010].

Algorithm 3: XOR for sequential bits

```
C(p,7) = xor(C(p,7), C(p,8));
C(p,6) = xor(C(p,6), C(p,7));
C(p,5) = xor(C(p,5), C(p,6));
C(p,4) = xor(C(p,4), C(p,5));
C(p,3) = xor(C(p,3), C(p,4));
C(p,2) = xor(C(p,2), C(p,3));
C(p,1) = xor(C(p,1), C(p,2));
```

(v) Complement and swap

The bits of each C(p) which are equal to one are counted. One's complement operation is done when the number of bits which are one is odd, otherwise four bits swapping operation is performed. The complement and swap operations are presented in Algorithm 4. All zeroes replace with ones and all ones replace with zeroes to carry out one's complement operation. From MSB to LSB, the first 4 bits are swapped with the last 4 bits to perform four bits swapping operation. For instance, suppose that C(p) is [10010110]. After applying Algorithm 3 and Algorithm 4, new C(p) becomes [01110010] and [00100111], respectively. In another example, assume that only LSB of C(p) is altered and it becomes 1 instead of 0 as compared with previous example and C(p) is [10010111]. After applying Algorithm 3 and Algorithm 4, new C(p) becomes [10001101] and [11011000], respectively. In these two examples, decimal values of the new C(p) after applying Algorithm 3 and Algorithm 4 become 39 and 216, respectively. When the new C(p) values are compared with each other in two examples, it is clear that only one bit change in C(p) leads huge alteration in the new value of C(p) after carrying out XOR for sequential bits operation and complement and swap operations. A minor change in a pixel of the image including doctor's voice comments as pixel values causes a huge change in the encrypted medical cover image. It means that the suggested method can resist differential attack.

Algorithm 4: Complement and swap

```
Count the bits equal to one
for i = 1:8 do
if C(p,i) = = 1 do
counter = counter + 1;
end if
end for
If the number of bits equal to one is odd, perform
  complement otherwise carry out four bits swapping
  operation
m = mod(counter,2);
if m = = 1 do
C(p,1:8) = complement(C(p,1:8));
else do
C_temp(p,1:8) = C(p,1:8);
C(p,1:4) = C_temp(p,5:8);
C(p,5:8) = C_temp(p,1:4);
end if
```

(vi) XOR operation with next pixel

The effect of a pixel should be delivered to all pixels to obtain an image steganography scheme resistant against differential attack. Each binary pixel, C(p), is XORed with next pixel, C(p + 1), in order that the encryption scheme can resist differential attack. The result of XOR operation becomes the new value of next pixel. Moreover, before performing this operation, each pixel is also XORed with the key values, S(p), obtained from chaotic system to increase the complexity of the steganography scheme. XOR operation with next pixel is carried out using Algorithm 5.

Algorithm 5: XOR operation with next pixel.

```
XY = xor(X,Y);
YZ = xor(Y,Z);
```

```
XY = xor(X,Y);
XZ = xor(X,Z);
S = [X;Y;Z;XY;YZ;XZ];
C(p) = C(p) ⊕ S(p);
C(p + 1) = C(p) ⊕ C(p + 1);
```

The algorithm of XOR operation with next pixel is carried out from C(1) to C(N) and then from C(N) to C(1) to make sure that any slight alteration in a pixel can have an effect on the all pixels in the image.

(vii) Data hiding based on LSB method

In this part of steganography scheme, encrypted voice comments of the doctor are embedded in cover medical image. The audio data to be hidden which are converted to an encrypted image are embedded to the R, G, B components of the cover image. Each pixel of the encrypted image including audio data is embedded to the related pixel in the cover medical image. From MSB to LSB, the first 3 bits, the next 3 bits and the last 2 bits of C(p) are embedded to the last 3 bits of R, the last 3 bits of G and the last 2 bits of B components of the cover image. Algorithm 6 presents data hiding based on LSB method. Cover medical image is given as D(N,8,3). Each R, G, B components of D(p) is defined between 0 and 255, p = 1,2,…,N.

Algorithm 6: Data hiding based on LSB method

```
for p = 1:N do
Embedding encrypted audio data in R component of cover medical image
D(p,6:8,1) = C(p,1:3);
Embedding encrypted audio data in G component of cover medical image
D(p,6:8,2) = C(p,4:6);
Embedding encrypted audio data in B component of cover medical image
D(p,7:8,3) = C(p,7:8);
end for
```

Figure 1 presents a new chaotic system-based steganography algorithm scheme to provide the hiding of the voice comments of the doctor. The steps of steganography scheme are presented below. These ten steps present the encryption method and voice data hiding method. In the decoding phase, the exact reverse processes of these 10 steps are performed in order to uncover the voice data belonging to the doctor.

Step 1: Input a 8-bit audio data including the comments of the doctor.

Step 2: Convert the audio data to pixel value.

Step 3: Perform pseudorandom pixel placement in a blank image with the size of $m \times m$ pixels using Algorithm 1.

Step 4: A key which is called R(p) is generated from chaotic system. Perform logical XOR operation presented in Algorithm 2.

Step 5: XOR for sequential bits, complement and swap and XOR operation with next pixel operations are performed one after another. Encrypted audio data have been obtained and the presented steganography method is able to be robust to differential attack using Algorithm 3, Algorithm 4, and Algorithm 5.

Step 6: Input a RGB cover medical image of $m \times m$ pixels.

Step 7: The cover image is split into R, G, B components.

Step 8: Hide the audio data in cover medical image using Algorithm 6.

Step 9: Obtain R, G, B components of stego medical image.

Step 10: Recover RGB stego medical image which includes the encrypted voice comments of the doctor.

Figure 2a, b presents image histograms for R, G, B components of cover image and stego image, respectively. Figure 2c, d shows the time series and histogram for secret audio data and obtained audio data, respectively. It is obvious from Fig. 2a, b, both histograms are relatively similar and audio data to be hidden do not change the cover image dramatically. In addition, Fig. 2c, d proves that the secret audio data can be successfully obtained from stego image. Figure 3 demonstrates the correlations in the horizon, vertical and diagonal directions for stego image and cover image. When Fig. 3a, b is compared, it can be clearly seen that the audio data make only minor alteration on stego image.

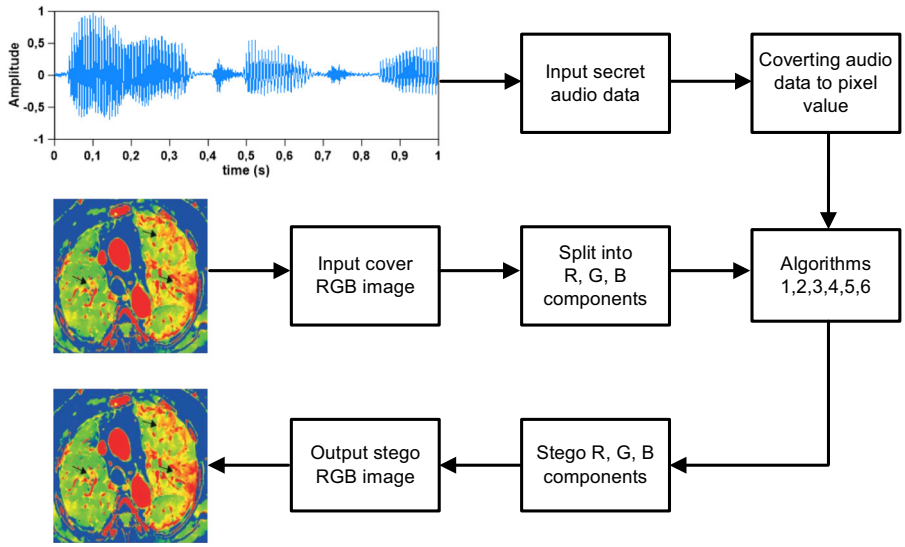


Fig. 1 A chaos-based steganography scheme

In image processing theory, there are numerous kinds of quality measurement parameters to determine the similarity between the original image and modified image. Root-mean-squared error (RMSE), mean squared error (MSE), peak-signal-to-noise ratio (PSNR), mean absolute error (MAE), and Structural Similarity Index Metric (SSIM) are utilized as quality measurement parameters in this study [35]. SSIM is given as:

$$\mathrm{SSIM}(\mathrm{CI},\ \mathrm{SI}) = \frac{(2\mu_{\mathrm{CI}}\mu_{\mathrm{SI}} + c_1)(2\sigma_{\mathrm{CISI}} + c_2)}{(\mu_{\mathrm{CI}}^2 + \mu_{\mathrm{SI}}^2 + c_1)(\sigma_{\mathrm{CI}}^2 + \sigma_{\mathrm{SI}}^2 + c_2)} \tag{6}$$

$$\mu_{\mathrm{CI}} = \frac{1}{M \times N}\sum_{i=1}^{M\times N} \mathrm{CI}_i \tag{7}$$

$$\mu_{\mathrm{SI}} = \frac{1}{M \times N}\sum_{i=1}^{MxN} \mathrm{SI}_i \tag{8}$$

$$\sigma_{\mathrm{CI}}^2 = \frac{1}{M \times N - 1}\sum_{i=1}^{M\times N} (\mathrm{CI}_i - \mu_{\mathrm{CI}})^2 \tag{9}$$

$$\sigma_{\mathrm{SI}}^2 = \frac{1}{M \times N - 1}\sum_{i=1}^{M\times N} (\mathrm{SI}_i - \mu_{\mathrm{SI}})^2 \tag{10}$$

$$\sigma_{\mathrm{CISI}} = \frac{1}{M \times N - 1}\sum_{i=1}^{M\times N} (\mathrm{CI}_i - \mu_{\mathrm{CI}})(\mathrm{SI}_i - \mu_{\mathrm{SI}}) \tag{11}$$

where c_1 and c_2 are constants. σ_{CISI}, σ_{SI}^2, σ_{CI}^2, μ_{SI}, μ_{CI}, SI and CI represent the covariance of cover and stego images, the variance of stego image, the variance of cover image, the average of stego image, the average of cover image, stego image and cover image. M and N are the dimensions of the image. MSE, RMSE, MAE, and PSNR are given, respectively, in Eqs. (12)–(15).

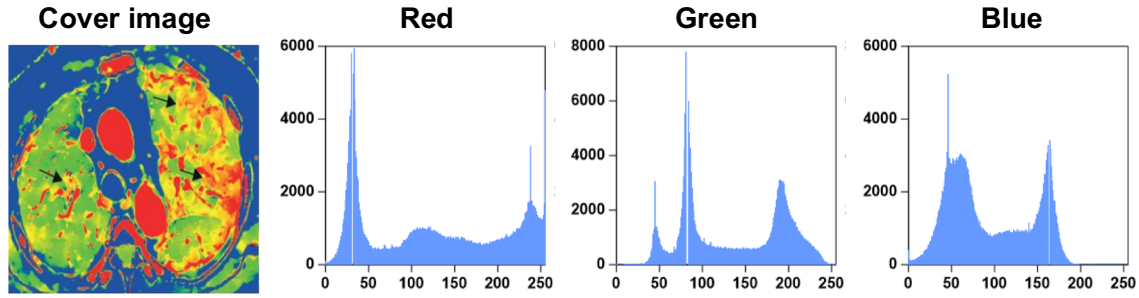
$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} (\mathrm{CI}(i,j) - \mathrm{SI}(i,j))^2 \tag{12}$$

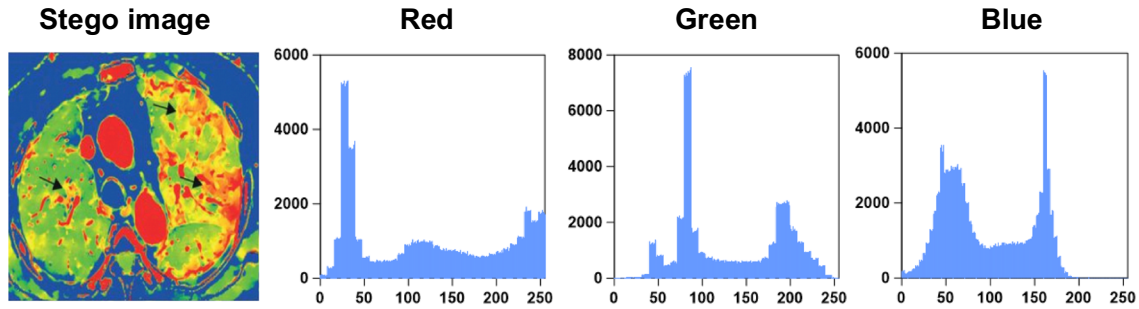
$$\mathrm{RMSE} = \sqrt{\mathrm{MSE}} \tag{13}$$

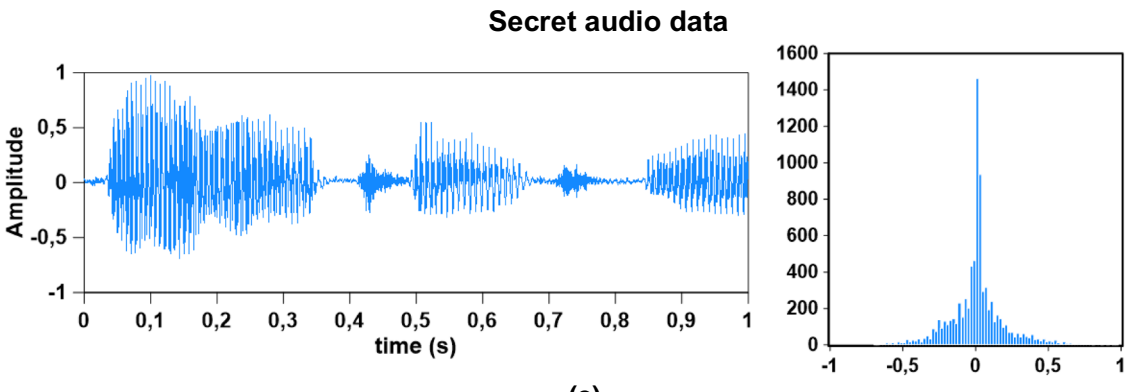
$$\mathrm{MAE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} |\mathrm{CI}(i,j) - \mathrm{SI}(i,j)| \tag{14}$$

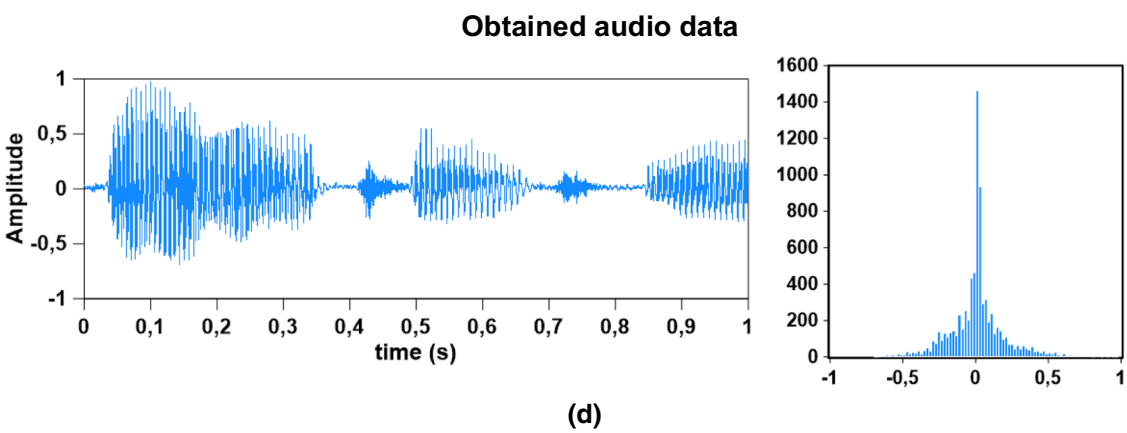
$$\mathrm{PSNR} = 10\log_{10}\frac{(2^8 - 1)^2}{\sqrt{\mathrm{MSE}}} \tag{15}$$

Table 1 gives similarity metrics between cover image including no audio data and stego image including audio data for 512 × 512 pixel and 1024 × 1024 pixel images. When cover image is equal to stego image, the values of SSIM, MSE, RMSE, MAE, and PSNR are obtained as 1, 0, 0, 0 and ∞, respectively. The similarity metrics are determined


Cover image
Red
Green
Blue
(a)


Stego image
Red
Green
Blue
(b)


Secret audio data
Amplitude
time (s)
(c)


Obtained audio data
Amplitude
time (s)
(d)

◀**Fig. 2** The image histograms for R, G, B components **a** cover image, **b** stego image. The time series and histogram for **c** secret audio data, **d** obtained audio data

for R, G, B components of stego image and cover image. Table 1 shows that stego image with doctor's voice comments is relatively similar to plain cover image. As expected, the values of similarity metrics are obtained as closer to the ideal values for blue component compared to red and green components. Because, 2 bits are hidden in blue component, while 3 bits are hidden both red and green components. Moreover, using a smaller cover image in steganography method increases the similarity between cover and stego images.

3 Security analyses

Any introduced steganography method should have the ability to exhibit good performance and a good encryption technique should defense the commonly known security risks. Various security analyses such as differential attack, statistical attacks and initial condition sensitivity must be carried out in order to

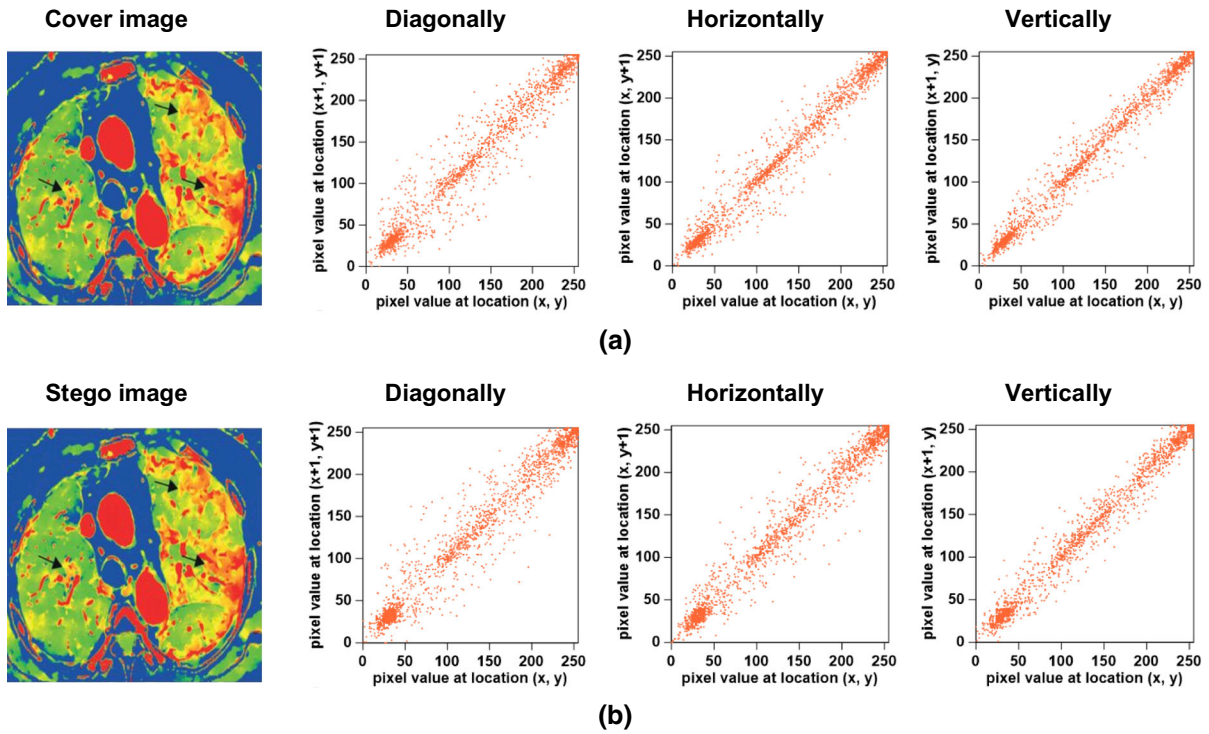


Fig. 3 The correlation coefficients in the diagonal, horizon and vertical directions **a** cover image, **b** stego image

Table 1 Similarity metrics between cover image and stego image in terms of R, G, B components

Image size	CI(i,j) = SI(i,j)	SSIM 1	MSE 0	RMSE 0	MAE 0	PSNR ∞
512 × 512 pixels	Red	0.8337	10.9875	3.3147	2.6856	37.7218
	Green	0.7926	10.2826	3.2066	2.5981	38.0098
	Blue	0.9273	2.5263	1.5894	1.2556	44.1060
1024 × 1024 pixels	Red	0.7081	10.9596	3.3105	2.6832	37.7329
	Green	0.6639	10.2863	3.2072	2.5981	38.0082
	Blue	0.8645	2.5226	1.5883	1.2555	44.1122

present the effectiveness and robustness of the suggested steganography scheme.

3.1 Differential attack analysis

One of the security attacks which is commonly used is called differential attack. An encryption scheme with diffusion property displays high performance of being resistant against differential attack [36]. By making a minor alteration on the plain image such as changing the value of one pixel, the attackers try to determine significant relationships among the encrypted image and the plain image. When a minor modification in the plain image leads a huge difference in the encrypted image, the encrypted image is considered as strong against differential attack. Two well-known measures which are number of pixels change rate (NPCR) and unified average changing intensity (UACI) are carried out to evaluate the effect of only one pixel changing in the plain image over the encrypted image [22, 24, 36–38]. These measures are defined as:

$$\mathrm{NPCR} = \frac{1}{W \times H} \sum_{i,j} D(i,j) \times 100\% \tag{16}$$

$$\mathrm{UACI} = \frac{1}{W \times H \times 255} \sum_{i,j} |C_1(i,j) - C_2(i,j)| \times 100\% \tag{17}$$

Where C_1 and C_2 indicate two encrypted images for two plain images which are different by one bit only, H and W show the height and width of the image. D is an array consisting of 0 and 1. If $C_1(i,j) = C_2(i,j)$, then $D(i,j)$ is equal to 0, otherwise $D(i,j)$ is equal to 1. The number of different pixels is given by NPCR. The average intensity changes between two images is determined by UACI. When UACI and NPCR values are large enough, the introduced steganography method is resistant against differential attacks [24, 39]. The value of any sample in audio data is changed with a difference of 1 to perform differential attack analysis. A one-second audio file whose sample rate is 8 kHz is used as a secret data in this study. The value of audio sample at position (5649) is increased by 1 for numerical analysis to determine the values of UACI and NPCR. To increase the security of the suggested steganography scheme, Algorithms 3, 4, 5 are utilized. By using these three algorithms, the proposed steganography method can resist differential attack. Table 2 presents the effect of Algorithms 3, 4, 5 on resisting differential attack. As can be seen in Table 2, after using the suggested steganography algorithm, the values of UACI and NPCR become large enough. However, NPCR and UACI values are quite small when Algorithms 3, 4, 5 are not utilized in steganography scheme.

The introduced steganography scheme is tested against differential attack. Ten 8-bit samples of the doctor's voice comments are randomly selected and the values of these samples are changed with a difference of 1. The results of UACI and NPCR for ten samples are presented in Table 3. The average values of ten samples for UACI and NPCR are 33.5688% and 99.8069%, respectively. Table 4 presents a comparative study of the introduced algorithm to previous algorithms in terms of the values of UACI, NPCR, and information entropy.

3.2 Statistical attack analyses

Statistical attack analyses such as correlations of two neighboring pixels, histogram, and information entropy are performed in this part of work.

3.2.1 Histogram analysis

The distribution of intensity levels belonging to each pixel of the image is shown by the histogram plot. In other words, the histogram demonstrates the values of pixel distribution. For an ideal cryptosystem, the histogram for the encrypted image must be distributed uniformly and is supposed to be flat to avoid statistical attacks. Figure 4 presents the histogram of encrypted audio data as an image including the comments of the doctor. Figure 4 shows that the pixels belonging to the encrypted audio data as an image are distributed uniformly and the encrypted image is not able to offer any significant information with regard to the plain image. Thus, steganography algorithm scheme introduced in this paper shows good confusion properties [24, 37, 38].

3.2.2 Correlation coefficient analysis of two neighboring pixels

An image including meaningful information may have high correlations among its neighboring pixels. Because of this, a powerful image steganography

Table 2 The effect of Algorithms 3, 4, 5 on resisting differential attack

	NPCR (%) (5649)	UACI (%) (5649)
The steganography scheme	99.7074	33.5321
The steganography scheme without using Algorithms 3, 4, 5	0.0004	0.000001

Table 3 Results of NPCR and UACI tests for ten samples

Position	(5649)	(255)	(2216)	(370)	(778)
NPCR (%)	99.7074	99.6975	99.8741	99.7890	99.8680
UACI (%)	33.5321	33.5076	33.5517	33.5614	33.5977
Position	(6588)	(5559)	(2537)	(7602)	(276)
NPCR (%)	99.8260	99.6090	99.9062	99.8142	99.9771
UACI (%)	33.5764	33.5546	33.5778	33.6274	33.6011

Table 4 Comparative study of NPCR, UACI and information entropy of the introduced algorithm to previous algorithms

Images	NPCR	UACI	Entropy
[24][a]	98.465	35.8008	7.9990
[37]	99.61	33.47	7.9993
[39]	99.2453	36.4973	7.9970
[40][a]	99.61	33.38	7.9980
[41][a]	99.2172	33.4054	7.9968
[42][a]	99.5799	33.4342	7.9852
[43][a]	99.6058	33.526	7.9973
[44][a]	99.6689	33.5561	7.9979
[45][a]	99.6155	33.2744	7.9992
[46][a]	99.61	33.44	7.9997
[47]	99.6068	33.4597	7.9993
[48]	99.6204	30.7972	7.9972
This study	99.8069	33.5688	7.9993

[a]The mean value of R, G, B components is calculated

algorithm scheme should have the ability to break the correlations between neighboring pixels of the encrypted image and the correlation between two pixels should be nearly zero. If the correlation value belonging to the encrypted image is close to 1, then encrypted image is highly correlated and the encryption scheme fails to defense against statistical attack. The correlation analysis determining the similarity in plain and encrypted images has been carried out for the

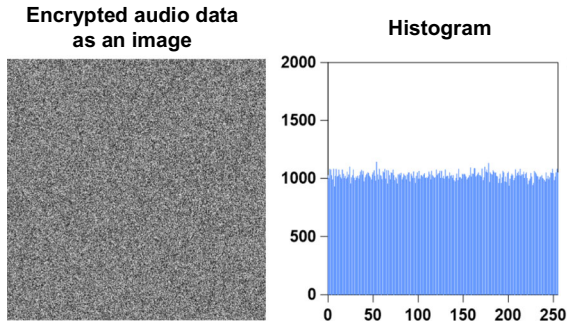


Fig. 4 The histogram of the encrypted voice comments of doctor as an image

encrypted audio data as an image along vertical, horizontal and diagonal directions [24, 36–38]. In order to present correlation coefficient between two neighboring pixels, the following processes have been performed. Firstly, 2000 pairs of two neighboring pixels are randomly selected with the diagonal, vertical and horizontal directions from the encrypted image. In addition, the correlation coefficient value belonging to the encrypted image is calculated using the equations given below [24, 39].

$$\mathrm{corr}(x,y) = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{18}$$

$$\mathrm{cov}(x,y) = \frac{1}{T}\sum_{i=1}^{T}[x_i - E(x)][y_i - E(y)] \tag{19}$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}[x_i - E(x)]^2 \tag{20}$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i \tag{21}$$

where x and y represent the values of two neighboring pixels and T indicates the total pairs of neighboring pixels. The values of correlation are given to find if there is a small correlation among two neighboring

pixels in the encrypted image [24]. The correlations between two neighboring pixels of the encrypted image, cover image and stego image are presented in Table 5 for 512 × 512 pixel and 1024 × 1024 pixel images. The values of the correlations belonging to encrypted image along the horizontal, vertical and diagonal, directions are almost zero. The correlation distributions in the encrypted image along three directions are presented in Fig. 5. Both Fig. 5 and Table 5 prove that the proposed steganography algorithm using a chaotic system can be used to deliver the encrypted information safely. In addition, utilizing a bigger cover image decreases the correlation coefficients of the encrypted images.

3.2.3 Information entropy analysis

Among numerous randomness test standards, the information entropy is used to show uncertainties of the image information. The pixels of a desired encrypted image should be distributed uniformly. The distribution of pixel intensity value in image can be measured by the information entropy. When the entropy of the image is higher, the uncertainty is bigger. It means that the decryption procedure for the image needs more information. On the contrary, the more orderly the encrypted image is, the smaller the information entropy is. The value of ideal entropy is equal to 8 [24, 36, 37, 39, 49]. $H(m)$ which is the information entropy of m can be calculated as

$$H(m) = -\sum_{i=1}^{L} P(m_i)\log_2 P(m_i) \tag{22}$$

where L indicates grayscale level, $P(m_i)$ denotes the probability of the m_ith possible pixel. The entropy is measured in bits as log is base 2 logarithm. Using Eq. (22), the entropy is calculated as 7.9993 bits for the encrypted audio data. The value of information entropy indicates that the encrypted image shows the behavior of a random source and the proposed steganography algorithm is resistant to the statistical attacks. In other words, the probability of accidental data and information leakage of doctor comments is quite low [24, 36].

3.3 Initial condition sensitivity analysis

For a good steganography algorithm, it is vital to be sensitive to the initial condition belonging to the chaotic system. Initial condition sensitivity analysis is done to show the functioning of the introduced algorithm technique [24]. This analysis is performed utilizing one parameter in chaotic system with a slight difference. The precision is found as 10^{-16} for the chaotic system used in the steganography scheme. When the initial condition is altered, different sequence is obtained from the chaotic system. However, if the alteration in the value of initial condition becomes smaller than the stated precision, the sequence obtained from the chaotic system remains unchanged. This situation should be considered as the constraint of the steganography scheme.

In initial condition sensitivity analysis, the encryption stage is performed using original parameter b. However, in the decryption stage, an increase of 10^{-16} in parameter b has been realized and all other parameters have remained the same to understand the effect of the value of the initial condition on encryption scheme. Figure 6 shows the initial condition sensitivity analysis. The obtained audio data from decrypted image with false parameter b is given in Fig. 6a. It is clear that the proposed steganography scheme is sensitive to initial condition. Thus, the

Table 5 The correlation coefficient values between two neighboring pixels of the encrypted image, cover image and stego image

Direction	512 × 512 pixel image			1024 × 1024 pixel image		
	Encrypted image	Cover image	Stego image	Encrypted image	Cover image	Stego image
Diagonal	− 0.0023	0.9738	0.9722	− 0.0003	0.9928	0.9912
Horizontal	− 0.0027	0.9830	0.9814	0.0009	0.9954	0.9938
Vertical	0.0045	0.9893	0.9877	0.0015	0.9973	0.9957

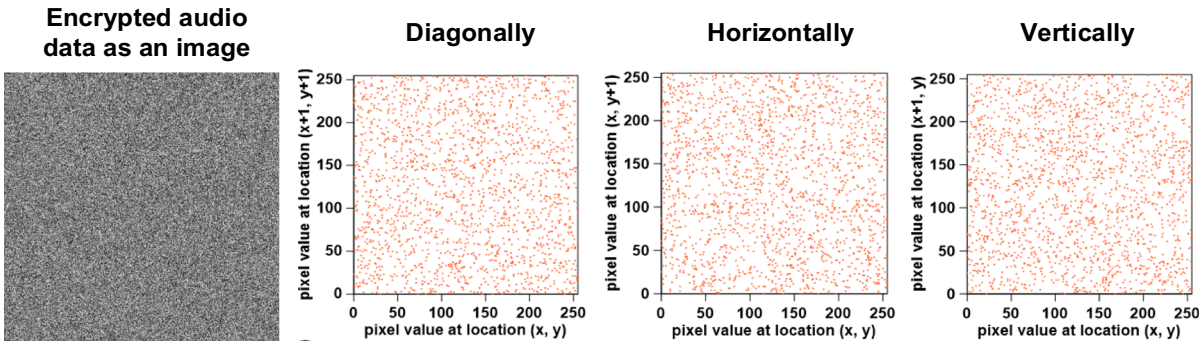


Fig. 5 The correlation coefficient of encrypted voice comments of doctor as an image in the diagonal, horizontal and vertical directions

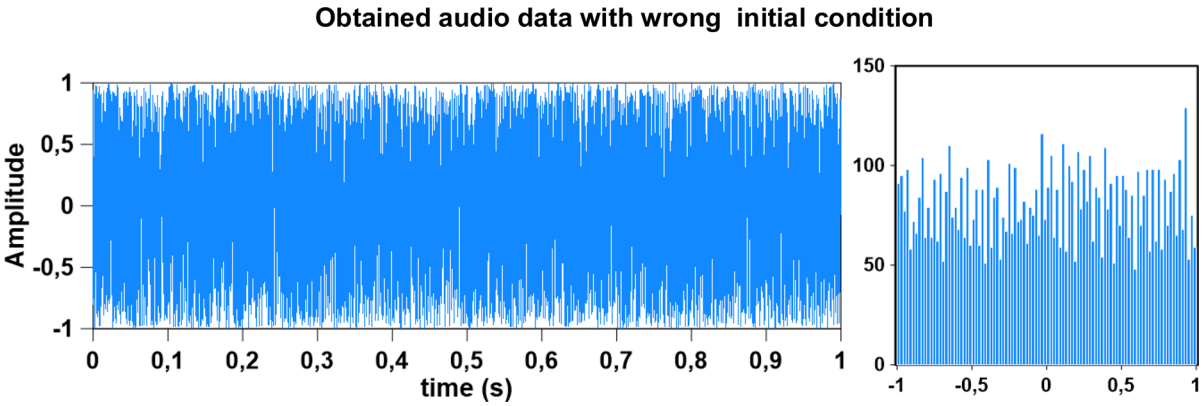


Fig. 6 Initial condition sensitivity analysis selecting parameter b with an increase of 10^{-16}

introduced algorithm is resistant against exhaustive attack.

3.4 Known plaintext and chosen plaintext attacks

Plaintext attacks carried out by pirates include known plaintext and chosen plaintext attacks. The pirates are able to access the encryption scheme and can produce encrypted image from a selected plain image in chosen plaintext attack. On the other hand, in known plaintext attack, the pirates have encryption scheme and they can access encrypted and plain image contents which are randomly defined, not chosen by pirates. Chosen plaintext attack is the most intense and effective attack since the pirates are able to select encrypted and plain image contents [22, 38, 50]. It is stated in Sect. 3.3 that the introduced steganography technique is highly sensitive to initial condition. It means that a slight alteration in the value of initial condition enables a great change in the content of encrypted and decrypted images. In addition, encrypted image content is linked to not only existing bit of pixel or pixel of image value but also directly linked to next bit of pixel or pixel of image value thanks to enhanced XOR operations such as XOR operation for sequential bits and XOR operation with next pixel algorithms. Because of the reasons stated above, the introduced steganography method is able to be resistant against known plaintext and chosen plaintext attacks. Table 6 presents the comparison of this study with previous studies about chaos theory. In this table, this study and previous studies are compared in terms of performing steganography technique, employing cryptography technique, including security analysis and being resistant to differential attack.

Table 6 The comparison between this study and previous studies on chaos theory

	This study	[1]	[6]	[21]	[22]	[23][a]	[24]	[37]	[39]	[42]	[45]	[47]	[48]	[49]
Steganography	✔	✔	✔	✗	✗	✔	✗	✗	✗	✗	✗	✗	✗	✗
Cryptography	✔	✔	✗	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Security analysis	✔	✗	✗	✔	✔	✗	✔	✔	✔	✔	✔	✔	✔	✔
Resistant to differential attack	✔	✗	✗	✗	✔	✗	✔	✔	✔	✔	✔	✔	✔	✗

[a] Security analysis and differential attack analysis are not given for sound steganography implementation

4 Conclusion

In this work, a novel image steganography technique for the purpose of hiding the encrypted audio data which include the comments of the doctor has been proposed. In the steganography scheme, audio data are firstly converted to pixel values and these values are placed randomly in a blank image. Then, the image including doctor comments has been encrypted and the image with audio data has been embedded in a medical cover image. The histogram of the encrypted voice comments of doctor as an image is extremely uniform. Therefore, the ciphered image with sound data does not offer any meaningful information to the pirates. It can be seen from the results of the coefficient analysis that the values of correlation among two neighboring pixels in the ciphered images in three directions which are diagonal, vertical and horizontal are almost zero. It indicates that the steganography algorithm scheme can powerfully remove correlations among the neighboring pixels. A powerful steganography scheme should offer an information entropy which is close to 8 for an encrypted image. The information entropy is obtained as 7.9993 bits using the proposed steganography scheme. Analyses such as information entropy, correlation coefficient and histogram have proved that the introduced chaos-based algorithm scheme is able to be robust against statistical attacks. In addition, the average of the ten UACI values is obtained as 33.5688% and the average of the ten NPCR values is obtained as 99.8069% for a 512×512 pixel cover image. Taking into account these two values, it can be said that the suggested steganography scheme can resist differential attack. Moreover, initial condition sensitivity analysis has proved that the proposed algorithm in this paper is also robust against exhaustive attack. The suggested algorithm can also withstand known plaintext and chosen plaintext attacks.

Data availability All data generated or analyzed during this study are included in this published article.

Declarations

Conflict of interest The author declares that there is no conflict of interest.

References

1. Miri, A., Faez, K.: Adaptive image steganography based on transform domain via genetic algorithm. Optik (Stuttg) **145**, 158–168 (2017). https://doi.org/10.1016/j.ijleo.2017.07.043
2. Davis, R.: The data encryption standard in perspective. IEEE Commun Soc Mag **16**, 5–9 (1978)
3. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun ACM **21**, 120–126 (1978)
4. Liu, S., Guo, C., Sheridan, J.T.: A review of optical image encryption techniques. Opt Laser Technol **57**, 327–342 (2014)
5. Liu, S., Sheridan, J.T.: Optical encryption by combining image scrambling techniques in fractional Fourier domains. Opt Commun **287**, 73–80 (2013)
6. Karakus, S., Avci, E.: A new image steganography method with optimum pixel similarity for data hiding in medical images. Med Hypotheses **139**, 109691 (2020). https://doi.org/10.1016/j.mehy.2020.109691
7. Cheddad, A., Condell, J., Curran, K., Mc, K.P.: Digital image steganography: survey and analysis of current methods. Signal Process **90**, 727–752 (2010)
8. Yashwanth, R.C., Kumar, G.M.: Review on ımage steganography. Indian J Sci Technol (2016). https://doi.org/10.17485/ijst/2015/v8i1/106446
9. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image Vis Comput **24**, 926–934 (2006)
10. Zhang, Y., Li, C., Li, Q., Zhang, D., Shu, S.: Breaking a chaotic image encryption algorithm based on perceptron

model. Nonlinear Dyn **69**, 1091–1096 (2012). https://doi.org/10.1007/s11071-012-0329-y
11. Li, L., Kong, L.: A new ımage encryption algorithm based on chaos. Xitong Fangzhen Xuebao/J Syst Simul **30**, 954–961 (2018). https://doi.org/10.16182/j.issn1004731x.joss.201803023
12. Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N.: Image encryption process based on chaotic synchronization phenomena. Signal Process **93**, 1328–1340 (2013). https://doi.org/10.1016/j.sigpro.2012.11.008
13. Li, P., Zhang, W., Li, Z., Liu, W., Halang, W.A.: FPGA implementation of a coupled-map-lattice-based cryptosystem. Int J Circuit Theory Appl **38**, 85–98 (2010)
14. Chen, W., Chen, X., Sheppard, C.J.R.: Optical image encryption based on diffractive imaging. Opt Lett **35**, 3817 (2010). https://doi.org/10.1364/ol.35.003817
15. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett **20**, 767 (1995). https://doi.org/10.1364/ol.20.000767
16. Kwok, H.S., Tang, W.K.S.: A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fractals **32**, 1518–1529 (2007). https://doi.org/10.1016/j.chaos.2005.11.090
17. Gao, H., Zhang, Y., Liang, S., Li, D.: A new chaotic algorithm for image encryption. Chaos Solitons Fractals **29**, 393–399 (2006). https://doi.org/10.1016/j.chaos.2005.08.110
18. Yang, C., Huang, S.: Secure color image encryption algorithm based on chaotic signals and its FPGA realization. Int J Circuit Theory Appl **46**, 2444–2461 (2018)
19. Çavuşoğlu, Ü., Panahi, S., Akgül, A., Jafari, S., Kaçar, S.: A new chaotic system with hidden attractor and its engineering applications: analog circuit realization and image encryption. Analog Integr Circuits Signal Process **98**, 85–99 (2019)
20. Zhang, Y., Wang, B.: Optical image encryption based on interference. Opt Lett **33**, 2443 (2008). https://doi.org/10.1364/ol.33.002443
21. Yildirim, M., Kacar, F.: Chaotic circuit with OTA based memristor on image cryptology. AEU - Int J Electron Commun **127**, 153490 (2020). https://doi.org/10.1016/j.aeue.2020.153490
22. Yildirim, M.: A color image encryption scheme reducing the correlations between R, G, B components. Optik (Stuttg) **237**, 166728 (2021). https://doi.org/10.1016/j.ijleo.2021.166728
23. Vaidyanathan, S., Akgul, A., Kaçar, S., Çavuşoğlu, U.: A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography. Eur Phys J Plus (2018). https://doi.org/10.1140/epjp/i2018-11872-8
24. Yildirim, M.: DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon. Microelectronics J **104**, 104878 (2020). https://doi.org/10.1016/j.mejo.2020.104878
25. Saxena, A., Fernandes, F.C.: DCT/DST-based transform coding for intra prediction in image/video coding. IEEE Trans Image Process **22**, 3974–3981 (2013)
26. Makbol, N.M., Khoo, B.E.: Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU-Int J Electron Commun **67**, 102–112 (2013)
27. Valandar, M.Y., Ayubi, P., Barani, M.J.: A new transform domain steganography based on modified logistic chaotic map for color images. J Inf Secur Appl **34**, 142–151 (2017). https://doi.org/10.1016/j.jisa.2017.04.004
28. Liu, B., Xiang, H., Liu, L.: Reducing the dynamical degradation of digital chaotic maps with time-delay linear feedback and parameter perturbation. Math Probl Eng (2020). https://doi.org/10.1155/2020/4926937
29. Liu, L., Miao, S.: Delay-introducing method to improve the dynamical degradation of a digital chaotic map. Inf Sci (Ny) **396**, 1–13 (2017). https://doi.org/10.1016/j.ins.2017.02.031
30. Si-Mohamed, S., Chebib, N., Sigovan, M., Zumbihl, L., Turquier, S., Boccalini, S., et al.: In vivo demonstration of pulmonary microvascular involvement in COVID-19 using dual-energy computed tomography. Eur Respir J (2020). https://doi.org/10.1183/13993003.02608-2020
31. Rezk, A.A., Madian, A.H., Radwan, A.G., Soliman, A.M.: Multiplierless chaotic pseudo random number generators. AEU-Int J Electron Commun **113**, 152947 (2020)
32. Ismail, S.M., Said, L.A., Rezk, A.A., Radwan, A.G., Madian, A.H., Abu-Elyazeed, M.F., et al.: Generalized fractional logistic map encryption system based on FPGA. AEU-Int J Electron Commun **80**, 114–126 (2017)
33. Kim, L.-W.: DeepX: Deep learning accelerator for restricted Boltzmann machine artificial neural networks. IEEE Trans Neural Networks Learn Syst **29**, 1441–1453 (2017)
34. Zhang GL, Leong PHW, Ho CH, Tsoi KH, Cheung CCC, Lee D-U, et al. Reconfigurable acceleration for Monte Carlo based financial simulation. Proceedings. 2005 IEEE Int. Conf. Field-Programmable Technol. 2005., IEEE; 2005, p. 215–22
35. Varnan, C.S., Jagan, A., Kaur, J., Jyoti, D., Rao, D.S.: Image quality assessment techniques in spatial domain. Int J Comput Sci Technol **2**, 177–184 (2011)
36. Hua, Z., Xu, B., Jin, F., Huang, H.: Image encryption using josephus problem and filtering diffusion. IEEE Access **7**, 8660–8674 (2019). https://doi.org/10.1109/ACCESS.2018.2890116
37. Hamza, R., Titouna, F.: A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Inf Secur J **25**, 162–179 (2016). https://doi.org/10.1080/19393555.2016.1212954
38. Khan, J.S., Ahmad, J.: Chaos based efficient selective image encryption. Multidimens Syst Signal Process **30**, 943–961 (2019). https://doi.org/10.1007/s11045-018-0589-x
39. Ye, R.: A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt Commun **284**, 5290–5298 (2011). https://doi.org/10.1016/j.optcom.2011.07.070
40. Zhang, Q., Guo, L., Wei, X.: Image encryption using DNA addition combining with chaotic maps. Math Comput Model **52**, 2028–2035 (2010)
41. Wei, X., Guo, L., Zhang, Q., Zhang, J., Lian, S.: A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw **85**, 290–299 (2012)
42. Liu, H., Wang, X.: Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl **59**,

3320–3327 (2010). https://doi.org/10.1016/j.camwa.2010.03.017
43. Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M.: Hash key-based image encryption using crossover operator and chaos. Multimed Tools Appl **75**, 4753–4769 (2016)
44. Norouzi, B., Seyedzadeh, S.M., Mirzakuchaki, S., Mosavi, M.R.: A novel image encryption based on hash function with only two-round diffusion process. Multimed Syst **20**, 45–64 (2014)
45. Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M.: A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dyn **83**, 1123–1136 (2016). https://doi.org/10.1007/s11071-015-2392-7
46. Kanso, A., Ghebleh, M.: A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul **17**, 2943–2959 (2012)
47. Zhang, Y.: The image encryption algorithm based on chaos and DNA computing. Multimed Tools Appl **77**, 21589–21615 (2018). https://doi.org/10.1007/s11042-017-5585-x
48. Yu, W., Liu, Y., Gong, L., Tian, M., Tu, L.: Double-image encryption based on spatiotemporal chaos and DNA operations. Multimed Tools Appl **78**, 20037–20064 (2019). https://doi.org/10.1007/s11042-018-7110-2
49. Liu, L., Zhang, Q., Wei, X.: A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng **38**, 1240–1248 (2012). https://doi.org/10.1016/j.compeleceng.2012.02.007
50. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process **92**, 1101–1108 (2012). https://doi.org/10.1016/j.sigpro.2011.10.023