Multimedia Tools and Applications (2019) 78: 9971–9989
https://doi.org/10.1007/s11042-018-6584-2

An integer wavelet transform image steganography method based on 3D sine chaotic map

Milad Yousefi Valandar[1] · **Milad Jafari Barani**[1] · **Peyman Ayubi**[2] · **Maryam Aghazadeh**[2]

Received: 29 August 2017 / Revised: 8 July 2018 / Accepted: 21 August 2018 /
Published online: 1 September 2018

Abstract

Steganography is one of the well-known data hiding methods, which is used in many security companies and government communications. In this technique, the various types of digital media can be used as a cover to hide secret information without impress the general form of them. Generally, key space and security are two important matters in most steganography methods, and they have the direct impact in proposed method's security. Moreover, Chaotic maps have been used in many data hiding algorithms to increase the security and key space of proposed schemes. The main reasons of using chaotic maps in steganography methods are sensitivity to initial conditions and control parameters. This paper proposes a new steganography technique based on new 3d sine chaotic map. This map is used in embedding and extracting processes to increase the security of the proposed algorithm. Satisfactory performance, acceptable image distortion and stronger robustness against some attacks are the main features of proposed method, and they are shown in experimental results. Comparison with some existing method shows that the quality and performance of the proposed algorithm are good, and it has high security and acceptable robustness against cropping and salt & pepper attacks.

Keywords Color image steganography · Integer wavelet transform · Sine chaotic map · Data hiding

✉ Milad Yousefi Valandar
milad_yousefi@hotmail.com

Milad Jafari Barani
milad.jafare@gmail.com

Peyman Ayubi
p.ayubi@iaurmia.ac.ir

Maryam Aghazadeh
maryam_aghazadeh@hotmail.com

[1] Young Researchers and Elite Club, Urmia Branch, Islamic Azad University, Urmia, Iran

[2] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

1 Introduction

The most important issue in human's life is extending the variety of digital data. This problem is significantly increased day by day. Generally, large amounts of data are used in government or private agencies, medical centers and military's communications. On the other hand, each person has specific data, which include very important information about his/her private stuffs. However, it is a remarkable point to provide the security of these data as much as possible.

Usually, images, videos and audios are the most popular digital data, and more people use them. They are shared in many social networks and no one's paying attention to their security [41]. Nevertheless, difference methods have been proposed to enhance the security of digital data. The categories of proposed methods are based on their applications and robustness against attacks. On the other hand, digital data are considered as a cover to hide important information or secret messages. For example, important messages hide inside the other data in military or security systems. This process did not change the quality of covers, and it is hard to detect actual messages by the others. Different types of methods have been proposed to hide important information which cryptography, watermarking and steganography are the most well-known methods. In cryptography techniques, data is usually shuffled with special keys, and only the sender and receiver are able to reconstruct the data with same keys [1, 45]. In these methods, data protects themselves from attacks. Many image encryption methods have been proposed [5, 12, 16, 24, 25] for digital data which some of them are discussed in the following. Zhang Leihong et al. proposed a high-performance cryptography for large images in [23]. In this method, the sender encrypted image with Fast Fourier Transform and then this image encrypted again by the system of compressive ghost imaging (CGI). Likewise, the receiver decrypted image by FFT and compressive sensing (CS). The results of simulation showed the performance, security and combination of CS, and FFT improved the security of proposed method against chosen-plain text attack, cipher-text attack and noise attack. In [20], Manish Kumar et al. suggested a new data encryption method based on position substitution, shuffling and a diffusion process. This method generated a 3D matrix for finding the position of a text symbol and then this position shuffled by encryption key. Matrix generation and position shuffling are done by logistic chaotic map. The integrity of cipher text checked by its parity in the encrypted form. Simulation results demonstrate remarkable robustness of the proposed scheme against statistical attacks. Ting Hu et al. proposed an image cryptography based on chaotic map and a DNA sequence in [15]. Proposed approach employed the Logistic-Sine system (LSS) in the coupled map lattice (CML) to generate sequences with better chaotic characteristics. This algorithm diffused images with unique chaotic key, and the insertion of DNA is used to confuse DNA encode. Experimental results demonstrated the acceptable speed of proposed method and good robustness against some recognized attacks. Akram Belazi et al. presented an image encryption scheme based on a chaotic map [4]. Proposed scheme used substitution-boxes, linear fractional transform and lifting wavelet transform to encrypt the sensitive parts of images. Proposed algorithm used dynamic keys instead of fixed key to control the encryption process and make any attacks impossible. Extensive experiments showed the high performance and great potential of proposed approach.

In watermarking methods, the watermarks are embedded inside digital media to protect them against many illegal manipulations. Usually, watermarks are the composition information of owners. Difference types of watermarking methods have been proposed in [3, 6, 34, 39, 40]. Chuan Qin et al. proposed a new fragile watermarking method based on overlap-

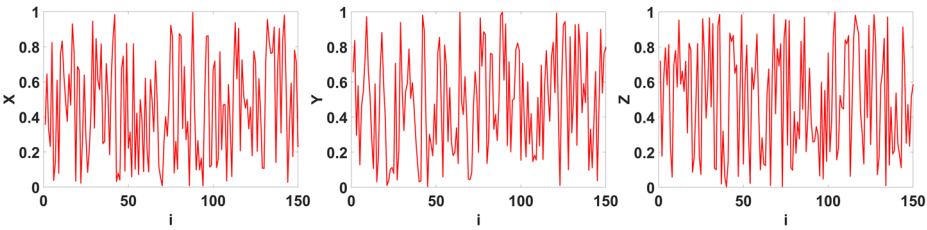


Fig. 1 Time series of 3d sine map for x_i (left), y_i (middle) and z_i (right)

ping strategy in [35]. This method used the block-wise mechanism and the pixel-wise for tampering localization and content recovery, respectively. This method embedded authentication bits into pixel's least significant bits (LSB), then used these bits to find forged parts. The results of tests demonstrated the capability of proposed method in localizing forged areas. M. Moosazadeha and G. Ekbatanifard presented a digital image watermarking algorithm [28]. Proposed technique used YCoCg-R color space to increase the robustness of the suggested algorithm against various attacks. Proposed method also utilized discrete cosine transform and the coefficient of relationship in embedding process. In this method, the blocks' complexities in the host image are calculated to select embedding blocks, and increased the resistance of the proposed scheme against JPEG compression. Comparison with similar techniques showed good performance of proposed method in imperceptibility, robustness and capacity of proposed approach. L. Chen and J. Zhao suggested a new blind watermarking scheme for depth-image-based rendering (DIBR) 3D images in [8]. They used contourlet transform in embedding and extracting processes. The simulation results illustrated that the proposed method has acceptable robustness against noise addition, image compression, geometric attacks and good performance in terms of depth image variation. Zhuhong Shao et al. presented a robust watermarking technique based on chaotic map and orthogonal Fourier-Mellin moments. This method contained ownership registration phase and verification phase. In this method, a binary future of image is calculated with orthogonal Fourier-Mellin moments, and chaotic map generated the verification of image. Experimental results illustrated acceptable validity and security of proposed method against difference attacks.

Steganography is the art of hiding a secure message inside different types of digital media. The actual challenge in this technique is hiding important data in a cover without destroy any parts of cover. Generally, many special steganography methods have been proposed for different messages and covers [21, 22, 26, 33, 44]. Images are the most popular covers in the steganography techniques. Generally, spatial domain and transform domain steganography are the most well-known techniques in image steganography methods. The spatial domain schemes embed the bits of secure message in cover bits directly [7, 30, 31]. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) are the most well-known transforms, that used in transform domain methods. These transforms apply on cover and stego images to improve the visual quality of methods in embedding and extracting processes. Generally, proposed approaches used difference way to enhance the robustness. For example, some schemes use transforms, chaos maps or combined methods. M. Ghebleh and A. Kanso introduced a steganography method based on 3D chaotic cat map and lifted discrete wavelet transforms [11]. This method used Sweldens lifting scheme to ensure integer-to-integer transform. The experimental results

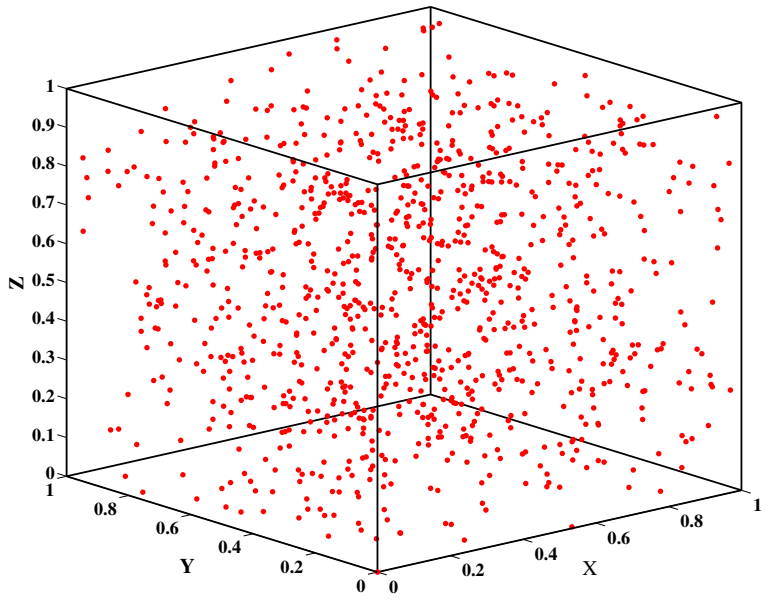


Fig. 2 The attractor of 3d sine map, for $i = 1, \ldots, 5000$

demonstrated the efficiency and flexibility of proposed method. Mehdi Hussain et al. presented a new data hiding method for digital images in [17]. Proposed method used the difference values between pixels in each block to determine the selection of parity-bit pixel value difference (PBPVD) and improved rightmost digit replacement (iRMDR). Experimental results determined good visual quality and high robustness against RS and histogram analysis attacks. R. González et al. suggested a new method for images steganography in [27]. This paper used Bernoulli chaotic maps and the least significant bit technique in embedding and extracting processes. In this method, secure message bits are encrypted, and they are embedded in random RGB channels. The experimental results showed good improvement in the image fidelity, and peak signal to noise ratio (PSNR).

The remaining part of this paper is organized as follows: The chaotic map is described in Section 2. Section 3 presents proposed steganography method. Performance evaluation and experimental results of the proposed method are presented in Section 4. The comparison results of proposed method with other algorithms are investigated in Section 5. Finally, Section 6 concludes this paper.

2 Extraction of 3D sine map

Sensitivity to initial conditions and control parameters are the main features of chaotic maps. These features have been used in many security systems and methods. Generally, to create chaotic behaviors the simple linear or non-linear equations are used. For example, logistic map is one of the well-known chaotic map. This map is very simple, fast and it has some

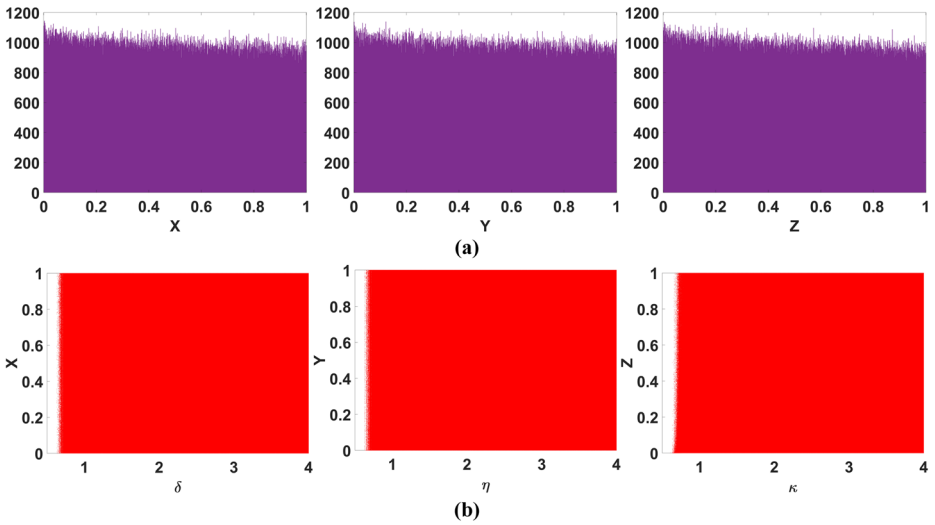


Fig. 3 Histogram analysis and bifurcation of 3d sine map, **a** Histogram analysis, **b** Bifurcation diagrams

unique properties. Sine map is another simple map that has chaotic behaviors and it is very similar to logistic map [14]. The classical form of this map is defined by:

$$x_{n+1} = \mu sin(\pi x_n) \tag{1}$$

where $\mu > 0$ and it is control parameter, x_0 is initial condition and it is in interval [0,1]. This map has a control keys and one dimension, so it isn't good to use in color images. In order to increase the key space of this map and its dimension, this paper introduced a new three dimensional sine map. In the first steps, the ϕ_1, ϕ_2 and ϕ_3 functions are defined by following equation:

$$\begin{cases} \phi_1(x_n, y_n) = sin(\pi\, x(1-y)) \\ \phi_2(y_n, z_n) = sin(\pi\, y(1-z)) \\ \phi_3(z_n, x_n) = sin(\pi\, z(1-x)) \end{cases} \tag{2}$$

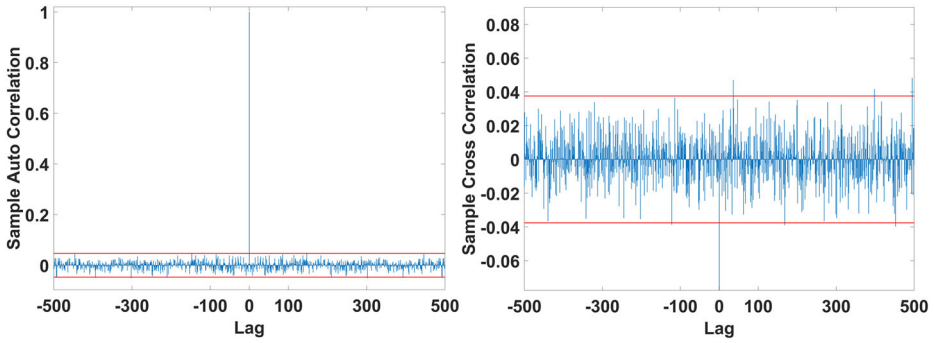


Fig. 4 Cross correlation between sequences x_i, y_i (right) and auto correlation of sequence x_i (left)

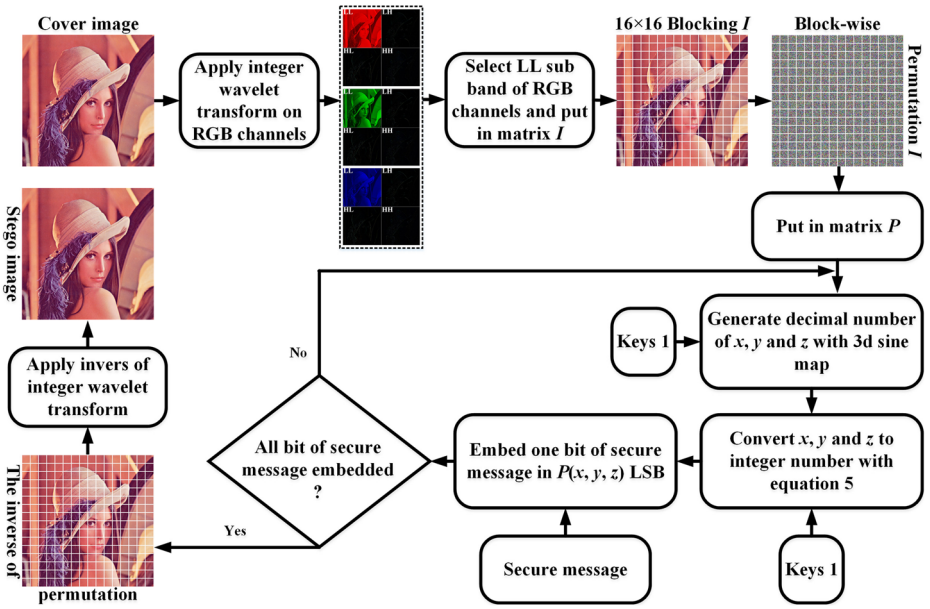


Fig. 5 The diagram of embedding phases in proposed steganography method

In the next step, δ, η and κ control keys are added to increase the key space. New functions are calculated by:

$$\begin{cases} x_{n+1} = \delta \frac{\phi_1(x_n, y_n)}{\phi_2(y_n, z_n)} \\ y_{n+1} = \eta \frac{\phi_2(y_n, z_n)}{\phi_3(z_n, x_n)} \\ z_{n+1} = \kappa \frac{\phi_3(z_n, x_n)}{\phi_1(x_n, y_n)} \end{cases} \tag{3}$$

Modulo operation is used in the next step to generate results in interval [0,1]. Finally, the main formula of new three dimensional sine map is defined by:

$$\begin{cases} x_{n+1} \equiv \left[\frac{\delta^3 sin(\pi x_n (1-y_n))}{sin(\pi y_n (1-z_n))} \right] \ mod \ 1 \\ y_{n+1} \equiv \left[\frac{\eta^3 sin(\pi y_n (1-z_n))}{sin(\pi z_n (1-x_n))} \right] \ mod \ 1 \\ z_{n+1} \equiv \left[\frac{\kappa^3 sin(\pi z_n (1-x_n))}{sin(\pi x_n (1-y_n))} \right] \ mod \ 1 \end{cases} \tag{4}$$

where x_0, y_0 and z_0 are initial conditions and they are in interval [0,1]. δ, η and κ are control parameters and they are in interval [1,4]. The simulation results of map show that the power 3 of control keys generate better pseudo random numbers. Figure 1 illustrates the time series of x_i, y_i and z_i $(i = 1, \ldots, 150)$ sequences. The visual representation of attractor for 3d sine map is shown in Fig. 2. Histogram analysis and bifurcation diagram are shown in Fig. 3. These figures show the chaotic behavior of 3d sine map.

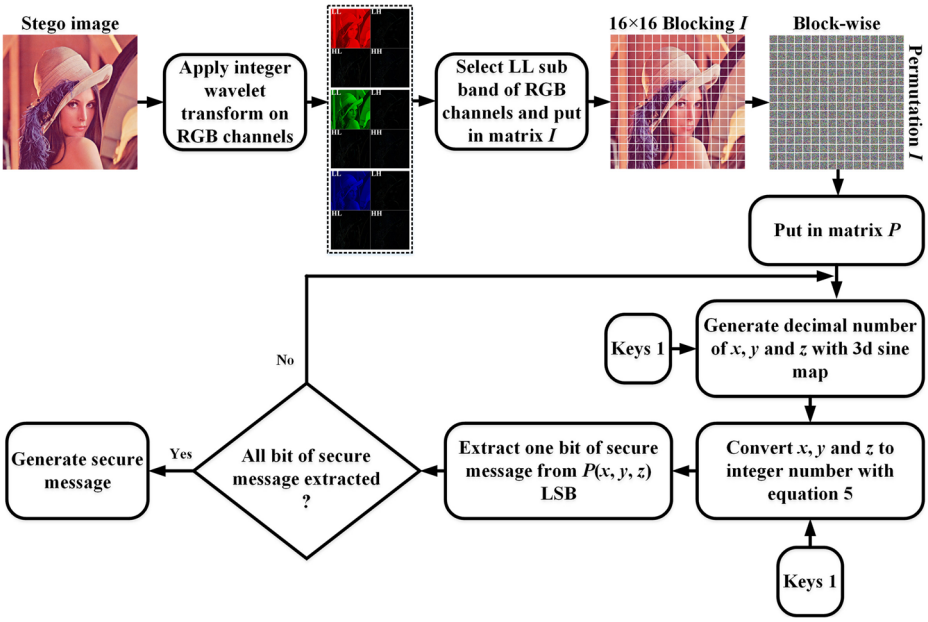


Fig. 6 The diagram of extracting phases in proposed steganography method

Cross correlation and auto correlation are the other tests which used to evaluate the generated sequences by 3d sine map. Cross correlation is the correlations between two sequences, and it shows the best interval for these sequences. The values of this test are between 1 and -1 in standard form. Auto correlation is the correlations between a sequence and itself. Figure 4 shows the results of cross correlation between sequences x_i and y_i, and auto correlation for sequence x_i $(i = 1, \ldots, 2000)$.

ENT, NIST and DIEHARD test suites are the most well-known statistical tests. These tests have been developed to show the randomness properties of pseudo-random number generators. This paper use these tests to investigate the randomness of 3d sine map. Three sequences are generated for x_i, y_i and z_i $(i = 10000000)$, separately. These sequences are saved as bin files and used in ENT, NIST and DIEHARD test suits. The results of these test suites are shown in Tables 1, 2, and 3.

Table 1 ENT test suite of 3d sine map

Test name	P-value		
	x	y	z
Entropy	7.999989	7.999997	7.999993
Arithmetic mean	127.6783	127.3936	127.4903
Monte carlo	3.1415926548	3.1415926352	3.1415926262
Chi-square	267.51	282.37	273.73
Serial correlation coefficient	0.000093	0.000173	0.000043

Table 2 NIST test suite of 3d sine map

Test name	P-value		
	x	y	z
Frequency	0.634773	0.854674	0.567785
Block-frequency	0.375777	0.546766	0.785674
Cumulative-sums (forward)	0.546754	0.587858	0.678564
Cumulative-sums (reverse)	0.458788	0.785678	0.686541
Runs	0.587578	0.857854	0.789842
Longest-runs	0.546734	0.784763	0.467478
Rank	0.619782	0.784849	0.678458
FFT	0.757854	0.536347	0.678578
Non-overlapping-templates	0.864736	0.635783	0.776763
Overlapping-templates	0.567327	0.578473	0.767836
Universal	0.562375	0.456734	0.634767
Approximate entropy	0.436467	0.484785	0.678464
Random-excursions	0.784578	0.567588	0.754673
Random-excursions variant	0.845784	0.585478	0.596535
Serial 1	0.567851	0.747347	0.673632
Serial 2	0.723519	0.622257	0.795421

3 Proposed steganography method

This section presents a new digital image steganography. The main processes of proposed steganography are embedding and extracting processes. Embedding process contains seven phases. In phase one, a cover image with size $M \times N \times K$ and secure message with size $a \times b$ enter in the algorithm. Phase two applies integer wavelet transform on RGB channels of cover image and puts the LL sub bands on matrix I. Blocking process is started in phase three and algorithm divides matrix I into 16×16 non-overlapping blocks. The block-wise permutation is performed in phase four and then algorithm puts the permuted blocks in matrix P. Permutation process is used to increase the security of proposed approach. In phase five, 3d sine map uses keys 1 (x_0, y_0, z_0, δ, η and κ) to generate random decimal numbers by (4) and algorithm changes these numbers to integer form by (5) and key 2 (ω, σ and θ). In phase six, the output numbers of (5) are used as a coordinate and color channel in matrix P to embed the bits of secure message. These steps (phase five and phase six) are repeated until the proposed algorithm embeds all bits of hidden message. Proposed algorithm performs the inverse of block-wise permutation in phase seven and finally, algorithm applies the inverse of integer wavelet transform to generate stego image. The steps of embedding process are shown in Fig. 5. Proposed algorithm uses a mask matrix to prevent selecting pixels that have already been embedded.

$$\begin{cases} x_{n+1} \equiv 1 + mod\,(\omega \times x_n \times 10^{14}, M) \\ y_{n+1} \equiv 1 + mod\,(\sigma \times y_n \times 10^{14}, N) \\ z_{n+1} \equiv 1 + mod\,(\theta \times z_n \times 10^{14}, K) \end{cases} \tag{5}$$

Table 3 DIEHARD test suite of 3d sine map

Test name	P-value		
	x	y	z
Birthday spacing	0.546556	0.623562	0.435636
Overlapping permutation	0.572362	0.463465	0.567473
Binary rank	0.637347	0.435625	0.563457
Bitstream	0.456778	0.514673	0.447568
OPSO	0.356257	0.346235	0.347673
OQSO	0.365835	0.626525	0.567884
DNA	0.475481	0.546847	0.467848
Count the ones	0.367324	0.435734	0.574579
Parking lot	0.346756	0.367346	0.568547
Minimum distance	0.546736	0.475489	0.579256
3DS spheres	0.627934	0.580245	0.589207
Squeeze	0.235637	0.375591	0.402486
Overlapping sum	0.573468	0.495427	0.368025
Runs	0.467803	0.358246	0.483682

Extracting process includes six phase, which in phase one, stego image enters in extracting algorithm. Phase two applies integer wavelet transform on RGB channels of stego image and puts the LL sub bands on matrix I. In phase three, extracting algorithm divides matrix I into 16×16 non-overlapping blocks. The block-wise permutation is performed in phase four and algorithm puts the permuted blocks in matrix P. Proposed scheme permute the blocks of stego image to find the exact location of embedded pixels. In phase five, 3d sine map uses keys 1 to generate random decimal numbers by (4) and changes these numbers to integer form by (5) and keys 2 (Keys 1 and Keys 2 are same in embedding and extracting

Table 4 PSNR and SSIM results of proposed steganography with the number of color channels

Cover	Messages									
	77244 bits					9744 bits				
	PSNR	SSIM	Channels			PSNR	SSIM	Channels		
			R	G	B			R	G	B
Lena 1024×1024	53.76495	0.999642	25903	25637	25704	54.18924	0.999836	3285	3209	3250
Baboon 1024×1024	52.89769	0.999856	25685	25811	25748	53.22105	0.999949	3160	3257	3327
Peppers 1024×1024	54.78124	0.999691	25726	25874	25644	53.20573	0.999871	3260	3171	3313
Airplane 1024×1024	53.84573	0.999471	25635	25953	25656	52.90362	0.999603	3289	3136	3319
Lena 512×512	51.37613	0.998472	25872	25788	25584	51.18524	0.999617	3277	3205	3262
Baboon 512×512	52.42284	0.999189	25651	25805	25788	52.27376	0.999876	3329	3244	3171
Peppers 512×512	52.39078	0.998615	25692	25845	25707	52.21909	0.999694	3161	3350	3233
Airplane 512×512	51.98463	0.998058	25732	25406	26106	51.98378	0.999769	3240	3427	3077

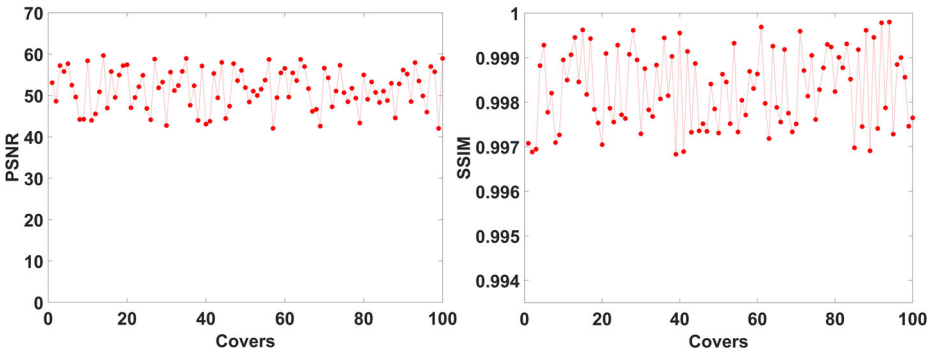


Fig. 7 The results of PSNR and SSIM measures for 100 cover images after embedding secure message

processes). In phase six, the output numbers of (5) are used as a coordinate and color channel in matrix P to extract the bits of secure message. Phase five and phase six are repeated until all bits of the secure message extracted. The extracting process is finished by generating secure message. Figure 6 demonstrates the extracting process of proposed technique. Mask matrix is used in extracting algorithm to avoid selecting pixels that have already been extracted.

4 Experimental results

The important issues in proposing new methods are examining the results of tests and the robustness of proposed methods against attacks. This paper uses some standard pictures like Lena, Peppers and Baboon with different hiding messages to evaluate the proposed method in embedding processes. The results of tests are calculated by using AMD Phenom II x4 processor, 8GB RAM, Linux Ubuntu 16 x64 OS and MATLAB R2016b x64 software.

4.1 PSNR and SSIM measures

Peak Signal to Noise Ratio (PSNR) and structural similarity index (SSIM) are two well-known measures, which used to compare differences between original images and the changed form of them. The results of PSNR show the visual quality of cover images after embedding process. PSNR is calculated by following equation:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{6}$$

where MAX_I is the value of possible pixel in the cover images. MSE is the mean square error and it is defined by:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - St(i,j)]^2 \tag{7}$$

where C and St are cover image and stego image, respectively. m and n are the size of cover image. SSIM predicts the perceived quality of images and measures the similarity of cover

Table 5 SSIM, BER and NCC values of extracted Baboon from attacked stego

Attack	Lena			Peppers			Baboon			Airplane		
	SSIM	BER	NCC	SSIM	BER	NCC	SSIM	BER	NCC	SSIM	BER	NCC
Resize [1024 1024]	0.7518	0.0145	0.9748	0.7628	0.0127	0.9782	0.8527	0.0154	0.9854	0.7621	0.0137	0.9734
Rotate (45°)	0.7634	0.0157	0.9597	0.6975	0.0152	0.9251	0.7714	0.0131	0.9755	0.7234	0.0152	0.9537
Sharpen	0.6728	0.0185	0.8908	0.6239	0.0181	0.8934	0.6947	0.0191	0.9584	0.6194	0.0189	0.8927
Blur	0.8143	0.0172	0.9651	0.7762	0.0163	0.9761	0.8639	0.0149	0.9892	0.7726	0.0134	0.9875
Gaussian noise (0,0.0001)	0.6925	0.0164	0.9582	0.6794	0.0137	0.9659	0.7015	0.0128	0.9623	0.6842	0.0149	0.9462
Speckle noise (0.02)	0.7194	0.0141	0.9625	0.6935	0.0158	0.9421	0.7683	0.0132	0.9758	0.6914	0.0173	0.9539
Median filter [3 3]	0.7907	0.0135	0.9749	0.7537	0.0134	0.9724	0.8519	0.0169	0.9806	0.7538	0.0157	0.9756
Wiener filter [3 3]	0.7936	0.0187	0.9754	0.7542	0.0149	0.9715	0.8537	0.0151	0.9879	0.7662	0.0138	0.9781
Shear	0.7459	0.0124	0.9682	0.6971	0.0167	0.9571	0.7329	0.0135	0.9746	0.7251	0.0142	0.9653
Histogram equalization	0.7394	0.0145	0.9673	0.6729	0.0132	0.9319	0.7958	0.0124	0.9857	0.7196	0.0139	0.9649
Translate [2 2]	0.7573	0.0142	0.9729	0.7318	0.0157	0.9648	0.8197	0.0162	0.9745	0.7457	0.0146	0.9686
Jpeg compression (QF=75)	0.7682	0.0147	0.9667	0.7442	0.0124	0.9663	0.8324	0.0146	0.9851	0.7429	0.0135	0.9728

image and stego image. The results of SSIM are defined by:

$$SSIM(I_1, I_2) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{8}$$

where σ_x and σ_y are the mean intensities of x and y, σ_x^2 and σ_y^2 are the variances of x and y, σ_{xy} is the co-variance of x and y, respectively. The averages of x and y are μ_y and μ_x, C_1 and C_2 are the variables to stabilize the division with weak denominator. The results of PSNR and SSIM measures after embedding different size of messages are shown in Table 4. This table also demonstrates the number of channels (RGB) that used in embedding process. The sizes of channels are almost same and show the proposed technique uses all channels of cover image in embedding secure messages. Figure 7 illustrates the PSNR and SSIM measures of 100 cover images after embedding secure message.

4.2 Robustness against attacks

The considerable parameter of proposing a steganography method is robustness against attacks. Generally, steganography hides a secure message in cover image and it can happen that some parts of cover image destroyed accidentally or changed by the attackers. According to these problems, proposed method should be resisted against any destruction. To test the robustness of proposed method, this section first embeds Baboon (256×256) image as a secure message in Lena and Peppers images, then apply cropping attack and salt & peppers noise on stego images. Figure 8 shows the reconstructed secret message after these attacks. This paper uses SSIM, BER and NCC measures to calculate the destruction of secure message after extracting it from attacked stego images. The results of these measures are shown in Table 5. In this table cover images are 512×512 and message (Baboon) is 256×256. According to the results, proposed method can be resist against some image processing attacks.

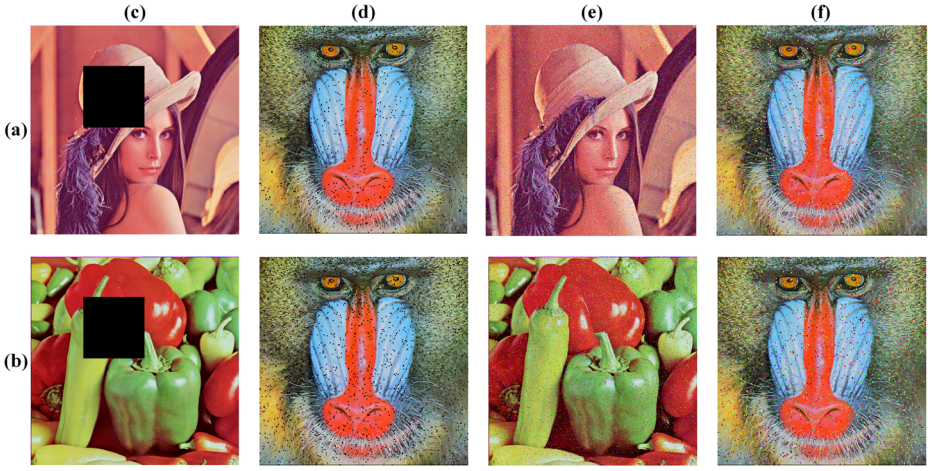


Fig. 8 Extracted Baboon secret message from stego images after Cropped and Salt & peppers noise attacks, **a** Lena 1024×1024, **b** Peppers 512×512, **c** Crop 100×100, **d** Extracted secure image after crop attack, **e** Salt & peppers noise ($parameter = 0.02$), **f** Extracted secure image after salt & peppers noise attack

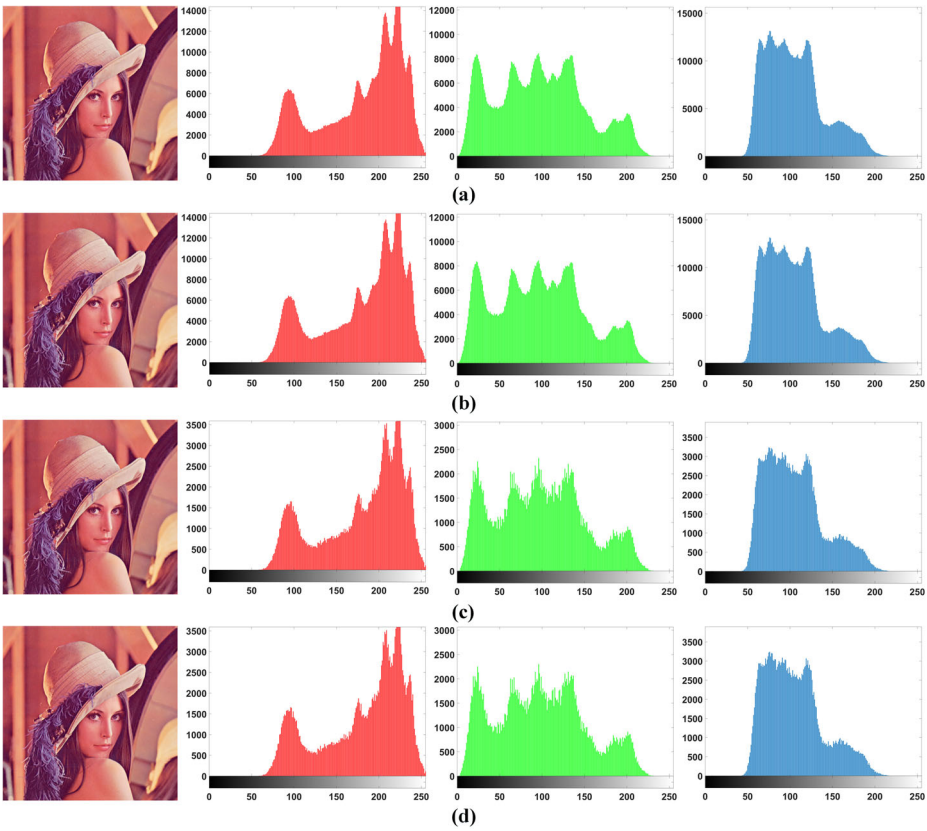


Fig. 9 Histogram analyses for RGB channels, **a** Cover image (Lena 1024 × 1024), **b** Stego image after embedding 77244 bits, **c** Cover image, (Lena 512 × 512), **d** Stego image after embedding 9744 bits

4.3 Histogram analysis

Image histogram is an useful tool in image processing field that used to show the number of pixels in images and their intensity values. In images steganography, histogram is used to investigate cover images after embedding process and it shows the distribution of secure message in cover images' channels. This paper embeds 77244 bits and 9744 bits in two different sizes of cover image to compare the results of histogram. The comparison results are shown in Fig. 9. This figure shows that the histograms of each cover image are very similar with their stego images and the distortion of Lena image is acceptable after embedding different size of secure messages.

4.4 Key space analysis

Key space is the important part of encryption methods and shows the capability of methods against brute force attack. The key space of proposed algorithm contains two different parts. First part is the keys which used in the new 3d sine map. The initial conditions of this map are three double keys (x_0, y_0, z_0) and the size of each initial key is 10^{-14}. The computational precision of control parameters (δ, η and κ) are 3×10^{-14}. Therefore, the general key space

Table 6 Comparison of proposed method with other color images schemes

Images	CLSB method		[2]		[13]		[18]		[29]		[31]		Proposed method	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
F 16	47.4882	0.9976	47.4852	0.9985	45.6879	0.9964	40.2347	0.9797	47.4902	0.9985	53.1665	0.9985	53.7294	0.9999
Building	28.8451	0.9963	28.8451	0.9973	28.8213	0.9948	40.2552	0.9765	28.8451	0.9972	43.4071	0.9973	43.8097	0.9989
Baboon	51.1648	0.9989	48.9531	0.9993	46.5568	0.9985	39.9997	0.9925	48.9536	0.9992	47.8747	0.9992	48.5478	0.9998
House	51.1659	0.9983	51.1776	0.999	47.6956	0.9974	40.2518	0.986	51.1564	0.9989	52.7303	0.9989	53.2479	0.9997
Trees	39.0436	0.9964	38.5418	0.997	38.2702	0.9956	39.5397	0.9858	38.5421	0.997	49.7496	0.997	49.8697	0.9998
Masjid	30.6466	0.9843	28.5361	0.9828	28.5173	0.981	39.6331	0.9881	28.5363	0.9828	44.7425	0.9828	46.5871	0.9994

Table 7 Comparison of proposed method with other gray scale images schemes

Method	Secret size	Cover image	PSNR	SSIM	NCC
Su et al. [38]	32 × 32	Lena	36.3521	0.9889	1
		Airplane	36.3160	0.9856	1
		Peppers	36.6869	0.9682	1
Thabit et al. [43]	49152 bits	Lena	43.29	–	–
		Airplane	40.27	–	–
		Baboon	34.33	–	–
		Peppers	41.71	–	–
Sajasi et al. [36]	256 × 256	Lena	47.78	–	–
		Baboon	49.98	–	–
Kanan et al. [19]	256 × 256	Lena	45.12	–	–
		Airplane	45.18	–	–
		Peppers	45.13	–	–
		Baboon	45.12	–	–
Subhedar et al. [42]	256 × 256	Lena	49.0369	0.9963	0.9996
		Airplane	49.2608	0.9971	0.9997
		Peppers	50.1480	0.9966	0.9997
		Baboon	37.7031	0.9917	0.9966
		Splash	54.8019	0.9975	0.9996
Proposed method	256 × 256	Lena	53.2145	0.9981	0.9995
		Airplane	52.6841	0.9992	0.9998
		Peppers	53.0574	0.9995	0.9991
		Baboon	52.9524	0.9986	0.9987
		Splash	53.1447	0.9989	0.9993

of 3d sine map is $3 \times 46 + 3 \times 48 = 282$ bits. Second part of key space is the control parameters (ω, σ and θ) which used in (5). The total key space of these parameters is 138 bits. According to these parts, we can conclude the main key space of proposed steganography is $282 + 138 = 420$ bits. This key length is large enough to defeat brute force attacks.

5 Comparison with similar methods

This article selects two types of existing method to compare with proposed steganography. First types of articles choose color images from Internet and public dataset like USC-SIPI-ID [9]. Table 6 demonstrates the comparison results of PSNR and SSIM between proposed method and existing method. In this table message size is 8 kb. Seconed types of methods have used transforms and gray scale images in embedding and extracting process. The grayscale images that used for comparison are in UCID database [37]. Table 7 illustrates the comparison results of PSNR, SSIM and NCC between proposed method and similar methods. This paper compares the key space of proposed methods with similar steganography methods in Table 8. The results of these tables show that the proposed method has

Table 8 Key space comparison of the proposed method with other schemes

Method	Key length (bits)	Key space
Parah et al. [32]	57	2^{57}
Hennawy et al. [10]	128	2^{128}
Muhammad et al. [31]	216	2^{216}
Proposed method	420	2^{420}

good performance after embedding secure message in two types of images and key space of presented algorithm is higher than some existing methods.

6 Conclusion

This paper proposed a new transform domain image steganography method based on 3d sine chaotic map. The chaotic map enhances the security of proposed steganography and increases the key space. The pixels of cover image are selected by the outputs of chaotic map to embed secure message bits. Bifurcation diagram and histogram analysis show the chaotic behavior of 3d sine map and the results of statistical tests present the randomness of this map. Cross correlation and auto correlation show the best interval for generated sequences. However, proposed algorithm uses integer wavelet transforms in embedding and extracting processes, and it is applied on cover and stego images. This transform uses the integer coefficients to increase the capability of proposed method in extracting process. Experimental results show acceptable imperceptibility of proposed method based on PSNR and SSIM measures. Proposed scheme also has large key space and good robustness against some image-processing attacks. Comparison results between proposed algorithm and some existing schemes show that the proposed steganography has good performance and quality in embedding and extracting processes.

Compliance with Ethical Standards

Conflict of interests All authors declare that they have no conflict of interest.

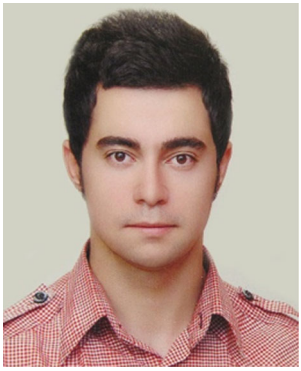
Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Akhavan A, Samsudin A, Akhshani A (2017) Cryptanalysis of an image encryption algorithm based on dna encoding. Opt Laser Technol 95:94–99
2. Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimed Tools Appl 30(1):55–88
3. Barani MJ, Ayubi P, Jalili F, Valandar MY, Azariyun E (2015) Image forgery detection in contourlet transform domain based on new chaotic cellular automata. Secur Commun Netw 8(18):4343–4361
4. Belazi A, El-Latif AAA, Diaconu A-V, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
5. Chai X (2017) An image encryption algorithm based on bit level brownian motion and new chaotic systems. Multimed Tools Appl 76(1):1159–1175
6. Chakraborty S, Chatterjee S, Dey N, Ashour AS, Hassanien AE (2017) Comparative approach between singular value decomposition and randomized singular value decomposition-based watermarking. In: Intelligent techniques in signal processing for multimedia security. Springer, pp 133–149

7. Chen X, Gao G, Liu D, Xia Z (2016) Steganalysis of lsb matching using characteristic function moment of pixel differences. China Commun 13(7):66–73
8. Chen L, Zhao J (2017) Robust contourlet-based blind watermarking for depth-image-based rendering 3d images. Signal Process Image Commun 54:56–65
9. Cheng W-C, Pedram M (2004) Chromatic encoding: a low power encoding technique for digital visual interface. IEEE Trans Consum Electron 50(1):320–328
10. El Hennawy HM, Omar AE, Kholaif SM (2015) Lea: link encryption algorithm proposed stream cipher algorithm. Ain Shams Eng J 6(1):57–65
11. Ghebleh M, Kanso A (2014) A robust chaotic algorithm for digital image steganography. Commun Nonlinear Sci Numer Simul 19(6):1898–1907
12. Ghebleh M, Kanso A, Stevanović D (2017) A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation. Multimedia Tools and Applications 77(6):7305–7326
13. Gutub AA-A et al (2010) Pixel indicator technique for rgb image steganography. J Emerg Technol Web Intell 2(1):56–64
14. Hilborn RC (2000) Chaos and nonlinear dynamics: an introduction for scientists and engineers, Oxford University Press on Demand, Oxford
15. Hu T, Liu Y, Gong L-H, Guo S-F, Yuan H-M (2017) Chaotic image cryptosystem using dna deletion and dna insertion. Signal Process 134:234–243
16. Hu T, Liu Y, Gong L-H, Ouyang C-J (2017) An image encryption scheme combining chaos with cycle operation for dna sequences. Nonlinear Dyn 87(1):51–66
17. Hussain M, Wahab AWA, Ho AT, Javed N, Jung K-H (2017) A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Process Image Commun 50:44–57
18. Jassim FA A novel steganography algorithm for hiding text in image using five modulus method, arXiv:1307.0642
19. Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst Appl 41(14):6123–6130
20. Kumar M, Kumar S, Budhiraja R, Das M, Singh S (2017) A cryptographic model based on logistic map and a 3-d matrix. J Inf Secur Appl 32:47–58
21. Lalitha R, Srinivasu PN (2017) An efficient data encryption through image via prime order symmetric key and bit shuffle technique. In: Computer communication, networking and internet security. Springer, pp 261–270
22. Lee C-F, Weng C-Y, Chen K-C (2017) An efficient reversible data hiding with reduplicated exploiting modification direction using image interpolation and edge detection. Multimed Tools Appl 76(7):9993–10016
23. Leihong Z, Zilan P, Luying W, Xiuhua M (2016) High-performance compression and double cryptography based on compressive ghost imaging with the fast fourier transform. Opt Lasers Eng 86:329–337
24. Li C, Luo G, Qin K, Li C (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dyn 87(1):127–133
25. Li Y, Gai K, Qiu L, Qiu M, Zhao H (2017) Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf Sci 387:103–115
26. Malik A, Sikka G, Verma HK (2017) An image interpolation based reversible data hiding scheme using pixel value adjusting feature. Multimed Tools Appl 76(11):13025–13046
27. Martínez-González RF, Díaz-Méndez JA, Palacios-Luengas L, López-Hernández J, Vázquez-Medina R (2016) A steganographic method using bernoulli's chaotic maps. Comput Electr Eng 54:435–449
28. Moosazadeh M, Ekbatanifard G (2017) An improved robust image watermarking method using dct and ycocg-r color space. Optik-Int J Light Electron Opt 140:975–988
29. Muhammad K, Ahmad J, Sajjad M, Zubair M Secure image steganography using cryptography and image transposition, arXiv:1510.04413
30. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2016) A novel magic lsb substitution method (m-lsb-sm) using multi-level encryption and achromatic component of an image. Multimed Tools Appl 75(22):14867–14893
31. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) Cisska-lsb: color image steganography using stego key-directed adaptive lsb substitution method. Multimed Tools Appl 76(6):8597–8626
32. Parah SA, Sheikh JA, Hafiz AM, Bhat GM (2014) Data hiding in scrambled images: a new double layer security data hiding technique. Comput Electr Eng 40(1):70–82

33. Parah SA, Sheikh JA, Assad UI, Bhat GM (2017) Hiding in encrypted images: a three tier security data hiding technique. Multidim Syst Sign Process 28(2):549–572
34. Parah SA, Sheikh JA, Loan NA, Bhat G (2017) A robust and computationally efficient digital watermarking technique using inter block pixel differencing. In: Multimedia forensics and security. Springer, pp 223–252
35. Qin C, Ji P, Zhang X, Dong J, Wang J (2017) Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Process 138:280–293
36. Sajasi S, Moghadam A-ME (2015) An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method. Appl Soft Comput 30:375–389
37. Schaefer G, Stich M (2004) Ucid: an uncompressed color image database. Storage Retr Methods Appl Multimed 5307:472–480
38. Su Q, Niu Y, Zou H, Zhao Y, Yao T (2014) A blind double color image watermarking algorithm based on qr decomposition. Multimed Tools Appl 72(1):987–1009
39. Su Q, Chen B (2017) Robust color image watermarking technique in the spatial domain. Soft Comput 22(1):91–106
40. Su Q, Wang G, Zhang X, Lv G, Chen B (2017) An improved color image watermarking algorithm based on qr decomposition. Multimed Tools Appl 76(1):707–729
41. Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13:95–113
42. Subhedar MS, Mankar VH (2016) Image steganography using redundant discrete wavelet transform and qr factorization. Comput Electr Eng 54:406–422
43. Thabit R, Khoo BE (2015) A new robust lossless data hiding scheme and its application to color medical images. Digit Signal Process 38:77–94
44. Valandar MY, Ayubi P, Barani MJ (2017) A new transform domain steganography based on modified logistic chaotic map for color images. J Inf Secur Appl 34:142–151
45. Xie EY, Li C, Yu S, Lü J (2017) On the cryptanalysis of fridrich's chaotic image encryption scheme. Signal Process 132:150–154



Milad Yousefi Valandar is a young researcher of computer engineering and security in Islamic Azad University, Iran. He received B.E. and M.Sc. in software engineering from Islamic Azad University, Urmia, Iran. His research interests include digital media security, image and video steganography, image and video watermarking, chaos theory and fractal, hash functions, image encryption and authentication.

Milad Jafari Barani was born in Naqadeh, Iran in 1985. He received B.E. degree in computer engineering from Islamic Azad University, Orumiyeh, Iran, respectively M.Sc. Degree in artificial intelligence in 2014 from Qazvin branch, Islamic Azad University, Qazvin, Iran. His research interests include Information Hiding, Image Authentication, Watermarking and image security.