Multimed Tools Appl (2017) 76:7849–7867
DOI 10.1007/s11042-016-3398-y

A novel method for digital image steganography based on a new three-dimensional chaotic map

Ami Sharif[1] · Majid Mollaeefar[1] · Mahboubeh Nazari[2]

Received: 14 September 2015 / Revised: 13 February 2016 / Accepted: 23 February 2016 /
Published online: 17 March 2016

Abstract This paper, presents a novel chaos-based image steganography algorithm. Because of efficient property of chaos based security systems besides steganography applicability in providing secure communication, chaos based steganography algorithms served as a hot topic in recent researches. The proposed scheme possess novelties and advantageous such as: 1) Introducing a novel 3-dimensional chaotic map (*LCA* map) with strong chaotic characteristics and maximum Lyapunov exponent 20.58, which is used for generating three chaotic sequences, each of them represents the number of row, column, and colour component, respectively. 2) Utilizing random selection procedure for selecting subsequences with length of $2L$, which L is the length of secret message 3) Specifying L pairs of triples host positions for embedding *LSBs* and *MSBs* of secret message by using three high level chaotic maps. 4) Entering some parameters dependent on elementary initial values, host image, and secret message features as a key point for adding additional layer of security alongside providing high sensitivity. 5) Providing high capacity for embedding secret message, which is equal to 50 % of whole image capacity ($\boldsymbol{M}\times\boldsymbol{N}\times 12$). The proposed method could be applied in different criterion such as, confidential communication and data storing, protection of data alteration, and etc. Our experimental results guarantees that our scheme is not only robust against differential attacks, but also has promising results such as highly sensitive keys, Quality index, *PSNR*, *MSE*, and hiding capacity as shown in statistical security analysis.

✉ Majid Mollaeefar
majid.mollaeefar@gmail.com

Ami Sharif
amir-sharif@hotmail.com

Mahboubeh Nazari
ma.am.math@gmail.com

[1] Department of Computer and Information Technology, International University of Imam Reza, Mashhad, Iran

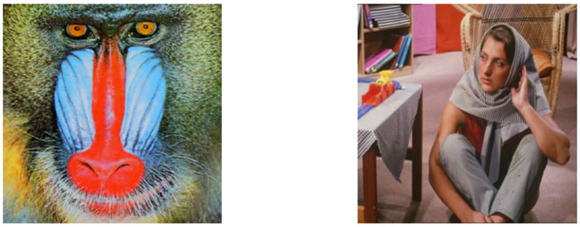
[2] Department of Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran

Keywords Information hiding · LSBs · 3-dimensional chaotic map · Statistical analysis · Imperceptibilty

1 Introduction

Due to the growth of internet connections for transmitting secret data, steganography plays an important role in the secure communications. Therefore, too many studies have been done in this field and it becomes an interesting research field in the information hiding. Indeed, the word steganography is obtained from the Greek words "stegos" means "cover" and "grapha" means "writing", defining it as "covered writing" that hides the existence of the message in itself [23]. Its main idea is to hide secret data in a carrier during communication. Besides, it provides potential for private and secure communication that has become a necessity of most of applications in today's world [6, 7, 13, 14, 18, 19]. The security systems categorized in two types, the first one is "cryptography" and the other one is "information hiding" [4]. The information hiding systems classified into two groups, which entitled "steganography" and "watermarking". The methodologies of watermarking and steganography is the same, but the purpose of these techniques is different [3]. Cryptography and steganography have the same purpose, i.e., to conceal the information message, but they use different methods in order to achieve this aim [5]. Watermarking used for copyright protection of digital data, while steganography used for information hiding. Steganography includes two categories. The first one is "linguistic steganography", which utilize natural language as a carrier for hiding secret data. The other one is "technical steganography", which uses multimedia carrier, such as image, audio and video for embedding secret data. With rising of chaos theory in the recent decades, researchers have used it as a reliable tool in their methods. Sensitivity to primary conditions, non-periodic, non-convergence and controlling parameters are unique properties of chaotic cryptography compared to traditional ones. These characteristics have attracted many researchers to use this tool as a vital solution in their studies. Potdar et al. [17] used a spatial domain technique in producing a fingerprinted secret sharing steganography for robustness against image cropping attacks. They break the image to some sub images and do the same with secret data and finally, put this segmented data in sub images. Shirali-Shahreza et al. [22] proposed a method for steganography based on linguistic methods. They used Persian and Arabic alphabet as a carrier for hiding secret data. Sabery et al. [21] proposed a method for hiding a secret image in a host image by using a simple logistic map. The logistic map used for determining the blocks of pixels that used for embedding process. Kanso et al. [15] proposed a digital image steganography method based on Arnold cat map. Roy et al. [20], presented a chaos based adaptive image steganography, which combines the efficiency of matrix encoding and LSBM to embed data besides using chaos to provide enhanced security. Bilal et al. [10], introduced a novel chaos-based zero-steganography algorithm, which embeds data based on relationship between cover image, chaotic sequence and payload, instead of directly embedding data in cover image. Bandyopadhyay et al. [9], proposed a chaotic method for steganography that encrypt secret bits before embedding procedure by using chaos. Ghebleh and Kanso [12], proposed a robust chaotic algorithm for digital image steganography that used 3-dimensional chaotic cat map alongside discrete wavelet transform. Das and Kar [11], presented a novel DNA-based image steganography that is using 2D chaotic map that used to construct DNA strand from cover image. Alam et al. [1], presented an improved method for image steganography using edge detection besides using logistic map as a secret key random number generation for random LSB substitution. Finally, Anees et al. [3] introduced a steganography technique in spatial domain for digital images based on chaotic maps for resolving pixel positions. Their method has two security shortcomings. First, this scheme does not have a dependency on its secret keys and host image. Therefore, the indices that produced for determining rows, columns, and colour components of carrier pixels are not sensitive to host image. This causes an adversary can use this breach to achieve some useful information about positions of embedded data and break steganography algorithm (Fig. 1). Second, in their method, the host image is first broken into "upper part" and "downer part" respectively to determine the positions of embedded data. This leads an adversary to find a position of embedded data with the help of the other place of them. In fact, he/she can obtain the positions of some embedded data by plus or minus of them with $n/2$, where n, represent the column size of the host image. Hence, these weaknesses exposed their algorithm to known message attack.

We proposed a novel method to overcome these shortcomings, which is not only highly dependent on "secret keys" and "original image", but also it has high-grade results. Indeed, we introduced a novel 3-dimensional chaotic map (*LCA* map) with maximum Lyapunov exponent 20.58. Moreover, by applying *LCA* map, three sequences X, Y and Z with length of more than $2L$ generated, where L is the length of secret message. These chaotic sequences are used for determining the number of rows, columns and color components of carrier pixels, respectively. Afterward, subsequences with a length of $2L$ of generating sequences are intercepted. Next, three high level chaotic maps are used for selection of desirable pairs of triples as host pixel positions for embedding *LSBs* and *MSBs* of secret message. Hence, for each letter of secret message, there are two proper positions that should be converted into binary of eight bits. Then, these bits are segmented into two equal parts. The first part "*MSB*" will remain unchanged and the



Secret Message: 'Alpha team go back to command

Baboon image															
First selected positions (15 positions)	103	206	85	112	2	45	20	68	215	4	65	23	216	1	89
Second selected positions (15 positions)	5	134	54	5	15	9	85	156	234	25	54	196	9	16	234

Barbara image															
First selected positions (15 positions)	103	206	85	112	2	45	20	68	215	4	65	23	216	1	89
Second selected positions (15 positions)	5	134	54	5	15	9	85	156	234	25	54	196	9	16	234

Fig. 1 Effect of no-dependency of initial states to secret message and host image, causes host pixel positions remain unchanged **a** selected positions of Baboon image, **b** selected positions of Barbara image

second part "*LSB*" will be replaced by the first *MSB* bits of secret message. The same procedure will be applied for the second selected pixel position to replace *LSB* bits of secret message. Finally, we convert binary positions into decimal and make steganography image. Our experimental results guarantees that the proposed method is robust against differential attacks and has eligible results such as highly sensitive keys, Quality index, *PSNR*, *MSE*, and hiding capacity.

The paper structure is as follows. Section 2 describes necessary mathematical basics. Our proposed method is explained in Section 3, after that, in Section 4 we come through statistical security analysis and finally, the conclusion is declared in Section 5.

2 High level chaotic maps

2.1 3-dimensional *LCA* map

We introduced a novel 3-dimensional chaotic map (*LCA* map) on interval [0, 1] that possesses strong chaotic characteristics and its maximum Lyapunov exponent is equal to 20.58, where control parameter $\alpha = 0.0001$, $r = 4$, and $N = 4$. The mathematical formula is as below:

$$\boldsymbol{LCA\ map} = \begin{cases} \boldsymbol{x_n} = \dfrac{1}{\alpha^2}\boldsymbol{tan}^2\left(\boldsymbol{N\ arctan}\sqrt{\boldsymbol{y_{n-1}}}\right)\ \boldsymbol{mod}\ 1 \\ \boldsymbol{y_n} = \quad \boldsymbol{r} \quad z_{n-1}\left(1-z_{n-1}\right) \\ z_n = \ 16\ \boldsymbol{x_{n-1}}^5 - 20\ \boldsymbol{x_{n-1}}^3 \ + \ 5\ \boldsymbol{x_{n-1}} \end{cases} \tag{1}$$

Where $\boldsymbol{\alpha} \in [0,\ 1/\boldsymbol{N}]$ and $\boldsymbol{r} \in [3.65, 4]$ are control parameters for *LCA* map. Besides, variables x_{n-1}, y_{n-1}, and z_{n-1} are initial state conditions, which are on the interval [0, 1], respectively. The maximum Lyapunov exponent of *LCA* map for $\alpha \in [0, 0.25]$ (in this case $1/N$ equal to 0.25) and spatiotemporal diagram are shown in Figs. 2 and 3, respectively.

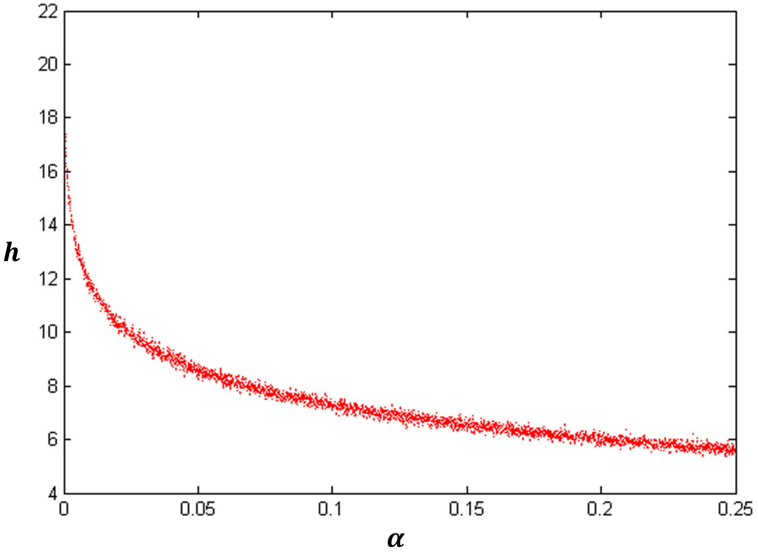


Fig. 2 Lyapunov diagram of *LCA* map for $r = 4$, $N = 4$ and parameter $0 \le \alpha \le 0.25$

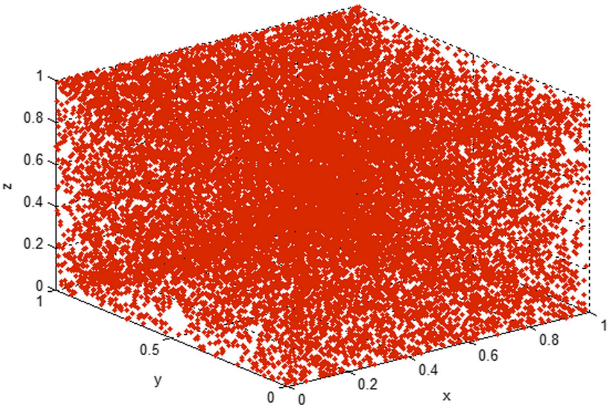


Fig. 3 Spatiotemporal diagram of 3-dimensional *LCA* map for 10000 iteration of initial values ($x_0 = 0.1$, $y_0 = 0.2$, $z_0 = 0.3$), which are in cubic $[0, 1]^3$

In following subsection (2.2, 2,3), in order to specify *L* pairs of triples host positions for embedding *LSBs* and *MSBs* of secret message, we utilized two high level chaotic maps that have been introduced in our previous work [16], besides Chebyshev map.

2.2 The cosines-arcsines system

The “*CA* map” is defined on the interval [0, 1] with the following mathematical formula:

$$X_{n+1} = CA(\gamma,\ X_n) = cos^2\left(\gamma \arcsin\left(\sqrt{|X_n|}\ \right)\right) \tag{2}$$

Where γ, is a control parameter in a range (0, 4) and X_n is initial state condition, which is in the interval [0, 1]. Moreover, in parameter value $\gamma = 3.976$ Lyapunov exponent has maximum value $\lambda = 1.38$.

2.3 The sinus-power logistic system

The “*SPL* map” is defined on interval [-0.48, 0.48]. Moreover, in parameter value $\beta = 3.465$ Lyapunov exponent has maximum value $\lambda = 1.518$. The mathematical formula of this chaotic map is as below:

$$X_{n+1} = SPL(\beta, X_n) = sin^2\left(\beta arcsin\left(\sqrt{|X_n|}\right)\right) + (1-\beta)2(|X_n|)\left(1-2\left|X_n\right|\right) \tag{3}$$

Where β is control parameter in the range (0, 3.5) and X_n is initial state condition with a range (-0.48, 0.48).

2.4 Chebyshev map

The last chaotic map that used in this scheme is “Chebyshev map”, which is defined on interval [-1, 1]. The mathematical formula of this map is as below:

$$x_{n+1} = Chebyshev(k, x_n) = \cos(k(\arccos(x_n))) \tag{4}$$

Where k is control parameter and X_n is an initial state condition that lies in interval [-1, 1]. Furthermore, this map has chaotic behaviour for $\boldsymbol{k} \geq 2$ and its Lyapunov exponent is equal to $\ln \boldsymbol{k}$.

3 Proposed method

Two main phases of proposed scheme are embedding and extraction phases, which are described in detailed as follows:

3.1 Embedding phase

The overall view of proposed method shown in Fig. 4. In order to make our scheme highly dependent on all of its secret keys and original image, we define four parameters as stated below:

$$L_M = \frac{1}{L} \sum_{i=1}^{L} MSB_i \tag{5}$$

$$L_L = \frac{1}{L} \sum_{i=1}^{L} LSB_i \tag{6}$$

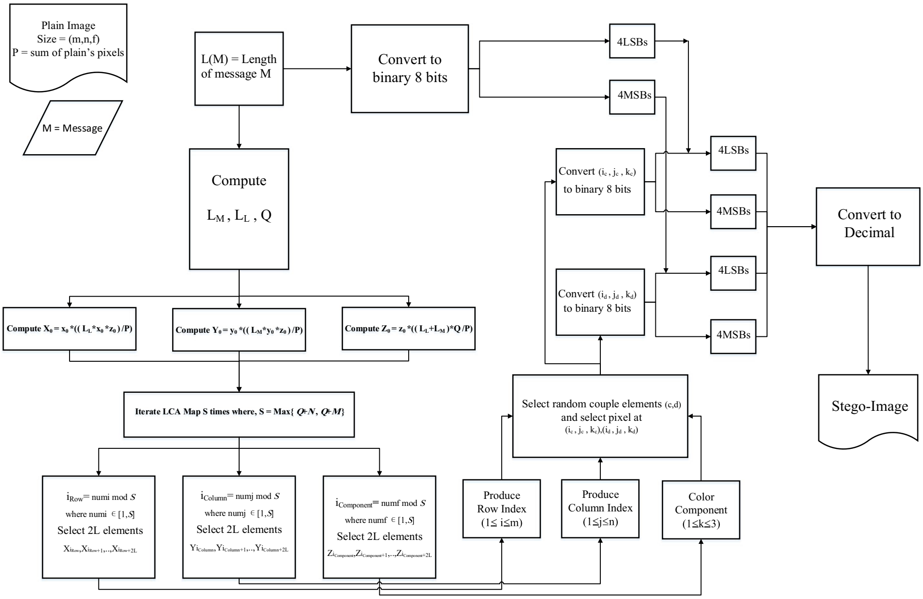

Plain Image
Size = (m,n,f)
P = sum of plain's pixels
M = Message
L(M) = Length of message M
Convert to binary 8 bits
4LSBs
4MSBs
Compute
L_M, L_L, Q
Convert (i_c, j_c, k_c) to binary 8 bits
4LSBs
4MSBs
4LSBs
4MSBs
Convert to Decimal
Convert (i_d, j_d, k_d) to binary 8 bits
Compute X0 = x0 *((LL*x0 *z0) /P)
Compute Y0 = y0 *((LM*y0 *z0) /P)
Compute Z0 = z0 *((LL+LM)*Q /P)
Iterate LCA Map S times where, S = Max{ Q+N, Q+M}
Select random couple elements (c,d) and select pixel at (ic, jc, kc),(id, jd, kd)
Stego-Image
iRow= numi mod S
where numi ∈ [1,S]
Select 2L elements
XiRow,XiRow+1,..,XiRow+2L
iColumn= numj mod S
where numj ∈ [1,S]
Select 2L elements
YiColumn,YiColumn+1,..,YiColumn+2L
iComponent= numf mod S
where numf ∈ [1,S]
Select 2L elements
ZiComponent,ZiComponent+1,..,ZiComponent+2L
Produce Row Index (1≤ i≤m)
Produce Column Index (1≤j≤n)
Color Component (1≤k≤3)

Fig. 4 Diagram of proposed chaotic steganography algorithm

$$P = \sum\nolimits_{i=1}^{m} \sum\nolimits_{j=1}^{n} p_{ij} \tag{7}$$

$$Q = \sum_{i=1}^{L} M_i \tag{8}$$

where L, represent the length of secret message, *MSBs* (*LSBs*) is most (least) significant bits of secret message, P is the sum of the whole of pixel values in the host image, and Q represents sum of all secret message letters (M_i) in binary mode. In order to provide high key sensitivity, we multiply this parameter to initial state conditions of the *LCA map* for building desired initial state conditions as below:

$$X_0 = \frac{L_L \times x_0 \times z_0}{P} \tag{9}$$

$$Y_o = \frac{L_M \times y_0 \times z_0}{P} \tag{10}$$

$$Z_0 = z_0 \times \frac{(L_{M+} L_L) \ \times Q}{P} \tag{11}$$

Then this modulated initial sate condition is used as an input for *LCA* map. We iterate this map s times where s is the maximum of $Q+M$ and $Q+N$. Next, we utilize a random selection technique in order to select *2L* random elements of generated sequences in previous steps. Indeed, this random selection method decreases transient effect and improves security of our scheme. In the following the procedure of random selection technique is described.

Subsequences $\tilde{X}, \tilde{Y}, \tilde{Z}$ with the length of *2L* are intercepted from *X*, *Y*, *Z* by starting from indices i_{Row}, i_{Column}, i_{Color}, respectively, where indices are produced based on following pseudo-code:

$$i_{Row} = Start\_index_{Row} = \bmod (P, \ s) \tag{12}$$

$$i_{Column} = Start\_index_{Column} = \bmod (P \times L_M, \ s) \tag{13}$$

$$i_{Color} = Start\_index_{Color} = \bmod (P \times L_L, \ s) \tag{14}$$

We note that if the procedure of the selection subsequences is stopped by reaching to the end of the main sequence, we start from the beginning to select remain elements. After that, by multiplying 10^6 and modulating, we reform these subsequences $\tilde{X}, \tilde{Y}, \tilde{Z}$ to integer sequences in intervals [1, *m*], [1, *n*], and [14, 23], which represent the number of row, column, and colour component, respectively. Now, we seek for random pairs of triples in subsequences $\tilde{X}, \tilde{Y}, \tilde{Z}$, which are used to embed *MSBs* and *LSBs* of secret message. For this, chaotic maps *CA*, *SPL* and Chebyshev with initial conditions, x_0, y_0,

z_0 are iterated 2L times. After sorting these three generating sequences, the corresponding indices for random selection of row, column, and colour component from $\tilde{X}, \tilde{Y}, \tilde{Z}$ are determined. We denote notation (i_l, j_l, k_l), $1 \leq l \leq 2L$, as 1^{th} random triple. The selected pixel values and secret message are converted into binary of eight bits and split into two equal parts *MSBs* and *LSBs*. The information of *MSBs* and *LSBs* will be embedded into *LSBs* in the specified positions (i_c, j_c, k_c) and (i_d, j_d, k_d), respectively, where $\mathrm{c} = 2l + 1$ and $d = 2l + 2$, $0 \leq l \leq L - 1$. Finally, by converting pixel values to decimal, the steganographic image will be obtained. In Fig. 5 the original and its steganographic image have been shown.

3.2 Extraction phase

In this phase, the extraction process secret message from steganographic image is described. Indeed, this procedure is the reverse of embedding algorithm. The receiving party must know secret keys (L, L_M, L_L, P, $\boldsymbol{\alpha}$, r, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, k, x_0, y_0, z_0, x_{LCA0}, y_{LCA0}, z_{LCA0}) to extract the secret message by following procedure. Frist, the stego-image used as an input in this phase. After that, by applying *LCA* map and using of desired initial state conditions (Eqs. 9–11), chaotic sequences X, Y, Z will be produced, respectively. In order to determine the positions of embedded data, *2L* random elements for each sequence $\tilde{\boldsymbol{X}}, \tilde{\boldsymbol{Y}}, \tilde{\boldsymbol{Z}}$, will be intercepted from X, Y, Z by starting indices specified in Eqs. 12–14, respectively. Thereafter, we use three chaotic maps (*CA*, *SPL* and Chebyshev) to find L pairs $(\mathrm{i_c}, \mathrm{j_c}, \mathrm{k_c})$ and $(\mathrm{i_d}, \mathrm{j_d}, \mathrm{k_d})$, of host pixel positions, in which the *MSBs* and *LSBs* of secret message are embedded, respectively. Next, receiver extracts data, including *MSBs* and *LSBs* from mentioning positions and joins them to each other. Finally, the secret message can be revealed after converting data to decimal.

4 Statistical security analysis

In this section, we provide some statistical analysis such as, correlation, entropy, homogeneity, contrast, energy, key sensitivity, mean squared error, peak signal to noise ratio, quality of the

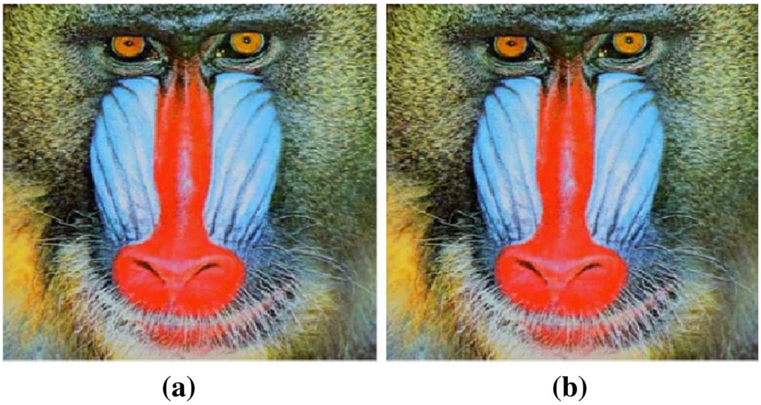


Fig. 5 **a** original image. **b** Steganographic image achieved by applying proposed Steganographic algorithm on original baboon image

index, histogram, and chi-square test, which prove our method is robust against statistical attacks. We use standard images that are used broadly in this criterion.[1]

4.1 Correlation

The purpose of this test is to determine the similarity between two images. The correlation of the image can be calculated based on below equation:

$$corr = \sum_{i,\ j} \frac{(i - \mu i)(j - \mu j)p(i,\ j)}{\sigma_i \sigma_j} \tag{15}$$

Where i, j represents the pixel positions; $p\ (i, j)$ is the pixel value at ith row and jth column; μ is the variance; σ is the standard deviation.

4.2 Information entropy

In information theory, entropy is a scale for showing randomness in information. This scale can be calculated based on below equation:

$$H(s) = -\sum_{i=0}^{2^Q-1} P(s_i)\log_2 P(s_i) \tag{16}$$

In the above equation, $P\ (s_i)$ is likelihood frequency of symbol $s_i \in s$ and Q is the number of bits, used for displaying symbol s_i.

4.3 Homogeneity

The homogeneity analysis is a metric that returns a value, for determining the closeness of the distribution of elements in the gray level co-occurrence matrix (*GLCM*) to the *GLCM* diagonal. The homogeneity of an image can be calculated based on the following equation:

$$\boldsymbol{Hom} = \sum_{\boldsymbol{i},\boldsymbol{j}} \frac{\boldsymbol{p}(\boldsymbol{i},\boldsymbol{j})}{1 + |\boldsymbol{i} - \boldsymbol{j}|} \tag{17}$$

Where $p\ (i, j)$ is the pixel value at the ith row and jth column and the values of (i, j) represent the indices of row and column numbers, respectively.

4.4 Contrast

Contrast analysis returns a measure of the intensity contrast between a pixel and its neighbor over the whole image. This analysis enables the viewer to better recognize the objects in the texture of an image. The mathematical formula of this analysis is as below:

$$\boldsymbol{C} = \sum_{\boldsymbol{i},\boldsymbol{j}} |\boldsymbol{i} - \boldsymbol{j}|^2\, \boldsymbol{p}\ (\boldsymbol{i},\ \boldsymbol{j}) \tag{18}$$

[1] http://sipi.usc.edu/database/

4.5 Energy

The energy analysis is used to measure the energy of the encrypted image. It returns the sum of squared elements in the *GLCM*. This analysis can be done with the help of Eq. (19):

$$\boldsymbol{E} = \sum_{\boldsymbol{i},\boldsymbol{j}} \boldsymbol{p}\,(\boldsymbol{i},\ \boldsymbol{j})^2 \tag{19}$$

The results of correlation, entropy, homogeneity, contrast and energy analysis provided in Table 1. As it is shown obvious based on the results provided in Table 1, the original image and steganographic image are identical. This proves that our proposed method not only has good efficiency, but also it produces an image with high quality. A key point is that when the steganographic image be the same as host image, an adversary cannot use statistical attacks, due to the fact that all statistical characteristics of host image are the same as steganographic one. Therefore, our scheme is robust against statistical attacks.

4.6 Image histogram

The steganographic image resistant against statistical attack when the colour histogram of steganographic image is the same as host image. The image histogram of Baboon plain image and its steganographic image are depicted in Fig. 6.

Table 1 Statistical security analysis of standard images

Statistical analysis	Image	Original image			Steganographic image		
		Red	Green	Blue	Red	Green	Blue
Entropy	Lena	7.5687	7.0914	6.8148	7.5687	7.0916	6.8147
	Baboon	7.7880	7.5484	7.7927	7.7881	7.5484	7.7927
	Barbara	7.5781	7.4109	7.5077	7.5782	7.4109	7.5077
	Pepper	7.3374	7.5207	7.0578	7.3374	7.5208	7.0578
Correlation	Lena	0.9417	0.9164	0.8883	0.9417	0.9164	0.8883
	Baboon	0.8829	0.8205	0.8929	0.8829	0.8205	0.8929
	Barbara	0.9131	0.8969	0.9140	0.9131	0.8969	0.9140
	Pepper	0.9289	0.9582	0.9184	0.9289	0.9582	0.9184
Homogeneity	Lena	0.8137	0.8201	0.8264	0.8137	0.8201	0.8264
	Baboon	0.6970	0.6769	0.6774	0.6970	0.6769	0.6774
	Barbara	0.7668	0.7839	0.7631	0.7668	0.7839	0.7631
	Pepper	0.8289	0.8285	0.8197	0.8289	0.8285	0.8197
Contrast	Lena	0.6188	0.6651	0.6435	0.6188	0.6651	0.6435
	Baboon	0.7425	0.7847	0.7546	0.7425	0.7847	0.7546
	Barbara	0.7626	0.7464	0.7631	0.7626	0.7464	0.7631
	Pepper	0.6001	0.6201	0.6010	0.6001	0.6201	0.6010
Energy	Lena	0.0856	0.1076	0.1594	0.0856	0.1076	0.1594
	Baboon	0.0456	0.0463	0.0463	0.0456	0.0463	0.0463
	Barbara	0.0731	0.0716	0.0689	0.0731	0.0716	0.0689
	Pepper	0.1083	0.0960	0.1296	0.1083	0.0960	0.1296

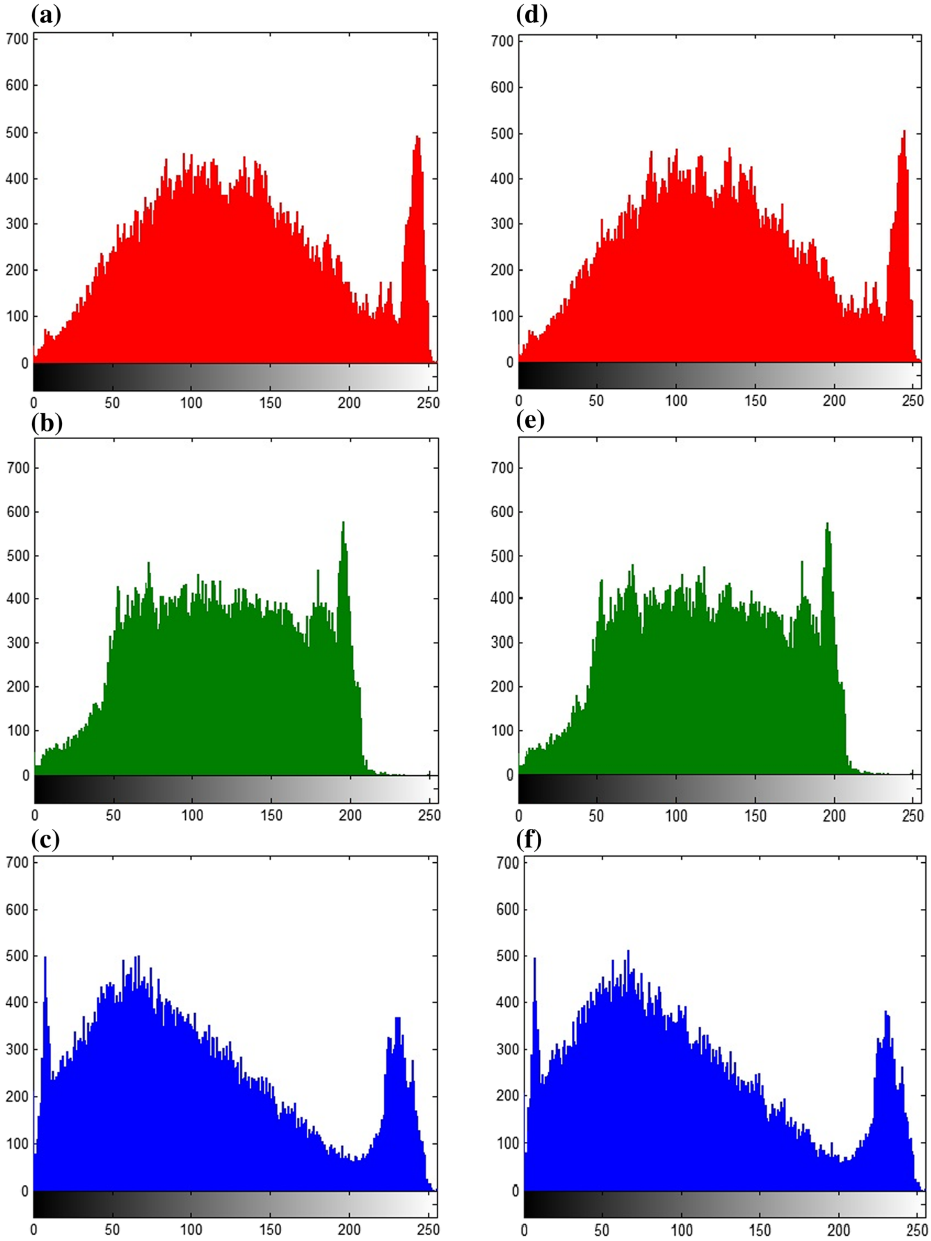


Fig. 6 Image histogram (**a**), (**b**), (**c**) Histogram of plain image for *red*, *green* and *blue* component (**d**), (**e**), (**f**) Histogram of steganographic image for *red*, *green* and *blue* component

4.7 Key sensitivity

Based on using high level chaotic maps, such as *LCA* map with large maximum Lyapunov exponent besides making dependent relations between initial condition and effective parameters, we enhance key sensitivity. In order to show this sensitivity, the baboon image is used for test, we apply a little change (10^{-16}) to one of initial state conditions of chaotic maps. As it is obvious in Fig. 7, secret data cannot be extracted, which embedded into the steganographic image.

4.8 Hiding capacity

One important subject in steganographic algorithm is hiding capacity. A steganographic algorithm called powerful, if it can embed a high mass of secret data. In our proposed method, we used 4bits of *LSBs* in all channels to embed data, so our hiding capacity is equal to 4/8. A comparison between our method and other available methods provide in Table 2.

As you can see in Table 2, our proposed method has the highest hiding capacity among other available chaos-based methods. Hence, we can embed secret messages with longer length and this is a vital advantage for steganography algorithm.

4.9 Quality index

In order to measure, quality of steganographic image, we use quality index [24] that is calculated based on below formula:

$$Q = \frac{4\sigma_{HT}\, H'T'}{\left(\sigma_H^2 + \sigma_T^2\right)\left[H'^2 + T'^2\right]} \tag{20}$$

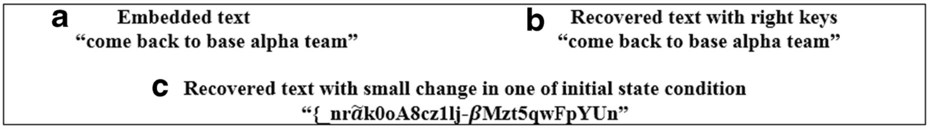
Where,

$$\sigma_H^2 = \frac{1}{N-1}\sum_{i=1}^{N}(H_i - H')2 \tag{21}$$

$$H' = \frac{1}{N}\sum_{i=1}^{N} H_i,\ T' = \frac{1}{N}\sum_{i=1}^{N} T_i \tag{22}$$

$$\sigma_H^2 = \frac{1}{N-1}\sum\nolimits_{i=1}^{N}\left(T_i - T'\right)^2 \tag{23}$$

In the above equation, n is the number of pixels in the image, H is the host image and T is the steganography image. The value of Q is between 1 and -1. If the calculated value be -1, it means that, the host image and the steganographic image don't have any similarity, but if it equals to 1, it means that the two images are identical. The calculated value for this test after applying our method with fifty thousand letters equal to 0.999705171806858, which is so



a Embedded text
"come back to base alpha team"

b Recovered text with right keys
"come back to base alpha team"

c Recovered text with small change in one of initial state condition
"{_nrα̃k0oA8cz1lj-βMzt5qwFpYUn"

Fig. 7 Key sensitivity (**a**) secret embedded text (**b**) recovered text with right keys (**c**) recovered data with small change in SPL map initial state condition $y_{LCA0} + 10^{-16}$

Table 2 Comparison between our proposed method and other available chaos-based methods of hiding capacity

Method	Hiding capacity
Proposed method	4/8
Aness et al. (2014) [3]	4/8
Aziz et al. hiding scheme (2015) [8]	3/8
Ghebleh et al. hiding scheme (2014) [12]	2.25/8

close to one. It means that our method has a good image quality. A comparison of quality index between proposed method and some available methods for Baboon image provided in Table 3.

Based on Table 3, this subject can be deduced that our steganographic image has high similarity with the original image. Furthermore, its values for the test image is better than other available methods. Therefore, as mentioned before, if the steganographic image is very close to its original one the adversary cannot use statistical analysis to extract secret message and achieve his purpose of breaking steganography algorithm.

4.10 Chi-square test

In the proposed method, we use *LSBs* of the host image to embed secret data, therefor, the *LSB* plane of image would be changed after embedding process. Chi-square test, [8] is kinds of statistical analysis that helps us to understand whether a difference between expected signal and observed signal exist or not. The result of this test is shown in Fig. 8. If the red line comes close to 1, it means that, there is a data, which is embedded in host image, in contrast, if it's close to zero, it means existence of hidden secret data in the host image can't observe.

4.11 MSE

Mean squared error shows the difference between host image and steganography image. It's calculated based on below formula:

$$MSE = \frac{1}{N}\sum_{i=1}^{n} \left(x_i - x_i^*\right)^2 \tag{24}$$

Table 3 Comparison of quality index between proposed method and some available methods for Baboon image

Methods	Quality index
Proposed method	0.99970
Aness et al.'s scheme (2014) [3]	0.99943
Aziz et al. hiding scheme (2015) [8]	0.99920
Ghebleh et al. (2014) [12]	0.99910
Bandyopadhyay et al. (2014) [9]	0.99870
Alam et al. (2014) [2]	0.99800

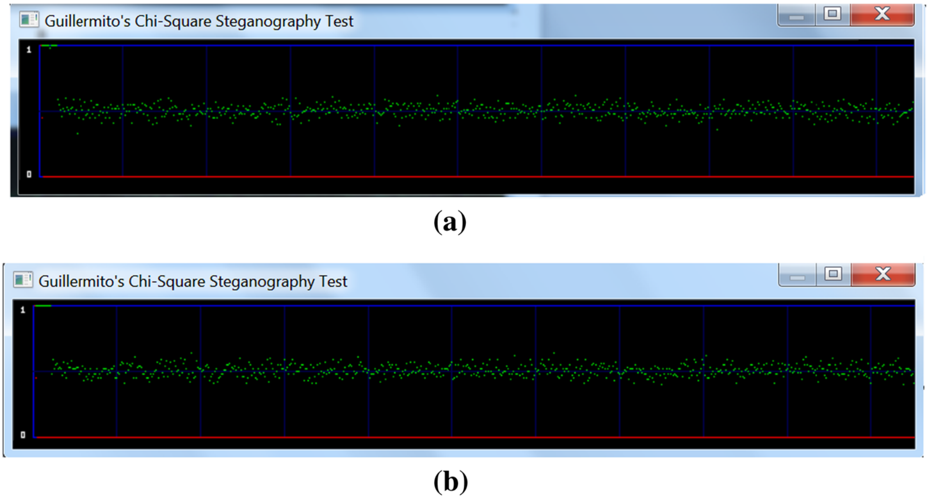

Guillermito's Chi-Square Steganography Test
1
0
(a)
Guillermito's Chi-Square Steganography Test
1
0
(b)

Fig. 8 Chi-Square test (**a**) host image of baboon (**b**) Steganographic image produced by our proposed method

As you can see in Fig. 8, our proposed method embed secret data in such a way that the *LSB* plane of the image would not be changed, because the red line is equal to zero. Indeed, the adversary cannot gain any useful information from steganographic image, due to the fact that there is no change occurred in *the LSB plane* of the image. Therefore, our scheme passes this test successfully and it will be robust against this kind of analysis.

4.12 *PSNR* analysis

Another important test which shows the strength of steganography method is *PSNR* test. As it's shown in below equation, we get the signal strength and divide it by mean squared error, so provides a better comparative statistical analysis.

$$PSNR = 10.\log_{10}\frac{\left(Max_i^2\right)}{MSE_{avg}} \qquad (25)$$

The results of Quality index and *PSNR* for Baboon (256 × 256,512 × 512) are stated in Tables 4 and 5, respectively.

As you can see in the above table, the proposed method has a promising result of *PSNR* analysis. The Quality index for all length of secret messages has the amazing value 0.999. This

Table 4 Statistical security analysis of *PSNR* and Quality index for Baboon (256 × 256) image

Length of message (chars)	Length of message (bits)	PSNR	Quality index
10000	80000	43.1189	0.999605430887160
20000	160000	40.2507	0.999682914275348
30000	240000	38.7540	0.999652148974817
40000	320000	37.7169	0.999688836713221
50000	400000	36.9914	0.999705171806858
98304	786432	34.8905	0.999501320520888

Table 5 Statistical security analysis of PSNR and Quality index for Baboon (512 × 12) image

Length of message (chars)	Length of message (bits)	PSNR	Quality index
10000	80000	48.9988	0.999715799434268
20000	160000	46.1938	0.999705306617473
30000	240000	44.6715	0.999695228770336
40000	320000	43.6704	0.999659380794601
50000	400000	42.8614	0.999629380794601
393216	3145728	39.9328	0.999009043233058

value for Quality index means that the steganographic image is identical to the original image. Hence, the adversary cannot do statistical analysis to break the steganography algorithm and extract secret message.

Based on the above table, if the size of the image becomes higher the results get better in both of analytical aspects. Therefore, we should remark this key point that such a good value for booth *PSNR* and Quality index lead to robustness against statistical attack, because when the host image and steganographic image be identical he cannot achieve information about the steganographic image and extract secret message.

4.13 Image fidelity

Another metric, which is used to show robustness of our scheme is image fidelity. The fidelity measure is measured by Image Fidelity that is calculated based on below equation:

$$IF = 1 - \frac{\sum_{I,\ J}(P(i,j) - S(i,\ j))^2}{\sum_{I,\ J}P(i,j) \times S(i,\ j)} \tag{26}$$

A comparison between proposed method and other available schemes based on PSNR, quality index, and image fidelity for baboon image (with 262144 bit embedding) provided in Table 6.

As it is obvious, based on the above table, our proposed method has better *PSNR*, Quality index, and image fidelity value among other available methods. Hence, the proposed method has strength as mentioned and robust against statistical attack.

Table 6 Comparison between different schemes for baboon image (256 × 256)

Methods	PSNR	Quality index	Image fidelity
Proposed method	38.7540	0.99967	0.99940
Aness et al.'s scheme (2014) [3]	36.5450	0.99935	0.99932
Aziz et al. hiding scheme (2015) [8]	37.8350	0.99915	0.99912
Ghebleh et al. (2014) [12]	36.5437	0.99905	0.99900
Bandyopadhyay et al. (2014) [9]	33.5467	0.99865	0.99100
Alam et al. (2014) [2]	31.4356	0.99790	0.98756

4.14 Known cover attack

In this type of attack, the adversary has information about cover image *H*, and then he compares this cover image with steganographic image by using statistical analysis, in order to find different patterns between them. Determination of host pixel positions, which has done by high level chaotic maps, avoids this kind of attack for two reasons. First, specification of host pixel positions are highly dependent on message (Eq. 9-11) that causes an adversary by having cover and steganography image (without secret message) cannot be able to achieve critical information by statistical analysis. Second, uniformly distribution of chaotic orbits on total space of cover image for determining host pixel positions, prevents adversary from gaining useful information. Based on aforementioned facts beside experimental analysis (4.1 through 4.6), the proposed method embed data in such a way that there exist only a vital change between original and steganographic image. Therefore, the adversary could not be able to gain anything except similar patterns. Indeed, our method has a good statistical analysis, which makes our scheme robust against this type of attack.

4.15 Known message attack

In this attack, the adversary knows the original message (*M*). With original message and cover image *H*, nobody can obtain hidden information, because our proposed method is highly dependent on its secret keys and cover image, and if one of this parameters value changes a bit, the position of embedded data will change. So, our method is robust against this kind of attack.

5 Conclusion

This paper presented a novel 3-dimensional chaotic map (*LCA* map) with strong chaotic characteristics and high maximum Lyapunov exponent 20.58. Indeed, by using *LCA* map along with three high level chaotic maps, desirable pair of triples host positions for embedding *LSBs* and *MSBs* of secret message are determined. Indeed, the aforementioned high level chaotic maps provide a uniformly distributation of chaotic orbits in the total space of cover image, which produce a steganographic image that is possess high similarity with cover image. By entering some parameters, which are dependent on elementary initial values, host image and secret message features, we achieve high key sensitivity (10^{-16}) besides adding additional layer of security. In fact, as it is shown in Fig. 1, similar secret messages for different cover image or converse circumstance, produced different host pixel positions, which implies that the adversary could not be able to gain useful information to break our steganography scheme. Our statistical analysis (4.1 through 4.6) is not only prove that our scheme provide good statistical quality, but also guarantees robustness of our scheme against differential attacks (4.14, 4.15). Indeed, the steganographic image and cover image are similar to each other in high rate, which prevents obtaining different patterns that are useful for an adversary to break a steganography algorithm. Furthermore, comparison of proposed scheme with other available methods (Tables 2, 3, and 6) shows priority of our scheme in sense of hiding capacity (**12*MN*** bits for ***M*** × ***N*** cover image), quality index, *PSNR*, and image fidelity. Moreover, Our experimental results guarantees that our scheme is not only robust against differential attacks, but also has a promising results such as highly sensitive keys, Quality index (0.999705171806858), *PSNR*, and hiding capacity as shown in statistical security analysis.

References

1. Alam S, Kumar V, Siddiqui W, Ahmad M (2014) Key dependent image steganography using edge detection. In: Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on. IEEE, pp 85–88
2. Alam S, Kumar V, Siddiqui WA, Ahmad M (2014) Key dependent image steganography using edge detection. In: Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on. IEEE, pp 85–88
3. Anees A et al (2014) A technique for digital steganography using chaotic maps. Nonlinear Dyn 75(4):807–816
4. Arshad H, Nikooghadam M (2014) Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. J Med Syst 38(12):1–12
5. Arshad H, Nikooghadam M (2015) Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. J Supercomput 71(8):3163–3180
6. Arshad H, Nikooghadam M (2016) An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. Multimed Tools Appl 75(1):181–197
7. Arshad H, Teymoori V, Nikooghadam M, Abbassi H (2015) On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. J Med Syst 39(8):1–10
8. Aziz M, Tayarani-N MH, Afsar M (2015) A cycling chaos-based cryptic-free algorithm for image steganography. Nonlinear Dyn 80(3):1271–1290
9. Bandyopadhyay D, Dasgupta K, Mandal JK, Dutta P (2014) A novel secure image steganography method based on chaos theory in spatial domain. Int J Secur Priv Trust Manag (IJSPTM) 3(1):11–22
10. Bilal M, Imtiaz S, Abdul W, Ghouzali S, Asif S (2014) Chaos based Zero-steganography algorithm. Multimed Tools Appl 72(2):1073–1092
11. Das P, Kar N (2014) A DNA based image steganography using 2D chaotic map. In: Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, pp 1–5
12. Ghebleh M, Kanso A (2014) A robust chaotic algorithm for digital image steganography. Commun Nonlinear Sci Numer Simul 19(6):1898–1907
13. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. Computer 31(2):26–34
14. Judge J (2001) Steganography: past, present, future. SANS white paper
15. Kanso A, Own HS (2012) Steganographic algorithm based on a chaotic map. Commun Nonlinear Sci Numer Simul 17(8):3287–3302
16. Mollaeefar M, Sharif A, Nazari M (2015) A novel encryption scheme for colored image based on high level chaotic maps. Multimedia Tools Appl 1–23
17. Potdar VM, Han S, Chang E (2005) Fingerprinted secret sharing steganography for robustness against image cropping attacks. In: Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on. IEEE, pp 717–724
18. Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. IEEE Secur Priv 1(3):32–44
19. Provos N, Honeyman P (2001) Detecting steganographic content on the internet. Center for Information Technology Integration
20. Roy R, Sarkar A, Changder S (2013) Chaos based edge adaptive image steganography. Procedia Technol 10: 138–146
21. Sabery KM, Yaghoobi M (2008) A simple and robust approach for image hiding using chaotic logistic map. In Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on. IEEE, pp 623–627
22. Shirali-Shahreza MH, Shirali-Shahreza M (2006) A new approach to Persian/Arabic text steganography. In: Computer and Information Science, 2006 and 2006 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on. IEEE, pp 310–315
23. Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13:95–113
24. Wang Z, Bovik AC (2002) A universal image quality index. IEEE Signal Process Lett 9(3):81–84

Amir Sharif was born in 1990 in Birjand, south Khorasan Province. He received his B.Sc. degree in information technology from Birjand University in June 2012. Nowadays, he study secure communication in Imam Reza International University of Mashhad, attendant for M.Sc. degree. His filed of interest are image processing, steganography, Covert Channel, cryptography and security.

Majid Mollaeefar was born in 1989 in Gonbad-e Kavus, Golestan Province. He received his B.Sc. degree in information technology from Tabari University in June 2013. Nowadays, he study secure communication in Imam Reza International University of Mashhad, attendant for M.Sc. degree. His filed of interest are image processing, cloud security, Covert Channel, steganography and security.

Mahboubeh Nazari received B.Sc. degree from Ferdowsi University of Mashhad, Iran, in 2006, M.Sc. degree from Ferdowsi University of Mashhad, Iran, in 2008 and Ph.D. degree from Ferdowsi University of Mashhad, Iran, in 2013. She is Adjunct professor in Department of Mathematics at Ferdowsi University of Mashhad, Iran. Her research focuses on Dynamical Systems, Chaos theory and it's applications in Cryptography, Network Security and data Security.