IJICTR International Journal of Information & Communication Technology Research
ITRC

Volume 4- Number 3- June 2012 (13- 19)

Image Encryption Using Tent Chaotic Map and Arnold Cat Map

Elham Hasani
Department of Computer Engineering
Science and Research Branch, Islamic Azad University
Tehran, Iran
e.hasani@srbiau.ac.ir

Mohammad Eshghi
Computer Engineering Department
Shahid Beheshti University
Tehran, Iran
m-eshghi@sbu.ac.ir

Received: February 22, 2012- Accepted: May 27, 2012

***Abstract*—In this paper, a new algorithm for image encryption using chaotic tent map and Arnold cat map is proposed. This algorithm consists of two major phases, permutation and substitution. In the permutation phase, Arnold cat transform is used. A pseudo random image is produced using the chaotic tent map. In the substitution phase, the permuted image is Exclusively ORed to this pseudo random image in order to generate encrypted images. A computer simulation is used to evaluate the proposed algorithm and to compare its results to encrypted images of other methods. The criteria for these comparisons are chi-square test of histogram, correlation coefficients of pixels, NPCR (number of pixel change rate), UACI (unified average changing intensity), MSE (mean square error) and MAE (mean absolute error). These comparisons show that the proposed chaotic image encryption method has a high performance and security.**

Keywords-Image encryption, Permutation, Substitution, Arnold Cat map, Chaotic Tent map.

I. INTRODUCTION

In recent years, with the rapid development of computer networks, images are increasingly transmitted through networks such as internet. To protect such communications, image encryption technique has received considerable attention in the literature. Many image encryption schemes have been proposed for this purpose. Chaos-based encryption methods are one of such methods that produce a good combination of speed and high security [1, 2, 3].

Chaotic functions have numerous properties such as randomness, ergodicity and sensitivity to initial conditions. These properties cause a close relationship between cryptosystems and chaotic systems. Chaotic maps produce long-period, random-like chaotic sequences and a small difference of the initial value or system parameters leads to a large change of the chaotic sequences [3, 4].

Digital images have some features such as a high correlation between adjacent pixels and redundancy of data. For these reasons, traditional ciphers such as Advance Encryption Standard(AES), Data Encryption Standard (DES), Rivest and Shamir and Adleman (RSA) are not suitable for image encryption [4, 5, 6].

Mao et al. designed a new image encryption system based on distributed Baker map in time domain [7]. Zhou et al. introduced a parallel image encryption algorithm in time domain using the Kolmogrov flow map. In this algorithm, all of the pixels are permuted by this map and then are encrypted by Cipher Block Chain model [8]. Chen Wei-bin et al. proposed an image encryption algorithm based on Henon's chaotic system. In this system, the Arnold cat map is used to permute the positions of the image pixels. The permuted image is then encrypted based on Henon's chaotic system [9]. Borujeni et al. designed an image encryption algorithm based on chaotic maps and Tompking-Paig algorithm [10]. Khanzadi et al. proposed an image encryption algorithm using a random bit sequence generator (RBSG) based on logistic and tent map. In this algorithm, a plain image is permuted and then partitioned into 8 bit maps. In each bit map, bits are permuted and substituted. Finally, the 8 bit maps are composed to produce the encrypted image [11].

In this paper, a new algorithm for image encryption using tent chaotic function is proposed. This algorithm consists of two major phases, permutation and substitution [2, 12]. In permutation phase, an image is decomposed into 8 bit planes and Arnold cat map is used to permute bits of 4 most significant bit planes of the image and other bit planes are not changed. Then, these bit planes are merged to generate a permuted image. In the substitution phase, this permuted image is Exclusively ORed to a pseudo random image produced through a chaotic process.

The rest of the paper is organized as follows. In section 2 the design of the proposed chaotic image encryption scheme is discussed in details. In section 3, image encryption scheme is evaluated, followed by a comparison between image encryption scheme and the other methods in section 4. The paper concludes in section 5.

II. The Proposed Chaotic Image Encryption Scheme

In this section, a new algorithm for image encryption is proposed using tent chaotic map. This algorithm consists of two major phases, permutation and substitution. In the permutation phase, an image is decomposed into 8 bit planes and Arnold cat map is used to permute bits of 4 most significant bit planes of the image and the remaining bit planes are not changed. Then, these 8 bit planes are merged to generate a permuted image. In the substitution phase, this permuted image is Exclusively ORed to a pseudo random image, produced through a chaotic process. In the rest of this section, these steps are described in details.

A. Permutation Phase

The first step in this stage is image decomposition into 8 bit planes. In the second step the 4 most significant bit planes are permuted using the Arnold cat transform. The other bit planes are not changed. This is a two-dimensional Arnold cat map function, as stated in Eq. (1) [9, 13].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left(\begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \right) mod(N) \qquad (1)$$

We assume the dimension of the plain image is *N *N*. The control parameter of *c* and *d* are positive integers. If (*x,y*) is the original position of the plain image, then (*x',y'*) is the permuted position. The parameters *c* and *d* are used as the secret keys [12].

This function is not invertible. In order to use this function in an image encryption algorithm, it should be invertible. Therefore, we modified the function to convert it to an invertible function. This modification is shown in a pseudo code in Fig. 1.

```
for  x=1:128
  for  y=1:128
    m=mod(([1,C;D,(C*D)+1]*[x;y]),128);
     if ((m(1)==0) && (m(2)==0))
           x' =128;
          y'=128;
     elseif  (m(1)==0)
          x'=128;
          y'=m(2);
     elseif (m(2)==0)
          x'=m(1);
          y'=128;
     else
          x'=m(1);
          y'=m(2);
     end
  end
end
```

Fig. 1. Modification made to the Arnold cat transform in order to make it an invertible function

MOD operation is not invertible either. In order to use this function in an image encryption algorithm, it should be invertible. Therefore, we modified the function to convert it to an invertible function for decryption. This modification is shown in a pseudo code in Fig. 2.

```
for  x'=1:128
   for  y'=1:128
      n = ([(C*D)+1,-C;-D,1]*[ x'; y']);
      while (n(1)<=0)
         n(1)=n(1)+128;
      end
      while (n(2)<=0)
         n(2)=n(2)+128;
      end
      x=mod(n(1),128);
      y=mod(n(2),128);
   end
end
```

Fig. 2. Pseudo code of the modification made to the MOD operation

At the end of this stage, all bit planes are merged to obtain the permuted image.

Note that the proposed permutation on bit planes lead not only to permutation of the pixels but also to substitution of the pixels of the plain image. This results in obtaining a more encrypted image at the end of the algorithm.

In the proposed algorithm, bit planes are permuted using cat transforms. Bit planes number 1 and 3 are permuted with *c1* and *d1* parameters for a cat transform. Bit planes number 2 and 4 are permuted with *c2* and *d2* parameters for a cat transform.

B. Substitution Phase

To achieve a more uniform distribution histogram we added a substitution stage after the permutation stage. Tent map is a kind of chaotic function which is widely used in encryption systems. One dimensional tent mapping [2, 10] has the following expression:

$$x_{n+1} = \begin{cases} \frac{x_n}{a} & 0 \le x_n \le a \\ \frac{1-x_n}{1-a} & a < x_n \le 1 \end{cases} \quad (2)$$

Where x_0 is the initial value and $x_n \in [0,1]$. The control parameter $a \in (0,1)$ and when $a \neq 0.5$, the system enters a chaotic state [2, 10].

After permutation in the substitution phase, the permuted image is Exclusively ORed to a pseudo random image, produced through a chaotic process. In this process, the chaotic tent map is used to generate this pseudo random image.

III. SIMULATIONS AND SECURITY ANALYSIS

A computer simulation is used to evaluate the proposed algorithm. Some experimental results are given in this section to indicate the efficiency and security of our proposed scheme. In this section, the performance of the proposed chaotic image encryption scheme is analyzed based on some criteria such as Chi-square test of histogram, Correlation Coefficients of pixels (CC), Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean Square Error (MSE) and Mean Absolute Error (MAE). Two other criteria for security analysis are key space and key sensitivity [10, 14].

For security analysis, the plain image, Lena, with the size 128*128 is considered. Image permutation is the first phase of image encryption, where the Arnold cat map parameters are chosen as *c1* =15, *d1* =2, *c2*= 20 and *d2*=4. Image substitution is the second phase of image encryption where the control parameter of the tent map and its initial value are selected as a = 0.45 and x_0=0.85.

A. Histogram

Chi-square test of a histogram, Eq. (3), is one of the important criteria in Security Analysis. This value shows the uniformity of the histogram. The less the chi-square value of an image causes the more uniform the histogram and the more secure the image encryption system [10].

$$x^2 = \sum_{k=1}^{256} \frac{(O_k - E_k)}{E_k} \quad (3)$$

Parameter k is the number of gray levels, O_k is observed occurrence frequencies of each gray level and E_k is the expected occurrence frequencies of each gray level.

The plain image, Lena, with the size 128*128 is shown in Fig. 3(a) and the histogram of the plain image is shown in Fig. 3(b). The permuted image is shown in Fig. 3(c) and the histogram of the permuted image is shown in Fig. 3(d). The ciphered image is shown in Fig. 3(e) and the histogram of the ciphered image is shown in Fig.3(f). The results of chi-square test on Lena image are shown in Table 1.

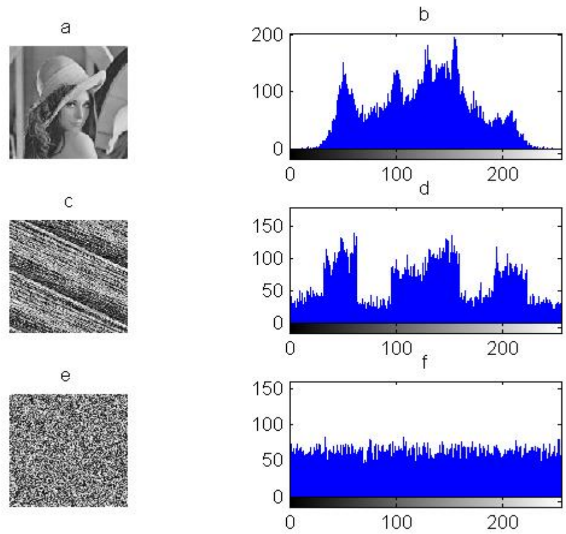


Fig. 3. (a) Plain image, (b) Histogram of the plain image, (c) Permuted image, (d) Histogram of the permuted image, (e) Ciphered image, (f) Histogram of the ciphered image

Table 1. Chi-square test results of Lena image

Image	Plain Image	Permuted Image	Encrypted Image
Chi-square	10229	4154	**198**

B. Correlation Coefficient

Correlation coefficient, Eq. (4), gives the statistical relationships between two adjacent pixels in vertical, horizontal, and diagonal sets. For better resistance of an image encryption system against statistical attacks, correlation coefficients of pixels in the encrypted image should have a low value [5].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad (4)$$

where

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} \left(x_i - \frac{1}{N} \sum_{i=1}^{N} x_i \right)^2$$

$$cov(x,y) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N}(x_i - \mathrm{E(x)})\,(y_i - \mathrm{E(y)})$$

and

$$E(x) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N} Z_i$$

Parameters x and y are gray level of two adjacent pixels.

The results of correlation coefficient test of Lena image are shown in Table 2.

The correlation between two horizontally, vertically and diagonally adjacent pixels of the plain image is shown in Fig. 4 (a), (b) and (c), respectively. The correlation values of the encrypted image are also shown in Fig. 4 (d), (e) and (f), respectively.

Table 2. Correlation coefficient test results of Lena image

Image / Correlation	Plain Image	Permuted Image	Encrypted Image
Vertical	0.9527	0.1557	**0.0020**
Horizontal	0.8948	0.3160	**0.0312**
Diagonal	0.8563	0.2679	**0.0100**
Average	0.9012	0.2465	**0.0144**

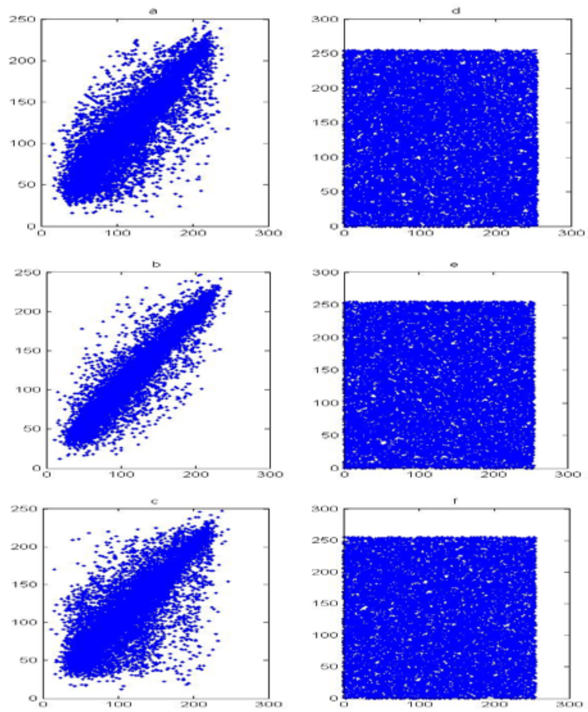


Fig. 4. (a) Horizontal correlation of the plain image, (b)Vertical correlation of the plain image, (c) Diagonal correlation of the plain image, (d) Horizontal correlation of the encrypted image, (e) Vertical correlation of the encrypted image, (f) Diagonal correlation of the encrypted image.

C. NPCR and UACI

The number of Pixel Change Rate (NPCR) is a criterion proportionate to the number of pixels whose gray levels are changed in an encrypted image. NPCR is defined in Eq. (5).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (5)$$

where

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases}$$

Parameters W and H are width and height of the image. $C_1(i,j)$ is the gray level of a pixel in a plain image and $C_2(i,j)$ is the gray level of a pixel in an encrypted image [5,10].

Unified Average Changing Intensity (UACI) criterion is proportionate to average changing intensity between the plain image and the encrypted image, Eq. (6).

$$UACI = \frac{1}{\mathrm{W \times H}}\left[\sum_{\mathrm{i,j}} \frac{|\mathrm{C_1(i,j)} - \mathrm{C_2(i,j)}|}{255}\right] \times 100\% \quad (6)$$

Parameters W and H are width and height of the image. $C_1(i,j)$ is the gray level of a pixel in the plain image and $C_2(i,j)$ is the gray level of a pixel in the ciphered image [5, 10]. NPCR and UACI of the permuted and encrypted images of Lena are shown in Table 3.

Table 3. NPCR and UACI test results of Lena image

Image / Criteria	Permuted Image	Encrypted Image
NPCR	92.2546%	**99.6216%**
UACI	26.1014%	**28.5102%**

D. MSE and MAE

The encrypted image should have a significant difference with the plain image. This difference is measured by Mean Square Error (MSE) and Mean Absolute Error (MAE) criteria. MSE and MAE values are stated in Eq. (7) and (8) respectively [10].

$$MSE = \frac{1}{\mathrm{W*H}}\sum_{j=1}^{H}\sum_{i=1}^{W}\left(a_{ij} - b_{ij}\right)^2 \quad (7)$$

$$MAE = \frac{1}{\mathrm{W*H}}\sum_{j=1}^{H}\sum_{i=1}^{W}\left|\left(a_{ij} - b_{ij}\right)\right| \quad (8)$$

Parameters W and H are width and height of the image. a_{ij} is the gray level of the pixel in the plain image and b_{ij} is the gray level of the pixel in the encrypted image. MSE and MAE of the permuted and encrypted images of Lena are shown in Table 4.

Table 4. MSE and MAE test results

Image Criteria	Permuted Image	Encrypted Image
MSE	6606	**7694**
MAE	66.5586	**72.7010**

E. Key space

In order to protect an encryption system against any brute-force attack, it has to have a large key space. In our proposed system, there are six keys, including $c1, d1, c2, d2, x_0$ and a. The total length of the keys is 256 bits. As a result, the key space of the proposed encryption system is 2^{256}, which is large enough to protect the encryption system against any potential brute-force attack.

F. Key sensitivity

Key sensitivity is one of the important criteria in image encryption algorithms [15, 16]. To test this in the proposed scheme, we consider fixing all the keys except the control parameter of the tent map. A small change in the control parameter causes a significant change in the decrypted image. The decrypted image with correct keys is shown in Fig. 5(a) and the histogram of the decrypted image is shown in Fig. 5(b). Also the incorrect decrypted image with a=0.4500000001 is shown in Fig. 5(c) and the histogram of this image is shown in Fig. 5(d).

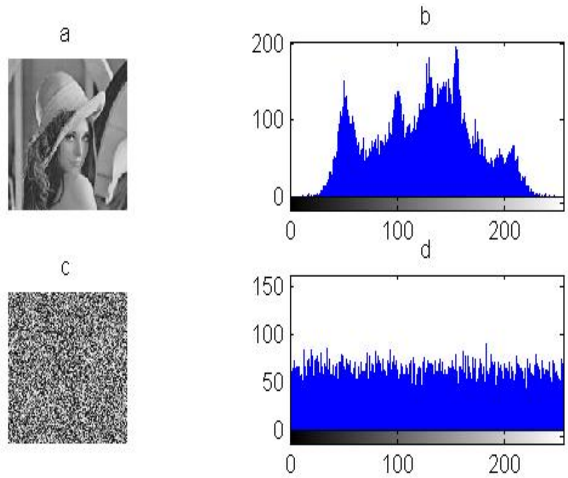


Fig. 5. (a) Correct decrypted image with a=0.45, (b) Histogram of correct decrypted image, (c) Incorrect decrypted image with a=0.4500000001, (d) Histogram of incorrect decrypted image.

IV. COMPARISON

In order to compare the performance of the proposed algorithm to other methods, the proposed method is first used and applied to eight standard images and its performance is evaluated based on seven criteria. The averages of these criteria for these eight images are obtained. These averages are considered as the performance of the proposed algorithm. Then, the performance of other methods, based on these criteria, is compared to the performance of the proposed image encryption system.

The proposed algorithm is tested on the eight standard images, including Lena, Peppers, Cameraman, Splash, Lake, Baboon, House and Airplane.

The seven criteria which are used in this comparison are Chi-square of histogram, Correlation Coefficients of pixels (CC), Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean Square Error (MSE), Mean Absolute Error (MAE) and key space.

This test for each image is repeated for 10 times for different values of the keys, $c1, d1, c2, d2, x_0$ and a. Table 5 shows the average performance of the proposed method on eight standard images.

The performance of other methods, based on these criteria, is compared to the performance of the proposed image encryption system. Table 6 shows these comparisons.

In the other methods presented in Table 6, the results were obtained from implementing the algorithm only on the standard image, LENA. Also, in some encrypted systems presented in the Table 6, such as Zhou et al. the results were obtained following two iterations of implementing the algorithm, which, due to the need for creating an encryption with a higher security, would certainly incur a higher cost compared to a single iteration of implementation. Since an algorithm may produce acceptable results on a given image, but lead to generally undesirable results on different images [2, 5], the proposed algorithm in this study was tested on 8 standard images. The average values of these tests are compared in the table with the values obtained for different algorithms tested only on Lena by other researchers. It is worth noting that the results of our proposed algorithm are from a single iteration of implementation on the images while the results of some methods are the outcome of multiple iterations of using the algorithms.

Table 5. The average performance of the proposed method on eight standard images

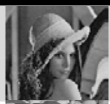
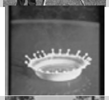
Criteria Image	Image	Chi-square	NPCR	UACI	CC (average H,V,D)	MAE	MSE
Lena		231.90	99.609%	28.479%	0.0213	72.622	7670
Peppers		232.83	99.619%	29.37%	0.0138	74.895	8250
Camera man		238.68	99.616%	30.414%	0.0246	77.556	8920
Splash		252.57	99.625%	30.028%	0.0760	76.571	8670
Lake		235.76	99.603%	31.387%	0.038	80.037	9570
Baboon		256.22	99.617%	27.064%	0.0079	69.015	6740
House		241.10	99.620%	28.614%	0.011	72.966	7720
Airplane		255.10	99.595%	32.4%	0.019	82.674	1019
Average		**241.526**	**99.612%**	**29.717%**	**0.0262**	**75.790**	**7319.8**

Table 6. Comparison of the proposed method to other methods based on seven criteria

Criteria / Schemes	chi-square	MSE	MAE	Average of Correlation Coefficient	NPCR	UACI	Key space
Wang et al. [2] 1nd round	NA	NA	NA	0.005919	44.267%	14.874%	NA
Mao et al. [7] 1nd round	NA	NA	NA	0.03121	37%	9%	2^{128}
Zhou et al. [8] 2nd round	NA	NA	NA	0.015	25.0%	8.5%	NA
Borujeni et al. [10]	290	NA	35.1	0.13	99.7%	29.3%	2^{218}
Khanzadi et al. [11]	243	NA	NA	0.003164	99.61%	33.35%	2^{2160}
Zhang et al. [12] 1nd round	NA	NA	NA	NA	37.6389 %	12.7034 %	NA
Zhang et al. [17] 2nd round	NA	NA	NA	0.0411	21.5%	2.5%	NA
Gao et al. [18]	NA	NA	NA	0.03786	37%	NA	10^{45}
Wang et al. [19] 1nd round	NA	NA	NA	0.0059194	44.33%	14.89%	NA
Average value of proposed method	**241.526**	**7319.8**	**75.790**	**0.0262**	**99.612%**	**29.717%**	**2^{256} ~10^{77}**

V. Conclusion

In this paper, a new algorithm for image encryption using chaotic functions was proposed. This algorithm consisted of two major phases, permutation and substitution. In the permutation phase, the plain image was decomposed into eight bit planes. The four most significant bit planes were permuted using a proposed modified Arnold cat map while other four bit planes were kept constant. Then, the permuted and other bit planes were merged to generate the permuted image. Note that the proposed permutation on bit planes caused not only the permutation of the pixels but also to substitution of the pixels of the plain image. A pseudo random image was produced, using the tent chaotic map. In the substitution phase, the permuted image was Exclusively ORed to this pseudo random image, to generate the encrypted image.

A computer simulation was used to evaluate and compare the proposed algorithm to encrypted images of other methods. These comparisons were based on Chi-square test of histogram, Correlation Coefficients of pixels (CC), Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean Square Error (MSE), Mean Absolute Error (MAE) and key space. These comparisons showed the superiority of the proposed chaotic image encryption system.

Acknowledgment

This paper is extracted from the MSc thesis.

Reference

[1] H. S. Kwok and W. K. S. Tang, "A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation", J. of Chaos, Solitons & Fractals, vol. 32, pp. 1518–1529, 2007.

[2] Y. Wang, K. W. Wong, X. Liao and G. Chen, "A New Chaos-based Fast Image Encryption Algorithm", J. of Applied Soft Computing, Vol. 11, Issue 1, pp. 514-522, 2011.

[3] I. S. Sam, P. Devaraj and R. S. Bhuvaneswaran, "A Novel Image Cipher based on Mixed Transformed Logistic Maps", J. of Multimedia Tools and Applications, Vol. 56, pp. 315-330, 2012.

[4] H. Khanzadi, M. A. Omam, F. Lotfifar and M. Eshghi "Image Encryption Based on Gyrator Transform Using Chaotic Maps", Signal Processing (ICSP) conference, China, 2010.

[5] S. M. Seyedzadeh and S. Mirzakuchaki, "A Fast Color Image Encryption Algorithm based on Coupled Two-Dimensional Piecewise Chaotic Map", J. of Signal Processing, Vol. 92, pp.1202–1215, 2012.

[6] N. K. Pareek , V. P and K. K. Sub, "Image Encryption Using Chaotic Logistic Map", J. of Image and Vision Computing, vol. 24, pp. 926–934, 2006.

[7] Y. Mao, G. Chen and S. Lian, "A novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", International Journal of Bifurcation and Chaos, vol. 14, pp. 3613–3624, 2004.

[8] Q. Zhou, K-wo, Wong, X. Liao, T. Xiang and Y. Hu, "Parallel image encryption algorithm based on discretized chaotic map", J. of Chaos, Solitons & Fractals, vol. 38, pp. 1081–1092, 2008.

[9] C. Wei-bin and Z. Xin, "Image Encryption Algorithm Based on Henon Chaotic System", Image Analysis and Signal Processing (IASP), IEEE conference, 2009.

[10] S. E. Borujeni and M. Eshghi, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm", J. of Mathematical Problems in Engineering, Vol. 22, 2009.

[11] H. Khanzadi and M. Eshghi, "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", submitted to International Journal of Bifurcation and Chaos, 2011.

[12] G. Zhang and Q. Liu, "A Novel Image Encryption Method based on Total Shuffling Scheme", J. of Optics Communications, Vol. 284, pp. 2775–2780, 2011.

[13] Y. Heng-fu, W. Yan-peng and T. Zu-wei, "An Image Encryption Algorithm Based on Logistic Chaotic Maps and Arnold Transform", J. of Hengshui University, pp. 40-43, 2008.

[14] S. Lian, J. Sun and Z. wang, "Security Analysis of A Chaos-based Image Encryption Algorithm", J. of Statistical Mechanics and its Applications, Vol. 351, pp. 645-661, 2005.

[15] V. Patidar, N. K. Pareek, G. Purohit and K. K. Sud, "A Robust and Secure Chaotic Standard Map based Pseudorandom Permutation-Substitution Scheme for Image Encryption", J. of Optics Communications, Vol. 284, pp. 4331-4339, 2011.

[16] X. Wang and L. Teng, "An Image Blocks Encryption Algorithm based on Spatiotemporal Chaos", J. of Nonlinear Dynamics, Vol. 67, pp. 365-371, 2012.

[17] X. Zhang and W. Chen, "A New Chaotic Algorithm for Image Encryption", ICALIP, pp. 889-892, 2008.

[18] H. Gao, Y. Zhang, S. Liang and D. Li, "A new chaotic algorithm for image encryption", J. of Chaos, Solitons & Fractals, vol. 29, pp. 393–399, 2006.

[19] Y. Wang, K. W. W, X. L and G. C, "A new chaos-based fast image encryption algorithm", J. of Applied Soft Computing, vol. 11, pp. 514–522, 2009.

Elham Hasani was born in 1986 in Iran. She received her B.Sc. degree in Hardware Engineering from Islamic Azad University, Central Tehran Branch, in 2008 and her M.Sc. degree in Computer Architecture from Islamic Azad University, Science & Research Branch, Tehran, Iran. Her main research interest is image encryption systems.

Mohammad Eshghi (BS'78, Ms'89 and Phd'94) Mohammad Eshghi got his B.Sc. in Electrical Engineering from Sharif University of Technology in 1978, his M.Sc. degree in EE from Ohio University, Athens, Ohio, and his Ph.D in EE from Ohio State University, Columbus, Ohio, USA, in 1989 and 1994 respectively. He is now with the Electrical and Computer Engineering Faculty at Shahid Beheshti University, Tehran Iran. He is the manager of Information and Communication Center in that university. His research interest including digital signal processing and digital circuit design and implementation on field programmable gates arrays (FPGA).