

Maze Based Image Encryption Algorithm

Erdal GUVENOGLU¹

¹ Assistant Professor, Computer Engineering Department, Maltepe University, Istanbul, Turkey

Abstract - In this study, a maze based on a key value specified by the user is generated. Images are encrypted by using the pixel values located in the center of gravity of algorithms of the maze. Depending on the user key different mazes are generated. (Generated mazes differ from each other depending on the user key). In this study, the upper left corner of the maze is selected as a starting point. Selecting different starting points may result different solutions depending on the key. To be able to obtain different mazes and solutions makes difficult to estimate the encryption key used. The proposed method uses two different keys. The first one is the user key and the second one is the secret key generated according to the user key. Depth First Search algorithm is used to produce the maze. In the process, digital image encryption is found to be successful regardless of the type and format of the image. The proposed method is tested with detailed security analyses.

Key Words: Data security, Digital images, Image encryption, Information security.

1. INTRODUCTION

Under today's conditions, the popularity of multimedia elements is rapidly increasing and applications such as internet using these elements are gaining great importance in our daily lives. Multimedia elements are at higher risk due to the personal information they contain [1]. Considering developments especially in mobile technology, the greater risk on images can be clearly seen. This risk can be reduced using a variety of encryption techniques. It is common to use traditional text encryption methods such as DES, RSA and AES for the encryption of data. These methods can also be used to encrypt image files which consist of numerical data. However, there are two major drawbacks of these methods. The first of these; image data are much larger than text data and encrypting image files by traditional methods is very time consuming. Second, the encrypted text cannot be understood until it is converted back into its original version, whereas image data can be understood even if they are partially decrypted. Human minds can ignore the parts that are not

decrypted. Various image encryption techniques are developed to prevent images to be either partially or completely decrypted. Image encryption applications are widely used in many fields such as military communications, multimedia systems, medical sciences, Internet communications, etc.[2].

There are many methods to encrypt images. Almost all of these methods have three basic ideas [3-4] as follows: Value transformation [5-6-7], local permutation [8-9] and combinations of value transformation and local permutation methods [10]. Value transformation is described as a new value of the data value of original pixel after being subjected to the processing in algorithm. Local permutation algorithms are expressed as displacement of the position of the original pixel. Combinations of these are obtained by using these two methods together.

Image encryption techniques are divided into two groups as chaotic and non-chaotic-based techniques [2]. In chaotic encryption algorithms, parameters are asked from user for encryption and decryption and encryption key is changed in each step. If the user parameter used for encryption is not used for decryption, decoding process is not done correctly.

In this study, a chaotic method that provides image encrypting using pixel values in the center of gravity of cells in the algorithm of a maze generated by using the Depth First Search (DFS) algorithm has been proposed. This method is named Maze Based Image Encryption Algorithm (MBIEA). The secret key of the user is used while generating the maze. Encryption and decryption are tested on RGB and 8-bit gray-level images.

2. MAZE GENERATORS

Mazes are the structures that are impossible to find a way out due to their complex branching passages, pathways and walls. According to Greek mythology, the palace built by architect Daedalus for King of Crete Minos is also called maze. Remains of maze structured buildings are found in the archaeological excavations held in countries such as Crete and Egypt. Today, mazes have been source of inspiration to many computer games and academic studies.

In the literature, there are many methods to create mazes. These methods have different features from each other [11]. A maze basically consists of cells, walls, a starting and an ending cell. A maze should have a complicated path [12]. Most of the excellent mazes have a rectangular structure. A rectangular maze is created in dimensions in $m \times n$ (width: m cells, height: n cells). If there is only one path between two cells, then this maze is called as a perfect maze. Considering the security, a maze should have one exit only [11]. Basic components of a maze are shown in Figure 1.

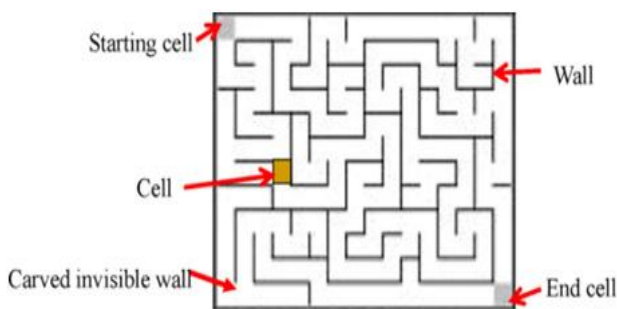


Fig -1: An example to illustrate a maze structure [11]

In this study, mazes should be generated very quickly due to the large file size of the images. Therefore, DFS algorithm, which creates mazes and finds the solution quickly, is used. Considering the image security, the maze should be extremely complicated and difficult to solve. In the present study, the width and height of the maze is the same with the size of the image to be encrypted.

3. DEPTH FIRST SEARCH MAZE ALGORITHM

DFS is an algorithm that can be used to create a maze. Recursion and stack structures are used to apply the method. Basically, any point can be selected as the starting point [13,14]. In this study, the upper left corner is specified as the starting point and the bottom right corner is specified as the end point. A grid -consists of n rows and m columns- is defined to apply the method.

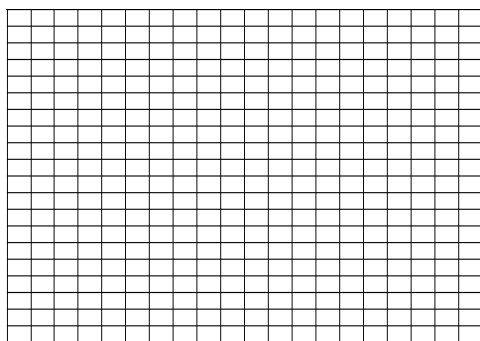


Fig -2: Segmentation in dimensions $n \times m$

A neighboring cell is selected randomly since no cell has been visited yet. The wall between these two neighboring cells is removed and the new cell is added to the stack. If there is a dead-end, we backtrack using the information in stack and all visited cells are marked. If it is not a dead-end, a new path connecting these two cells is drawn. These processes continue until all the cells are visited. Pseudo code of the DFS algorithm is given in [13, 15]. A maze sample obtained using the DFS algorithm is shown in Figure 3.

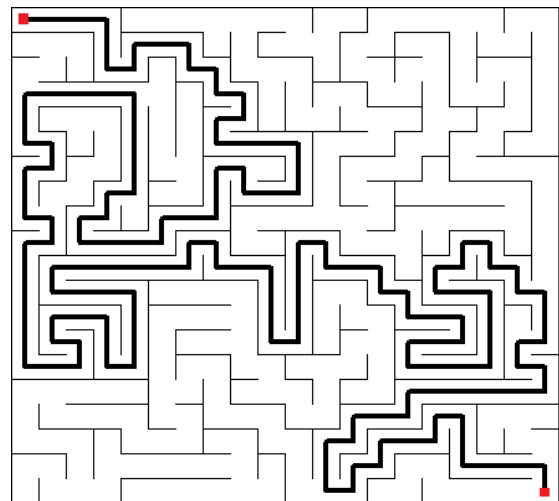


Fig -3: Example of a maze generated by DFS algorithm

In the DFS algorithm, neighbor cells are selected at random. However, if selection of neighbor cells is performed depending on a random number generator (RNG) and seed value, the same maze would be generated all the time. The password identified in this study is going to be used as the seed value for RNG.

4. PROPOSED METHOD FOR IMAGE ENCRYPTION AND DECRYPTION

The main idea of the MBIEA method is obtaining a secret key from pixel values located in the center of gravity of the cells on the solution of a maze generated using a passcode and encrypting the images by using the secret key obtained. The DFS algorithm is used to obtain the maze and its solution. The size of the maze generated is same with the image to be encrypted. The block diagram of the method is given in Figure 4.

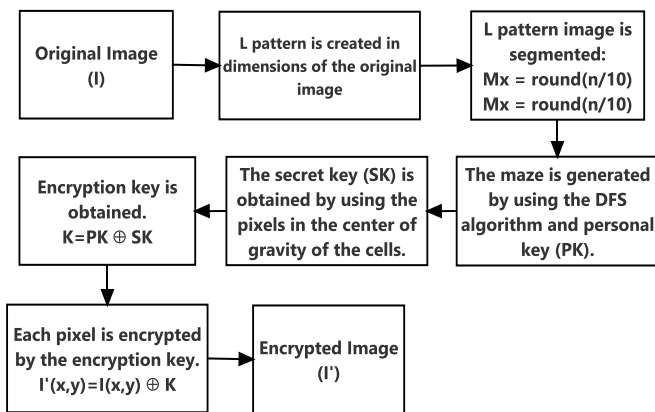


Fig -4: Block diagram of the method

An image (L) is created with a white background in dimensions $n \times m$ (the width of the image is n and the height is m) for the original image (I). L pattern image is the surface where the maze will be created on. Before creating the maze, a grid shown in Figure 2 is obtained on the L pattern image. Dimensions of each cell (width M_x and height M_y) are calculated by Equation (1).

$$M_x = \text{round}\left(\frac{m}{10}\right)$$

$$M_y = \text{round}\left(\frac{m}{10}\right) \tag{1}$$

The maze is generated by using the DFS algorithm and personal key (PK) of the user. In this method, the center of the gravity of the cell located on the upper left corner of the maze is selected as the starting point and the center of the gravity of the cell located on the lower right corner is selected as the end point. Different start and end points can also be selected. The solution path of the maze is drawn between coordinates corresponding to each cell's center of gravity.

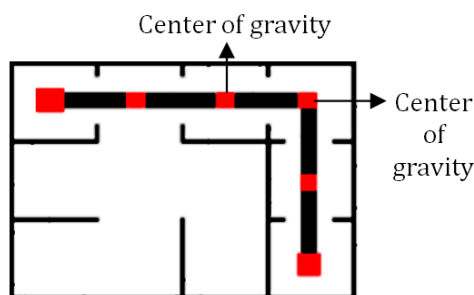


Fig -5: The center of gravity and connection of two cells

The dimensions of the maze image are same as the dimensions of the original image. Grey level color values are collected if the picture is a grey image where RGB values of the pixel is corresponding to the center of gravity coordinates of the cell. The total pixel color value is

represented by the secret key (SK). Different secret keys will be obtained in different solutions. The personal key and secret key are subjected to XOR process in order to make it more difficult to obtain the secret key. The new value obtained is used for encrypting the original image. The process of obtaining the key to be used for encryption is shown in equation (2).

$$K = PK \oplus SK \tag{2}$$

The encrypted 'I' image is obtained using equation (3) by subjecting each pixel value of the original image to XOR process with the help of resulting key (K)

$$I'(x,y) = I(x,y) \oplus K \tag{3}$$

The same steps are repeated to access the original image from the encrypted image. The original image can be obtained only by knowing the personal password.

5. SIMULATION AND SECURITY RESULTS

The commonly used "baboon.bmp" image with 512×512 dimensions and image processing area is used to test the proposed method. Assuming that the personal key is "1a23f4", the maze obtained and resulting images are presented in Figure 6.

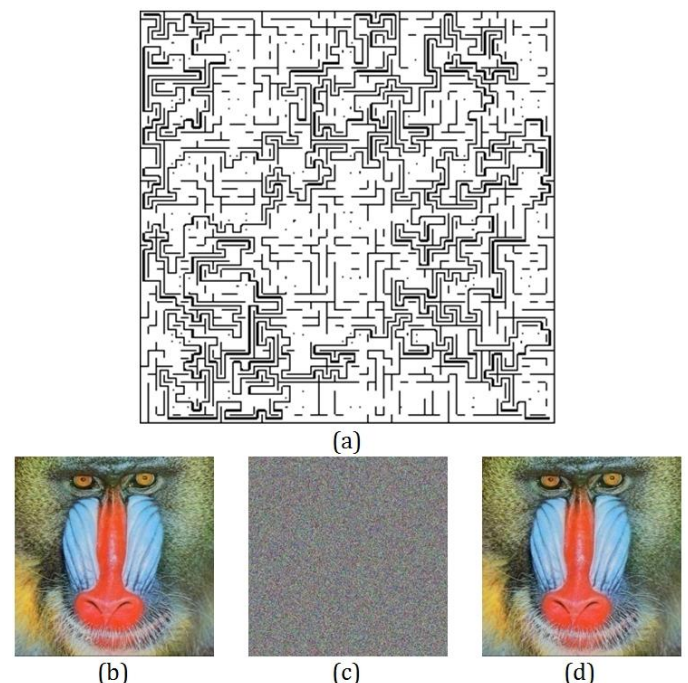


Fig -6: Application images a) created maze, b) original image, c) encrypted image, d) decrypted image

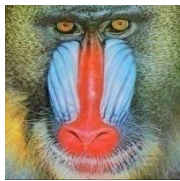



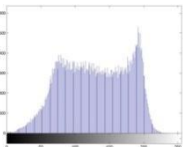
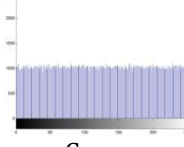
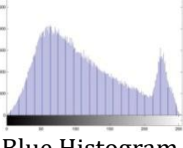
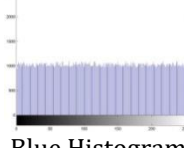

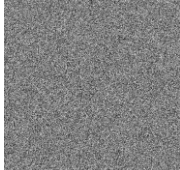
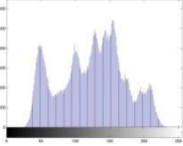
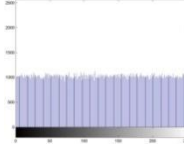
The security analyses of the proposed method are discussed in sections 5.1, 5.2, 5.3 and 5.4. The results

obtained by performing histogram, correlation, entropy and time analyses are given in detail.

5.1 Histogram Analysis

Histograms are used to show the distribution of grey level pixel values in the image. Pixel distributions in an encrypted image are extremely important [16]. An attacker can create a frequency analysis that serves to reveal the secret key or even pixels by using a histogram. These types of attacks are known as statistical attacks. Histograms of the original image and encrypted image should be different from each other in order to prevent the statistical attacks. Therefore, histogram of the encrypted image should show a relatively flat or statistically uniform distribution. Histogram distributions of colored "baboon" and grey level "lena" images of the proposed method are shown in Table 1.

Table-1: Histograms of the original and encrypted images

Original and Encrypted Images	Histograms of Original Images	Histograms of Encrypted Images
 	 Red Histogram	 Red Histogram
	 Green Histogram	 Green Histogram
	 Blue Histogram	 Blue Histogram
 	 Gray Image Histogram	 Gray Image Histogram

Considering the encrypted image histograms shown in Table 1, it is clearly seen that encrypted image histograms are distributed differently and homogeneously compared to decrypted image histograms. Thus, the method proposed is considered to be resistant to statistical attacks.

5.2 Correlation Analysis

Statistical correlation is a measure indicating the strength of the linear relationship between two random variables [17]. Assume that x and y are two variables in a series consisting of n elements, the correlation coefficient can be calculated by equation (4).

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

The parameters given in equation (4) can be obtained with the help of equations (5), (6) and (7).

$$\text{cov}(x,y) = \frac{1}{n} \sum_{i=0}^n [x_i - E(x)][y_i - E(y)] \tag{5}$$

$$D(x) = \frac{1}{n} \sum_{i=0}^n [x_i - E(x)]^2 \tag{6}$$

$$E(x) = \frac{1}{n} \sum_{i=0}^n x_i \tag{7}$$

In this study, 2,000 randomly selected pixels adjacent to each other are used for each encrypted image in all directions (horizontal, vertical and diagonal) to calculate the correlations of the pixels in the encrypted image. Results of the original images are presented in Table 2 and results of the encrypted images are presented in Table 3, respectively.

Table -2: Original images correlation

Original images	baboon	lena	Average
Horizontal	0.9231	0.9719	0.9475
Vertical	0.8660	0.9850	0.9255
Diagonal	0.8543	0.9593	0.9068

Table -3: Encrypted images correlation

Encrypted images	baboon	lena	Average
Horizontal	0.0009	0.0013	0.0011
Vertical	0.0016	-0.0014	0.0001
Diagonal	0.0004	0.0008	0.0006

There is a strong linear relationship between adjacent pixels in any encrypted image. A high correlation coefficient is characterized as close to +1 and -1. In other

words, close correlation values to +1 and -1 mean that there is a strong correlation between the pixels. On the other hand, the correlation coefficients close to 0 means that there is a weak correlation between the pixels. Considering the data given in Table 2, the correlation coefficient of the original image seems to be very close to 1, whereas as it can be seen in Table 3, the correlation coefficient of the encrypted image is very close to 0. Considering these results, the proposed encryption method fixes the relationship between adjacent pixels close to 0 and gives successful results. The distribution of correlation between the pixels is presented in Figure 7 for a better understanding. Correlation distributions of the original images are given in the left column and correlation distributions of the encrypted images are given in the right column, respectively. Considering these distributions, pixels of the encrypted image seem to spread evenly along the plane.

the value of entropy is smaller than 8, respectively. If the value of entropy is extremely smaller than 8, it is considered to be a threat against the security [18].

Considering that encrypted images are random messages, the ideal entropy value is expected to be 8. In a grey level image, the grey value 256 ($m_1=1, m_2=2, \dots, m_{256}=256$) and probability of each grey value is obtained from histogram of the image. Entropy test results of the original and encrypted images are given in Table 4.

Table -4: Entropy test results

Image	Size	Entropy original images	Entropy encrypted images
lena	512×512	7.4455	7.9992
baboon	512×512	7.7624	7.9998
Average		7.6039	7.9995

Considering the data given in Table 4, entropy values of the encrypted images seem to be very close to 8. Thus, the method proposed is considered to be resistant to statistical attacks.

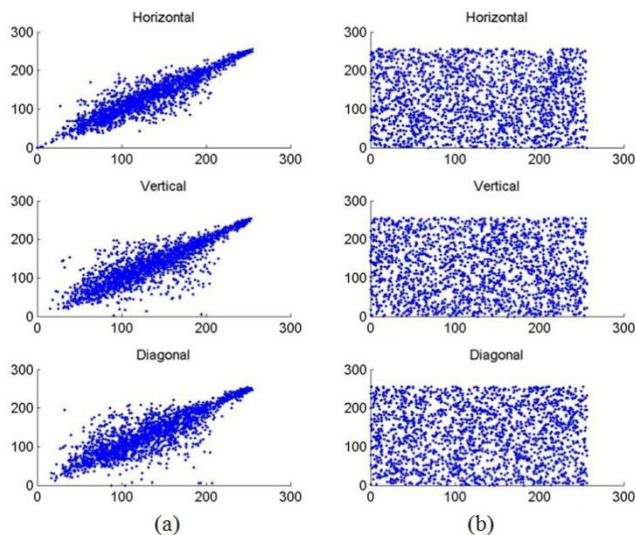


Fig -7: Correlation distributions between adjacent pixels in the original and encrypted “lena” image a) correlation distributions of original image, b) correlation distributions of encrypted image

5.4 Time Analysis

A total of 100 images within 512 × 512 pixel dimensions are selected randomly to test the speed of the method. The use key is assumed to be "1a23f4" for each image. Maze generation and encryption times for 100 images by taking these values into consideration along with maze generation times for encrypted images and decoding are presented in Chart 1 as milliseconds.

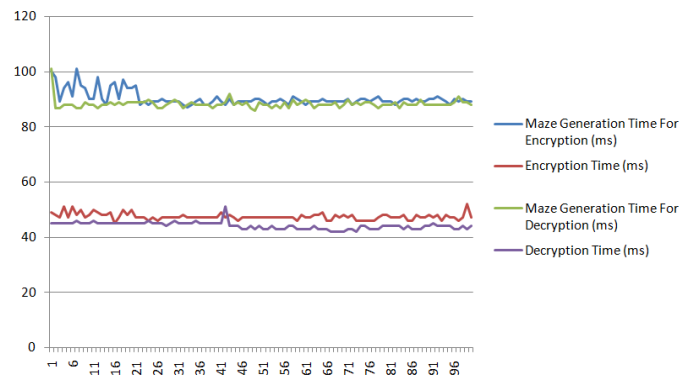


Chart -1: Time spent for encryption, decryption and maze generation for both operations

5.3 Entropy Analysis

Entropy is defined as the randomness and disorder in a system. Entropy of the m message is calculated by equation (8).

$$H(m) = \sum_{i=0}^{M \times N - 1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (8)$$

Where $P(m_i)$ represents the probabilities of m_i symbols in a message and $M \times N$ represents the total number of symbols. In a random message, the ideal entropy value is equal to 8 and in messages with lower rate of randomness,

5.5 Comparison with Other Methods

In this section, correlation coefficient and entropy values of the proposed method is compared statically with other methods. Comparison results are given in Table 5. In this table, H represents “High”, L represents “Low” and NS represents “Nearly the same”, respectively. Since results

are obtained on more than one image within the references examined, the average values of the results in the references are taken into account for comparisons.

Table -5: Comparison of the proposed method with other methods (H: high, L: low, NS: nearly the same)

References	Features	Encrypted image	MBIEA	
[1]	Correlation coefficient	Horizontal	-0.0065	H
		Vertical	not calculated	0.0001
		Diagonal	not calculated	0.0006
	Entropy (Average)		7.9972	H
[16]	Correlation coefficient	Horizontal	-0.0004	L
		Vertical	-0.0035	H
		Diagonal	0.00006	L
	Entropy (Average)		7.6738	H
[19]	Correlation coefficient	Horizontal	0.0052	H
		Vertical	0.0539	H
		Diagonal	0.1141	H
	Entropy (Average)		not calculated	7.9995
[20]	Correlation coefficient	Horizontal	0.0041	H
		Vertical	-0.0337	H
		Diagonal	not calculated	0.0006
	Entropy (Average)		not calculated	7.9995
[21]	Correlation coefficient	Horizontal	0.0014	L
		Vertical	0.0036	H
		Diagonal	0.0027	H
	Entropy (Average)		not calculated	7.9995
[22]	Correlation coefficient	Horizontal	0.0010	NS
		Vertical	0.0060	H
		Diagonal	0.0910	H
	Entropy (Average)		7.9981	H
[23]	Correlation coefficient	Horizontal	0.0024	H
		Vertical	-0.0231	H
		Diagonal	0.0013	H
	Entropy (Average)		not calculated	7.9995
[24]	Correlation coefficient	Horizontal	0.1645	H
		Vertical	0.1901	H
		Diagonal	not calculated	0.0006
	Entropy (Average)		7.9970	L
[25]	Correlation coefficient	Horizontal	0.0284	H
		Vertical	-0,0189	H
		Diagonal	not calculated	0.0006
	Entropy (Average)		not calculated	7.9995
[26]	Correlation coefficient (Average)	Horizontal	0.00043	L
		Vertical	0.00043	L
		Diagonal	0.00043	L
	Entropy (Average)		7.9957	H
[27]	Correlation coefficient	Horizontal	0.0319	H
		Vertical	0.0029	H
		Diagonal	0.0013	H
	Entropy (Average)		7.9973	H
[28]	Correlation coefficient	Horizontal	0.0574	H
		Vertical	0.0265	H
		Diagonal	0.0072	H
	Entropy (Average)		6.4023	H
[29]	Correlation coefficient	Horizontal	0.0007	L
		Vertical	0.0086	H
		Diagonal	-0.0057	H
	Entropy (Average)		7.9972	H
[30]	Correlation coefficient	Horizontal	0.0040	H
		Vertical	0.0046	H
		Diagonal	not calculated	0.0006
	Entropy (Average)		7.8412	H

6. CONCLUSIONS

In this study, a maze-based method has been proposed for encrypting and decrypting images. When we compared the proposed method with other methods in the literature, it seems to have a very high success rate. In the method, considering the starting (top left) and ending (bottom right) points of the maze, different maze and solutions are obtained depending on personal key of the user. The secret key is calculated depending on this. Thus, it is clear that a much larger key space can be obtained by changing the starting and end points of the maze. In such a case, the original image can be accessed by knowing the personal key of the user only. According to the information obtained from experimental results, it seems possible to use the proposed method to ensure the security of the image.

REFERENCES

- [1] S. Rohith, K.N. Hari Bhat, A.N. Sharma, "Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift", International Conference on Advances in Electronics Computers and Communications (ICAIECC), Bangalore(India), pp. 1-6, Oct. 2014. DOI:10.1109/ICAIECC.2014.7002404
- [2] P.R. Sankpal, P.A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey", 2014 Fifth International Conference on Signal and Image Processing (ICSIP), Karnataka (India), pp. 102-107, 8-10 Jan. 2014. DOI:10.1109/ICSIP.2014.80
- [3] L. Abraham, N. Daniel, "Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research, vol. 2, pp. 186-189, 2013.
- [4] M.B. Younas, J. Ahmad, "Comparative analysis of chaotic and non-chaotic image encryption schemes", In: 2014 International Conference on Emerging Technologies (ICET), Islamabad(Pakistan), pp. 81-86, 8-9 Dec. 2014. DOI:10.1109/ICET.2014.7021021
- [5] A. Sinha, K. Singh, "A technique for image encryption using digital signature", Optics Communications, vol. 218, pp. 229-234, 2003. DOI:10.1016/S0030-4018(03)01261-6
- [6] S.S. Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition, vol. 34. pp. 1229-1245, 2001.
- [7] C.C. Chang, M.S. Hwang, T.S. Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software; vol. 58, pp. 83-91, 2001.

- [8] J.I. Guo, J.C. Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", 10th VLSI Design/CAD Symposium, Nantou(Taiwan), pp. 327-330. 18-21 August 1999.
- [9] J.C. Yen, J.I. Guo, "A new chaotic image encryption algorithm", In: Proceedings of National Symposium on Telecommunications, Taiwan, pp. 358-362, 1998.
- [10] Y.V. Mitra, R. Subba, S.R.M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering, vol.1, pp.127-131, 2006.
- [11] T. Sukumar, K.R. Santha, "Maze Based Data Hiding Using Back Tracker Algorithm", International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 499-504, 2012.
- [12] H.L. Lee, C.F. Lee, L.H. Chen, "A perfect maze based steganographic method", Journal of Systems and Software, vol. 83, pp. 2528-2535, 2010. DOI:10.1016/j.jss.2010.07.054
- [13] R. Zhang, M. Yang, F. Wang, "Design and Implement of the Complex Maze Shortest Path Simulation System Based On Improved Ant Colony Optimization Algorithm", Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Harbin(China), pp. 779-783. 18-20 Sep. 2014. DOI:10.1109/IMCCC.2014.165
- [14] T. Terzimehic, S. Silajdzic, V. Vajnberger, J. Velagic, N. Osmic, "Path Finding Simulator for Mobile Robot Navigation", XXIII International Symposium on Information, Communication and Automation Technologies (ICAT), Sarajevo (Bosnia Herzegovina), pp. 1-6. 27-29 Oct. 2011. DOI:10.1109/ICAT.2011.6102086
- [15] S. Mahmud, U. Sarker, M. Islam, H. Sarwar, "A Greedy Approach in Path Selection for DFS Based Maze-map Discovery Algorithm for an Autonomous Robot", 15th International Conference on Computer and Information Technology (ICCIT), Chittagong (Bangladesh), pp. 546-550. 22-24 Dec. 2012. DOI:10.1109/ICCITechn.2012.6509798
- [16] S.K. Naveenkumar, H.T. Panduranga, "Triple image encryption based on integer transform and chaotic map", International Conference on Optical Imaging Sensor and Security (ICOSS), Tamil Nadu(India), pp. 1-6. 2-3 July 2013. DOI: 10.1109/ICOISS.2013.6678416
- [17] C.E. Shannon, "A Mathematical Theory of Communication", The Bell System Technical Journal, vol.27, pp. 379-423, 623-656. 1948.
- [18] R. Munir, "Security analysis of selective image encryption algorithm based on chaos and CBC-like mode", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Bali(Indonesia), pp. 142-146. 30-31 Oct. 2012. DOI: 10.1109/TSSA.2012.6366039
- [19] K. Sakthidasan, B.V. Santhosh-Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, vol.1(2), pp. 137-141, 2011. DOI:10.7763/IJIEET.2011.V1.23
- [20] N.K. Pareek, V. Patidar, K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, vol.24(9), pp. 926-934, 2006. DOI:10.1016/j.imavis.2006.02.021
- [21] S. Ahadpour, S. Yaser, "A chaos-based image encryption scheme using chaotic coupled map lattices", International Journal of Computer Applications, vol.49, pp. 15-18, 2012. DOI:10.5120/7599-0311
- [22] K. Gupta, S. Sanjay, "New approach for fast color image encryption using chaotic map", Journal of Information Security, vol.2, pp. 139-150, 2011.
- [23] M.T. Rodriguez-Sahagun, J.B. Mercado-Sanchez, D. Lopez-Mancilla, R. Jaimes-Reategui, J.H. Garcia-Lopez, "Image encryption based on Jacobi function", International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), Morelos (Mexico), pp. 109-114, 19-22 Nov. 2013. DOI:10.1109/ICMEAE.2013.20
- [24] S.K.N. Kumar, H.S.S. Kumar, H.T. Panduranga, "Hardware software co-simulation of dual image encryption using Latin square image", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode(India), pp. 1-5. 4-6 July 2013. DOI:10.1109/ICCCNT.2013.6726681
- [25] A. Paul, N. Das, A.K. Prusty, C. Das, "RGB image encryption by using discrete log with and Lorenz's chaotic function", 4th IEEE International Conference on Computer and Communication Technology (ICCCT), Allahabad(India), pp. 199-204. 20-22 Sep. 2013. DOI:10.1109/ICCCT.2013.6749627
- [26] R. Afarin, S. Mozaffari, "Image encryption using genetic algorithm and binary patterns", 10th International ISC Conference on Information Security and Cryptology (ISCISC), Yazd(Iran), pp. 1-5. 29-30 Aug. 2013. DOI: 10.1109/ISCISC.2013.6767332
- [27] S. Sheng, X. Wu, "A novel bit-level image encryption scheme using hyper-chaotic systems", 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Shenyang(China), pp.1015-1019, 23-25 July 2013. DOI:10.1109/FSKD.2013.6816344
- [28] S. Saeed, M.S. Umar, M.A. Ali, M. Ahmad, "A gray-scale image encryption using Fisher-Yates chaotic shuffling in wavelet domain", Recent Advances and Innovations in Engineering (ICRAIE), Jaipur(India), pp.1-5. 9-11 May 2014. DOI:10.1109/ICRAIE.2014.6909175
- [29] T. Gopalakrishnan, S. Ramakrishnan, M. Balakumar, "An image encryption using chaotic permutation and

diffusion", International Conference on Recent Trends in Information Technology (ICRTIT), Chennai(India),pp. 1-5, 10-12 Apr. 2014.
DOI:10.1109/ICRTIT.2014.6996091

- [30] M.G. Avasare, V.V. Kelkar, "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai(India), pp. 1-6. 15-17 Jan. 2015.

BIOGRAPHIES



Erdal Güvenoğlu graduated from Trakya University, Turkey, in 2001. He took M.Sc. degree from Trakya University, Turkey, in 2005, all in Computer Engineering. He took Ph.D. degree from Computer Engineering, Trakya University, Turkey, in 2012. His interest areas include image processing, image encryption, steganography and computer programming.