Electronic Letters on Science & Engineering 18(2) (2022)
Available online at dergipark.org.tr/else

An Efficient Method for Digital Image Encryption Based on Improved Chaotic Map

Muhammed MİLANİ[1*], Salim CEYHAN [2]

[1]Department of Computer Engineering, Bandirma Onyedi Eylul University, Balikesir, Turkey
Email: mmilani@bandirma.edu.tr, ORCID: 0000-0003-2450-0280
[2]Department of Computer Engineering, Bilecik Şeyh Edebali University, Bilecik, Turkey
Email: salim.ceyhan@bilecik.edu.tr, ORCID: 0000-0003-0274-6175

Abstract: With the development of information technologies and the increasing possibility of unauthorized access to data published on the Internet, the need to take care of data has become an important issue. One method that can be useful in data security is encryption. By using data encryption, data can be easily distributed in different environments safely. This paper presents and investigates an encryption method based on chaos theory for digital images. The chaotic mapping used in this paper is the Baker function, a two-dimensional function with chaotic properties in some situations. According to the research in analyzing systems based on chaos maps, the improved Baker function has been used in this article. The desired function increases the security of the proposed system against attacks. The tests and analyses performed on encrypted images show that the presented method has the necessary efficiency.

Keywords: Image Encryption, Chaotic map, Random number, Baker map.

İyileştirilmiş Kaotik Haritaya Dayalı Bir Dijital Görüntü Şifreleme Yöntemi

Özet: Bilişim teknolojilerinin gelişmesi ve internette yayınlanan verilere yetkisiz erişim olasılığının artmasıyla birlikte verilerin korunması ihtiyacı önemli bir konu haline gelmiştir. Veri güvenliğinde faydalı olabilecek yöntemlerden biri şifrelemedir. Veri şifreleme kullanılarak, veriler farklı ortamlarda güvenli bir şekilde kolayca dağıtılabilir. Bu makale, dijital görüntüler için kaos teorisine dayalı bir şifreleme yöntemini sunmakta ve incelemektedir. Bu yazıda kullanılan kaotik haritalama, bazı durumlarda kaotik özelliklere sahip iki boyutlu bir fonksiyon olan Baker fonksiyonudur. Kaotik haritalarına dayalı sistemlerin analizinde yapılan araştırmaya göre, bu makalede iyilelştirilmiş Baker fonksiyonu kullanılmıştır. İstenilen fonksiyon, önerilen sistemin saldırılara karşı güvenliğini arttırır. Şifrelenmiş görüntüler üzerinde yapılan testler ve analizler, sunulan yöntemin gerekli verimliliğe sahip olduğunu göstermektedir.

Anahtar Kelimeler: Görüntü Şifreleme, Kaotik harita, Rastgele sayı, Baker haritası.

Reference to this paper should be made as follows (bu makaleye aşağıdaki şekilde atıfta bulunulmalı):
Milani, M., Salim, C. 'An Efficient Method for Digital Image Encryption Based on Improved Chaotic Map', Elec Lett Sci Eng, vol. 18(2) , (2022), 87-96

INTRODUCTION

There are many contexts where people share their data across various communication channels. Publishing data in different environments that are often available to the public can be unsafe and bring security risks [1,2]. For this purpose, various methods have been developed to secure data transmission. One of the ways to secure data transmission is data encryption. Using data encryption, they can be published more easily in different environments. Of course, data encryption can be done in different ways to protect data from unauthorized access, such as steganography and watermarking [3-6]. Data encryption has been investigated in different ways and methods. Some encryption methods are based on traditional methods [7], and some have used modern methods [8]. Some encryption methods have been proposed for textual data [9,10], some for image data [11, 12], and some for audio data [13].

In the meantime, encryption of images is one of the most important topics that play an important role in multimedia programs for the security of images and can solve the concerns that exist in the field of communication for the safe transmission of multimedia data [14]. The features that

* *Corresponding author; Tel.:+905317203041, mail mmilani@bandirma.edu.tr*

distinguish image encryption from other encryptions are a strong correlation between data, high compatibility, and high redundancy of image data. Also, images have a higher data volume than textual data [15]. According to the characteristics of digital images, using traditional methods such as AES or DES cannot be efficient because these methods involve low speed and small key space [16]. Therefore, various and more modern methods for image encryption were proposed [17,18].

Among the effective methods for image encryption is the use of chaotic systems. Chaotic systems have features that can be very efficient in generating pseudo-random numbers and can be used in image encryption. The effective characteristics of chaotic mappings are their high sensitivity to initial values and high periodicity. The characteristics of chaos maps make it possible to generate pseudo-random numbers with random characteristics and high speed. Many studies have shown that chaotic functions can be very effective for image encryption [19-21].

However, two categories of chaotic systems have been proposed, one-dimensional and multi-dimensional. One-dimensional chaotic functions have a simpler structure and are executed easily and at a much higher speed [22]. Nevertheless, One-dimensional chaotic functions are somewhat less reliable in terms of security since they have been widely discussed and many studies have been conducted on them, it becomes [23]. Of course, the multi-dimensional chaos functions have also lost their reliability with the same point of view. Recently, studies have been done on increasing the security power of chaos functions [24]. In this article, we will use a special type of function improved from a chaos function called Baker map, which has been proven to have a higher degree of confidence [25]. Usually, image encryption systems are analyzed in two phases: key generation and pixel encryption. In the key generation phase, a sequence of pseudo-random data is generated, and chaotic mappings are used in this phase. The pseudo-random data generated in the encryption phase is mixed with the pixel data of the images, and the encryption operation and the generation of encrypted images are performed.

In this paper, we used the Baker map chaotic function to generate a sequence of random numbers. The random data generated in the cryptographic operation is used according to the algorithm presented in section 3 of the article. The second part chaos systems and especially the Baker map function, and the proposed algorithm will be discussed in the third part. The fourth section will evaluate the proposed method.

1. Chaotic Maps

Chaos theory is one of the theories that is considered in dynamic systems. *Dynamic systems* change over time and have a special place in many sciences, including physical and behavioral sciences [26, 27]. Even though the discussion of the Chaos has been discussed before, the beginning of studies of this theory can be seen in 1965 by a person named Edward Lorenz, who researched meteorological issues [28]. By studying chaotic systems, he concluded that a slight change in the initial conditions of meteorological forecasts causes large fluctuations in the system's response.

The word chaos loosely defines disorder and lack of any structure or order. However, it must be said that chaotic systems' behavior seems random. However, there is no necessity for the existence of an element of accident in creating chaotic behavior, and certain dynamic systems (deterministic) can also show chaotic behavior. Today, chaos theory has gained much influence in various fields and tendencies. As such, it is hard to find a science or organization with no traces of chaos. Various functions behave chaotically under certain conditions. This article used the Baker map function, a two-dimensional mapping. In the rest of this section, we will first introduce the standard form of the Baker map and then examine its expanded version.

1.1. Baker map

A baker's map is a chaotic map obtained from the unit square inward. This function is topologically like a conjugate horse map. Like most chaotic maps, the baker's function also has chaotic characteristics in the special conditions that the operator creates. The generalized function related to the baker's map is given in equation 1.

$$(x_n, y_n) = \begin{cases} (\frac{x_{n-1}}{\alpha}, \alpha y_{n-1}) & , 0 < x_{n-1} \leq \alpha \\ (\frac{x_{n-1}-\alpha}{1-\alpha}, (1-\alpha)y_{n-1} + \alpha) & , \alpha < x_{n-1} \leq 1 \end{cases} \quad (1)$$

where α is a control parameter, if α is in the interval (0, 1) can produce results with chaotic characteristics.
Its state space is limited if the chaos functions are generated on a limited precision computing device such as a computer. In such cases, the sequences created with these chaos functions naturally become periodic. In such a case, the desired chaotic function does not satisfy its chaotic expectation. Such a state is called dynamic destruction [29]. Chaos maps cannot be considered secure enough for encryption despite dynamic destruction. Therefore, this article used the chaos function's improved version to solve the dynamic degradation problem.

1.2. Improved Baker map

According to the proposed method in [25], the following linear function can substitute the parameter a to eliminate the problem of dynamic destruction based on the Delay-introducing method.

$$g(x_i) = bx_i + by_i + 1 - 2b \quad (2)$$

where 0 < b < 1 is the linear coefficient. By applying equation 2 and general relation 1, we can consider the Delay-introducing mapping of the baker's function as equation 3.

$$(x_n, y_n) = \begin{cases} (\frac{x_{n-1}}{g(x_{n-1})}, \ g(x_{n-1})y_{n-1}) & , 0 < x_{n-1} \leq \alpha \\ (\frac{x_{n-1}-g(x_{n-1})}{1-g(x_{n-1})}, \ (1-g(x_{n-1}))y_{n-1} + g(x_{n-1})) & , \alpha < x_{n-1} \leq 1 \end{cases} \quad (3)$$

In this article, the improved function of the baker is used to generate pseudo-random numbers.

2. Proposed Method

The structure of digital images is such that each image contains several points called pixels. Each pixel has three numerical values between 0 and 255 that define that point's red, green, and blue values. There are two main methods for encrypting images, one of which is to change the numerical values of pixels, and the other is to move the values between pixels. In our proposed method, the change in the numerical values of the pixels is considered. However, the position of each point is also used along with the random number generated in the algorithm.
The proposed method generally creates 256 non-repeating sequences of random numbers between 0 and 255. The generated random array is used to select and change the value of the pixels. Baker mapping is used to generate this list. The initial values of the baker's mapping are calculated from the key value received by the user as an encryption key. The proposed algorithm selects each pixel of the image. It generates a new value for the corresponding pixel in the encrypted image based on the numerical value of the pixel, position, and random list.

2.1. Random List Generation

The improver Baker's mapping according to equation 3 is used in the proposed method. Two initial values and a coefficient called b are required for this mapping. The required initial values are obtained from the encryption key. Moreover, to create chaotic conditions, the value of b is considered equal to 0.2.
The ASCII code value of each character is calculated from the encryption key to generate the initial values. Then, each ASCII code is converted to its base two equivalent, creating a sequence of binary numbers. The binary sequence generated by equation 4 creates the initial values of x_0 and y_0.

$$\begin{cases} x_0 = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{7} k_{i,j}*2^{i*8+j}}{2^{n*8}} \\ y_0 = \frac{\sum_{i=n-1}^{0}\sum_{j=0}^{7} k_{i,j}*2^{i*8+j}}{2^{n*8}} \end{cases} \quad (4)$$

Here, $k_{i,j}$ is the binary value corresponding to the i^{th} character and its j^{th} bit, and n is number of characters in encryption key.
The initial values generated from equation 4 are placed in equation 3 and create a random sequence of numbers between 0 and 1. These random numbers should be mapped to the range from 0 to 255, which was produced by multiplying it by 255. Random numbers generated from 0 to 255 are placed in a list with a capacity of 256 houses. Of course, it should be noted that there should not be duplicate values in the randomly generated list. An algorithm related to random list generation is given in Listing 1.

List 1. Random List Generation Algorithm

```
ALGORITHM RandomList (KeyStr, b)

    //Generate a non-repeating list of numbers from 0 to 255.
    //Input: KeyStr as encryption key, b as control parameters of Baker's Map
    //Output: RandList as random List of numbers

    i ← 0
    while i<256
        R ← (Random Num)*255  // given from equation 3
        Chk ← 0
        for each L in RandList
            if R == L then
                Chk ← 1
        if  Chk==0 then
            RandList[i] ←R
            i++
    return RandList
```

2.2. Image Encryption

By creating a random list, encryption operations can be started. Image encryption is divided into two parts: Encryption and Decryption, in which the desired encrypted image and the encrypted image are obtained in the Encryption phase. Also, in the decryption stage, the encrypted image on the receiver's side can be converted to the original image. Of course, it should be noted that the same key must be used in both encryption and decryption steps. Otherwise, the decryption operation cannot recover the original file.
Each image pixel is considered separately in the encryption phase, and the encryption operation is performed on it. First, the image file, in the form of a matrix, is converted into a one-dimensional array. Converting to a one-dimensional array is done so that first, the pixels of one row is written

in the array, and then the pixels of the next row is written. This operation is performed until the last row of the image matrix.
Each value in the array obtained from the pixels is read and searched in the randomly created list. The desired value will be present in the list because the generated random list has all the values from 0 to 255. When the searched value is found, the corresponding index in the random list is added with the pixel index read in the image array, and the new position is calculated. Of course, at this stage, the remainder of the obtained total is calculated with 256 and considered a new position. Finally, the value in the index calculated in the random list is considered an encrypted pixel and placed in the corresponding pixel in the cipher image. The operation related to the encryption stage is clearly shown in Figure 1.

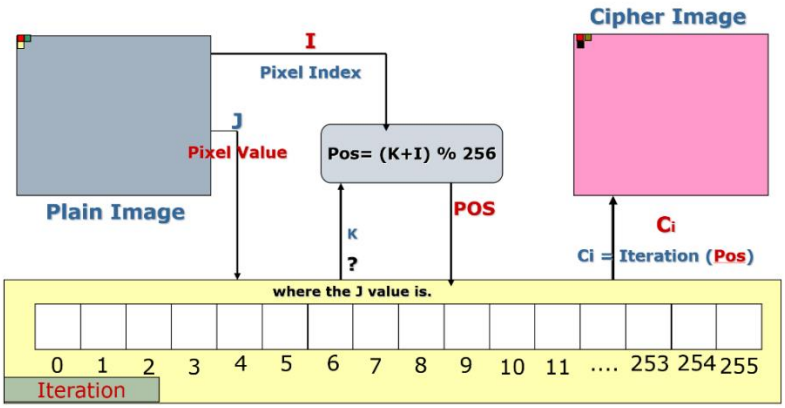
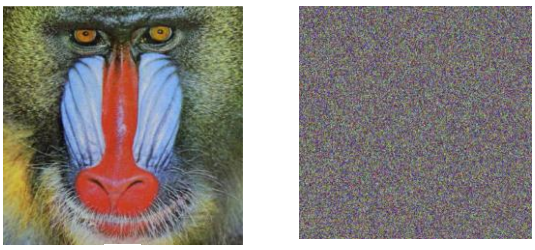


Figure 1 Operations related to image encryption

Considering that the encrypted image data is provided from the random list, the values will be between 0 and 255, and there will be no problem regarding the digital image data ranges. Figure 2 shows an example of an image file and its encrypted image.



(a) (b)

Figure 2- The Encryption phase for an image and its three colours. (a) Plain Image, (b) Cipher image

2.3. Image Decryption

One of the important features that most methods based on chaos systems have is the use of reversible operators such as mod. This feature makes the decryption phase very similar to the encryption phase. In the proposed method of this article, it is the same way. The only difference between this phase and the Encryption phase is that, in calculating the new index, the indices of the random list and the image array are subtracted, and the remainder is 256. The rest of the cases are similar to the encryption mode.

3. Result and analysis

To see the effectiveness of the proposed system, we implemented the algorithm of the article in the Matlab environment. In the implemented algorithm, the user enters the encryption key, which

can also be a text string to encrypt the image. The desired algorithm creates a random list based on the received key and encrypts the original image. In image encryption, the data of three image layers are considered separately, and each layer creates the encrypted layer separately. By combining the encrypted layers, the encrypted image is also obtained.
On the contrary, this operation should work properly. The original image should be obtained if we decrypt the encrypted image again with the same previous key. Also, suppose the encrypted image is decrypted with a key different from the encrypted key. In that case, the obtained image should not only be the same as the original image but also should not have any similarity with it. Figure 3 shows this clearly.

(a) (b) (c) (d)

Figure 3-(a) Plain image, (b) Cipher image with key_1, (c) Decrypted image with key_1, (d) Decrypted image with key_2

3.1. Differential Analysis

In differential attacks, they usually attempt to find connections that can analyse the encrypted image by changing one bit in the image. If the encryption system creates a condition that many different encrypted images are produced by changing one bit, it can be resistant to differential attacks. Usually, to analyse the efficiency of the system against differential attacks, two important criteria are examined. One of these measures is the number of pixel change rates (NPCR), and the other is the unified average changing intensity (UACI). Relationships 5 and 6 can be used to calculate these two measures.

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} C(i,j)}{N*M} * 100\%, \quad (5)$$

$$UACI = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} |P_1(i,j)-P_2(i,j)|}{255*N*M} * 100\% \quad (6)$$

Where the values of M and N indicate the length and width of the image. Moreover, if $P_1(i, j)$ is assumed as the pixel value of an image before changes, P_2 (i, j) is the value of the same pixel after changes. Table 1 shows the analyses of these two measures for several standard images for the case where alpha equals 0.001.

Table 1 Analysis of NPCR and UACI by changing a pixel at (122,102).

Image Name	NPCR	UACI	NPCR		UACI	
			Limit	Situation	Limit	Situation
Peppers (512*512)	99.6028	33.6092	99.5810	Passed	33.1594 33.7677	Passed
Mandrill (512*512)	99.6203	33.4541	99.5810	Passed	33.1594 33.7677	Passed
Lena (256*256)	99.5636	33.4512	99.5527	Passed	33.1594 33.7677	Passed

As can be seen in Table 1, the two investigated measures have acceptable values. Therefore, this method can effectively resist differential attacks.

3.2. Statistical attack

3.2.1.Correlation Coefficient

Simple correlation analysis is performed to determine the degree, intensity, and strength level and the direction of the relationship between two variables. If both variables are continuous variables and the data related to the variables show a normal distribution, the relationship between the variables is determined by the Pearson correlation coefficient. It is a linear relationship between the desired variables, determined or measured by the correlation coefficient. If the relationship between the variables is not linear, the calculated correlation coefficient is unsuitable for measuring the relationship between the variables. Here, the analysis shown in Figure 4 was performed to determine whether the images have linear relationships between neighboring pixels.

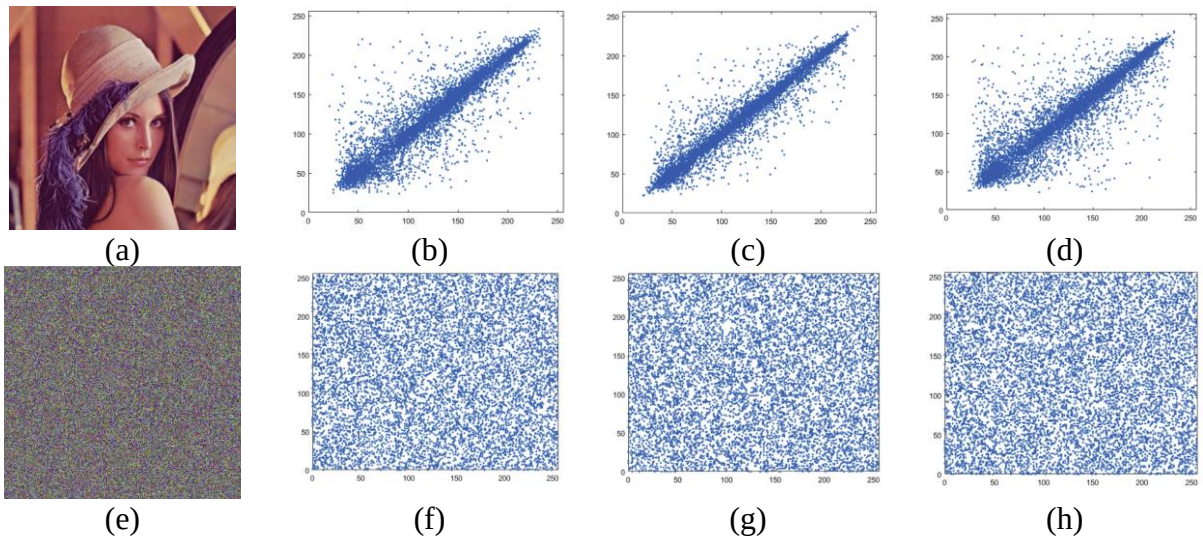


Figure 4. Correlation of two adjacent pixels (a) plain image of Lena; (b) vertical correlation of the plain image; (c) horizontal correlation of the plain image; (d) diagonal correlation of the plain image; (e) Encrypted image of Lena; (f) vertical correlation of the cipher image; (g) horizontal correlation of the cipher image (h) diagonal correlation for the cipher image.

The correlation coefficient of encrypted images can also be calculated to better check the correlation between pixels. In this article, we compared the correlation coefficient of the proposed method with some other methods. Table 2 shows this comparison for Lena image.

Table 2 –Correlation study for the offered method and some different methods

	Vertical	Horizontal	Diagonal
Plain Lena Image	0.9883	0.9906	0.9823
Wang [30]	0.0003	0.0027	0.0012
Chai [31]	0.0014	0.0285	0.0013
Zhang [32]	0.0226	0.0245	0.0193
Alawida [33]	-0.0017	-0.0084	-0.0019
Proposed Method	0.0049	0.0051	0.0011

According to Table 2, it can be seen that the proposed method significantly reduces a strong interaction in a clear image compared to other methods.

3.2.2.histogram analysis

Histogram analysis is among the analyzes that can show the efficiency of an image encryption system. Images with balanced histograms are more resistant to statistical analysis. Usually, images are not composed of balanced histograms; if the encrypted image is not balanced, it can provide hackers with data for image analysis. Therefore, one of the goals of an encryption system is to create encrypted images with a balanced histogram. Figure 5 shows that the system proposed in this article successfully balanced distribution.

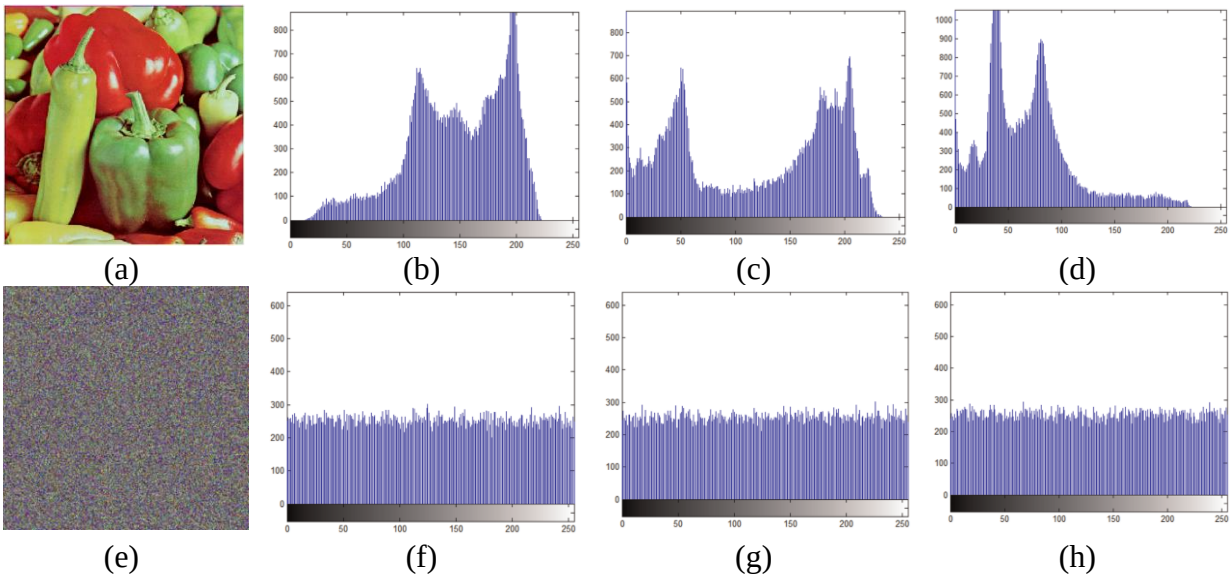


Figure 5. (a) Plain image, (b) R Histogram of Plain image, (c) G Histogram of Plain image, (d) B Histogram of Plain image, (e) Cipher image, (f) R Histogram of Cipher image, (g) G Histogram of Cipher image, (h) B Histogram of Cipher image,

3.3. Information entropy

In information theory, entropy means finding an infinite relationship between random numbers. This expression is based on Shannon's entropy and can be summarized by equation 7.

$$H(S) = \sum_{i=0}^{2N-1} P(s_i)\log\left(\frac{1}{P(s_i)}\right) \qquad (7)$$

If the value of this expression is equal to a small value, it is more suitable for statistical analysis. Therefore, a suitable encryption method should make the value of this expression in the encrypted image as high as possible.

Table 3 Entropy results of some plain and cipher images.

Image Name	Plain Image	Cipher Image
Lena	7.4472	7.9993
Peppers	7.6698	7.9975
House	7.0686	7.9963
Mandrill	7.7624	7.9991

Table 4 Comparing entropy results.

Images	Plain	Proposed Method	Wang [30]	Chai [31]	Zhang [32]	Alawida [33]
Lena	7.4472	7.9993	7.9993	7.9993	7.9885	7.9975

4. Conclusion

In this article, a method for image encryption is proposed. The proposed method is developed based on improved Baker's mapping. The main feature of the developed map is that it has solved the problem of dynamic destruction in chaotic maps. Also, due to the high sensitivity of chaotic functions, the system proposed in this article highly depends on the encryption key. In this sense, it is suitable for image encryption. The results show that the proposed system has sufficient security against attacks and unauthorized use of encrypted images. It should also be noted that the proposed system is well applicable for images of medium size. However, for high-volume images, which is the goal of real-time encryption or the encryption of stream video files, it can have problems such as low execution speed. Due to the daily increase of data published in common digital environments, the need to develop new encryption systems is very serious. Because previous and existing methods are reviewed and analyzed by hackers and unauthorized users, the developed methods will lose their reliability. Therefore, developing new and more resistant methods against attacks can bring more confidence in using common and common environments.

References

[1] Chen, L., Chen, J., Zhao, G., & Wang, S. (2019). Cryptanalysis and improvement of a chaos-based watermarking scheme. IEEE Access, 7, 97549-97565.
[2] Dou, Y., & Li, M. (2020). Cryptanalysis of a new color image encryption using combination of the 1d chaotic map. Applied Sciences, 10(6), 2187.
[3] Milani, M. M. R. A., Pour, S. H., & Pehlivan, H. Steganografi'de Ilke ve Yöntemler, ve Küçük Siyah-Beyaz Görüntüleri için Bir Steganografi Yöntem.
[4] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.
[5] Wadhera, S., Kamra, D., Rajpal, A., Jain, A., & Jain, V. (2022). A Comprehensive Review on Digital Image Watermarking. arXiv preprint arXiv:2207.06909.
[6] Milani, M. A Novel Approach for Hiding Information into Mathematical Expression. Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi, 7(2), 739-754.
[7] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75(10), 6663-6682.
[8] Anandkumar, R., and Kalpana, R. "A Review on Chaos-Based Image Encryption Using Fractal Function", In Examining Fractal Image Processing and Analysis (pp. 23-37). IGI Global (2020).
[9] Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. Procedia Computer Science, 54, 73-82.
[10] Sangwan, N. (2012). Text encryption with huffman compression. International Journal of Computer Applications, 54(6).
[11] Liu, S., Guo, C., & Sheridan, J. T. (2014). A review of optical image encryption techniques. Optics & Laser Technology, 57, 327-342.
[12] Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. Information Sciences, 480, 403-419.
[13] Lima, J. B., & da Silva Neto, E. F. (2016). Audio encryption based on the cosine number transform. Multimedia Tools and Applications, 75(14), 8403-8418.
[14] Hasimoto-Beltrán, R. (2008). High-performance multimedia encryption system based on chaos. Chaos: An Interdisciplinary Journal of Nonlinear Science, 18(2), 023110.
[15] Darwish, S. M., and Noori, Z. H. "Secure image compression approach based on fusion of 3D chaotic maps and arithmetic coding", IET Signal Processing, 13(3), 286-295 (2018).
[16] Wang, X. Y., Yang, L., Liu, R., and Kadir, A. "A chaotic image encryption algorithm based on perceptron model", Nonlinear Dynamics, 62(3), 615-621 (2010).
[17] Abd-El-Atty, B., Iliyasu, A. M., Alanezi, A., & Abd El-latif, A. A. (2021). Optical image encryption based on quantum walks. Optics and Lasers in Engineering, 138, 106403.

[18] Yan, X., Wang, X., & Xian, Y. (2021). Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. Multimedia Tools and Applications, 80(7), 10949-10983.

[19] Suneja, K., Dua, S., & Dua, M. (2019, March). A review of chaos based image encryption. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 693-698). IEEE.

[20] Kumar, M., Saxena, A., & Vuppala, S. S. (2020). A survey on chaos based image encryption techniques. In Multimedia security using chaotic maps: principles and methodologies (pp. 1-26). Springer, Cham.

[21] Milani, M. M. R. A., Pehlivan, H., & Pour, S. H. (2013). Kaos tabanlı bir şifreleme yöntemi ve analizi. XIII. Akademik Bilişim Konferansı Bildiriler Kitabı, 2-4.

[22] Talhaoui, M. Z., and Wang, X. "A new fractional one-dimensional chaotic map and its application in high-speed image encryption", Information Sciences, 550, 13-26 (2021).

[23] Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., and Mosavi, M. R. "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos", Multimedia Tools and Applications, 74(3), 781-811 (2015).

[24] Liu, L., Xiang, H., & Li, X. (2021). A novel perturbation method to reduce the dynamical degradation of digital chaotic maps. Nonlinear Dynamics, 103(1), 1099-1115.

[25] Liu, L., & Miao, S. (2017). Delay-introducing method to improve the dynamical degradation of a digital chaotic map. Information Sciences, 396, 1-13.

[26] Bak, P., Tang, C., & Wiesenfeld, K. (1988). Self-organized criticality. Physical review A, 38(1), 364.

[27] Beek, P. J. (1989). Timing and phase locking in cascade juggling. Ecological Psychology, 1(1), 55-96.

[28] Lorenz, E. N. (1965). On the possible reasons for long-period fluctuations of the general circulation. In Proc. WMO-IUGG Symp. on Research and Development Aspects of Long-Range Forecasting.

[29] Li, S.J., Chen, G.R., Mou, X.Q.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurc. Chaos 15, 3119–3151 (2004)

[30] Wang, X., Feng, L., Li, R., & Zhang, F. (2019). A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. *Nonlinear Dynamics*, *95*(4), 2797-2824.

[31] Chai, X. (2017). An image encryption algorithm based on bit level Brownian motion and new chaotic systems. *Multimedia Tools and Applications*, *76*(1), 1159-1175.

[32] Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications*, *77*(6), 6647-6669.

[33] Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160, 45-58