Rageed Hussein AL-Hashemy* and Sadiq A. Mehdi

A New Algorithm Based on Magic Square and a Novel Chaotic System for Image Encryption

https://doi.org/10.1515/jisys-2018-0404
Received October 3, 2018; previously published online February 1, 2019.

Abstract: This article introduces a simple and effective new algorithm for image encryption using a chaotic system which is based on the magic squares. This novel 3D chaotic system is invoked to generate a random key to encrypt any color image. A number of chaotic keys equal to the size of the image are generated by this chaotic system and arranged into a matrix then divided into non-overlapped submatrices. The image to be encrypted is also divided into sub-images, and each sub-image is multiplied by a magic matrix to produce another set of matrices. The XOR operation is then used on the resultant two sets of matrices to produce the encrypted image. The strength of the encryption method is tested in two folds. The first fold is the security analysis which includes key space analysis and sensitivity analysis. In the second fold, statistical analysis was performed, which includes the correlation coefficients, information entropy, the histogram, and analysis of differential attacks. Finally, the time of encryption and decryption was computed and show very good results.

Keywords: Chaotic system, magic square, image encryption, Lyapunov exponents.

1 Introduction

Recently, image security becomes an important issue to deal with. Therefore, image encryption is used in many fields to ensure high security and to protect image data. The growing and remarkable development in information systems technologies increases the need to find advanced technologies to protect information and preserve them from tampering, destruction, or penetration. One of these techniques is to show the image data and how to preserve it, creating many techniques for encrypted images.

Color image encryption is a technique to convert received image to another that is hard to understand. This paper proposes a novel three-dimensional chaotic system which is invoked to generate a key to encrypt color images. Image encryption is performed chaotically and randomly. It was proposed to create a chaotic three-dimensional system using new and repeated keys to encrypt chaotic complex images.

The chaotic system was tested by calculating the Lyapunov exponents method where one of them was positive and it was sensitive to the initial values, which means the system is a chaotic system. The strength of encryption has been determined by analyzing the correlation coefficient, entropy, histogram, and system efficiency where the time of encryption and decryption was very small.

In this paper, a novel three-dimensional chaotic system which is based on a magic square has been created for image encryption. Image encryption can work on color images with different sizes and which show high-speed encryption. It is a new technique to encrypt the image at random and is a difficult technique. The first magic square was a Chinese legend which was described literally in English as *the* scroll of the river Lohor Loh-Shu by Fuh-Hi. It is a 3×3 magic square with symbols rather than numbers. Today's Chinese scholars have only managed to trace the Loh-Shu back as far as the fourth century B.C. [4].

***Corresponding author: Rageed Hussein AL-Hashemy,** Computer Science Department, College of Education, University of Almustansirya, Baghdad, Iraq, e-mail: ragheed1968@uomustansiriyah.edu.iq
Sadiq A. Mehdi: Computer Science Department, College of Education, University of Almustansirya, Baghdad, Iraq

A chaotic system is a special dynamical nonlinear system, which has a number of characteristics such as sensitivity to initial conditions and irregular and unpredictable behavior [4]. When a dynamical system evolves with particular values of initial conditions and parameters, the chaotic behavior is obtained. In 1963, Lorenz discovered by accident the first chaotic system when the author built a model for weather modeling [2].

The model is created via three first-order differential autonomous equations. Various 3-dimensional chaotic systems were presented such as LÜ system, Chen system, Rossler system, etc. [6, 9, 10]. Due to Chaos properties, it is implemented nowadays in many various areas like engineering, computer science, mathematics, physics, geology, biology, robotics, etc. [10, 11, 14].

The paper is organized as follows: in Section 2, the related works are presented. Section 3 describes the theoretical background such as the magic square, the proposed chaotic system, Lyapunov exponents and Lyapunov dimensions, phase portraits, waveform analysis, and sensitivity to initial conditions. In Section 4, the proposed algorithm has been presented and analyzed, and its performance was evaluated by different statistical analysis methods and presented in Section 5. Eventually, conclusions are drawn in Section 6.

2 Related Work

Many researchers used chaotic systems and magic square for image encryption. Some related work is explained below.

Kester [8] proposed the work to upgrade a cipher algorithm for m*n size image encryption by shuffling the basic RGB pixel values. Finally, the algorithm made it possible for encryption and decryption of images based on the RGB pixel. During the decryption process, the values of the RGB pixel must be reconstructed.

Amalarethinam and Geetha [1] introduced an image encryption algorithm in view of applied Magic Rectangle (MR) as the plain picture is changed over into pieces of single bytes, and after that the square is substitute as the estimation of MR. Further, the control parameters of MR are chosen haphazardly by the client.

Zhang et al. [16] introduced an algorithm using the magic square transformation for the original image pre-process. This process is a pre-treatment on the basis of magic square algorithm improved ranks. After that an Arnold cat map, which is the most commonly used map in chaos-based image encryption, was used to scramble the second image. By using Henon technique, an array will produce the image's scrambled gray values, which transforms the images position and gray value at the same time to get the final encrypted image.

Wang and Luan [13] proposed a new algorithm composed of two stages: confusion and diffusion; the image in the confusion stage shuffles on unit level by using chaotic maps. Then in the diffusion stage the reversible cellular automata are performed on higher half pixel bits for many rounds, and the result of this procedure is the cipher image.

Sakthidasan and Krishna [12] proposed dynamic chaotic systems, which use one of the three chaotic systems, Lorenz or Chen or LU chaotic systems, based on a 16-byte key and applied on image encryption scheme to shuffle the image pixels' positions and use another one of the same three chaotic maps to make a confusion between the cipher image and the plain image to increase the resistance of the attack significantly. This work has bigger key space advantage in which the number of iterations is less and the ability of high security analysis. Therefore, the proposed system was highly efficient and a robust one.

Guan et al. [5] proposed a new method of image encryption that shifts the positions and modifies the values of the image pixels, then the values are combined together in order to mix up the values of the cipher image and the original one, which makes the relationship between the two images more confusing. In this work, the positions of the image pixels in the spatial domain are shuffled by using an Arnold cat map. The discrete output signal of Chen's chaotic system is pre-processed to suit the gray scale of encryption of the image. The encrypted shuffled image is pre-processed pixel by pixel; the results showed that the key space

is large enough to resist the brute force attack, and the gray values distribution of the encrypted image has a randomly behavior.

3 Theoretical Background

In this section, the different theories this paper has referred to are presented. To reach the highest chaotic system, we use Lyapunov exponents, Lyapunov dimensions and dimension Kaplan Yorke (D_{KY}). An XOR operation with the key is generated by the new chaotic system to get the encrypted image.

3.1 What Is a Magic Square?

A magic square is a matrix of n rows multiplied by n columns. Its values are integers, which are arranged such that the sum of the n numbers in any horizontal, vertical, or main diagonal lines is always the same number. The magic square with related classes of integer matrices has been studied in depth in the literature [7].

A basic magic square of order n can be defined as an arrangement of numbers from 1 to n^2 in an $n \times n$ matrix, which means every row, column, and diagonal add up to the same number. The formula ${}^1/_2\, n\,(n^2 + 1)$ is used to calculate the magic sum. In general, magic squares remain magic if the same positive integer is added to each number in the square or each number in the original square is multiplied by the same number; see Figure 1 [15]. From this figure, the sum of numbers in any row, column, or diagonal line is 34.

3.2 The Proposed Novel Chaotic System

The proposed chaotic system is designed by selecting the suitable parameter values a, b, c, d, and e, which are set randomly to find the values of x, y, and z. This allows finding a numerical solution for the differential equations, which helps to achieve the three-dimensional chaotic system. The parameter values are chosen as follows: $a = 5$, $b = 8$, $c = 15$, $d = 4$, and $e = 3$.

The novel three-dimensional chaotic system has been created with the three quadratic non-linearity terms using the differential equations described by Eq. (1):

$$\begin{aligned} \frac{dx}{dt} &= ay - xz \\ \frac{dy}{dt} &= -bxz + e^x \\ \frac{dz}{dt} &= -cCos(x) + dx\, y + ey \end{aligned} \tag{1}$$

where x, y, and z belong to real numbers which are called the states.

The three-dimensional system described in (1) is a chaotic system when the system parameters s are chosen as $a = 5$, $b = 8$, $c = 15$, $d = 4$, and $e = 3$ and the initial conditions are selected as $x(0) = 0.1$, $y(0) = 5$, and $z(0) = 10$.

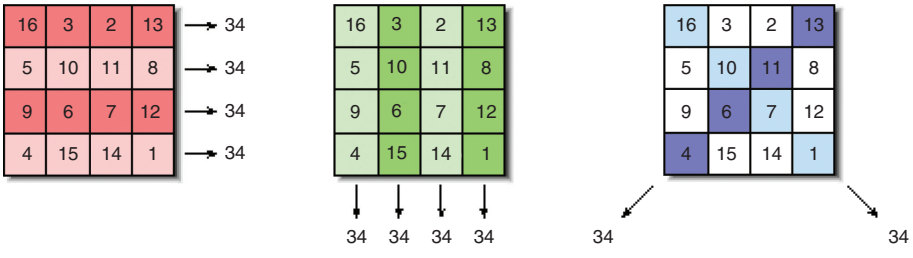

Figure 1: A Basic 4 × 4 Magic Square.

3.3 Lyapunov Exponents, Lyapunov Dimensions, and Bifurcation Diagram

3.3.1 Lyapunov Exponents

A quantitative measure of the sensitivity of the initial conditions is calculated by the Lyapunov exponent. It is the average divergence of infinitesimally close points on a trajectory, and it is represented by the natural logarithm of Lyapunov number; see Figure 2.

The Lyapunov number is given by

$$\text{Lyapunov number} = L(x_1) = \lim_{n\to\infty} (|f'(x_1)| \dots |f'(x_n)|)^{1/n}$$

Here, $\{x_1, x_2, \dots, x_n\}$ represent the trajectory of the map f on the solid line R.

If there are limits on the numbers of Lyapunov, the exponent of Lyapunov is defined as follows:

$$\text{Lyapunov exponent} = h(x_1) = \lim_{n\to\infty} \left(1/n\right)[ln|f'(x_1)| + \dots + ln|f'(x_n)|]$$

Therefore, the Lyapunov exponent can be used with chaotic behavior to measure the sensitive dependence on the initial state. This means that in the one-dimensional chaotic map, using the Lyapunov number, the separation coefficient of the adjacent point along the solid line is measured. The Lyapunov exponent is used to select the initial parameters of the chaotic map entering the chaotic area. There are three different cases of dynamics in the Lyapunov exponent as follows [3]:

- When all Lyapunov exponents are smaller than 0, the trajectory attracts stable points.
- When the Lyapunov exponent is 0, a simple attractor is easier than the set point. This means that the system is stable in a neutral fashion and the attractor is in a stable mode maintaining continuous separation.
- If at least one Lyapunov representative is positive, the dynamics are confused, and vice versa.

The three Lyapunov exponents of the novel chaotic system described in (1) are calculated as LE1 $=$ 1.26476, LE2 $=$ -2.87345, and LE3 $=$ -0.910875. Since LE1 is a positive Lyapunov exponent, and the rest of the Lyapunov exponents are negative, the new system indicates that it has chaotic characteristics.

3.3.2 Lyapunov Dimensions

The fractal dimension is also a typical characteristic of chaos calculated by Kaplan-Yorke dimension (D_{KY}), which is based on Lyapunov exponents. Let j be the first non-negative Lyapunov exponent; the D_{KY} is

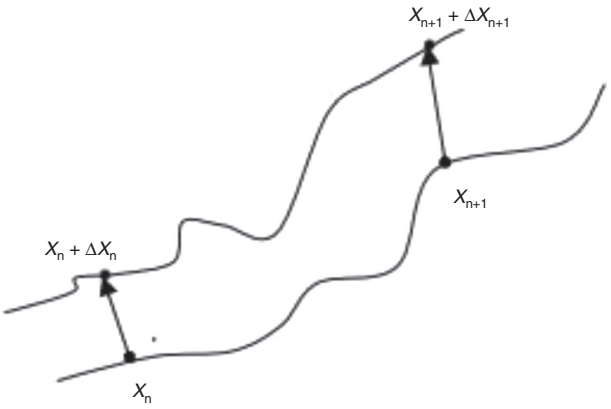

Figure 2: Lyapunov Exponents.

given by

$$D_{KY} = j + \frac{1}{|L_{Ej+1}|}\sum_{i=1}^{j} LE_i \tag{2}$$

The variable j, in this case, is the value which meets the conditions $\sum_{i=1}^{j} LE_i \geq 0$ and $\sum_{i=1}^{j+1} LE_i < 0$.

Since $LE_1 + LE_2 > 0$ and $LE_1 + LE_2 + LE_3 < 0$, the value of j is determined to be 2 and Kaplan-Yorke is computed to be 2.12316, which means that the Lyapunov dimension of system (1) is fractal. Because of the fractal nature, the new system has non-periodic orbits, and its nearby orbits diverge. Therefore, there is a real chaos in this nonlinear system [3].

3.3.3 Bifurcation Diagram

So far, the behavior has been shown only for some different values of ***e***. To see what happens for a wide range of ***e***, we can construct a bifurcation scheme numerically.

The system (1) is solved numerically by Mathematica program simulation, and the values of z for the maximums are kept track of after transients are discarded. We can look at the interesting region of the bifurcation diagram between $\boldsymbol{e} = 4$ and $\boldsymbol{e} = 5.5$. The plot points to limit cycle behavior. As ***e*** is decreased, it appears there is period doubling, which occurs between $\boldsymbol{e} = 5$ and $\boldsymbol{e} = 5.2$. The period doubling can be seen in a plot of z max for a range of ***e***. This is shown in Figure 3. We can see that for a range of ***e*** values, the maxima only take certain values. We can also see clearly that the top branch splits as ***e*** is decreased. Figure 4 zooms in on this

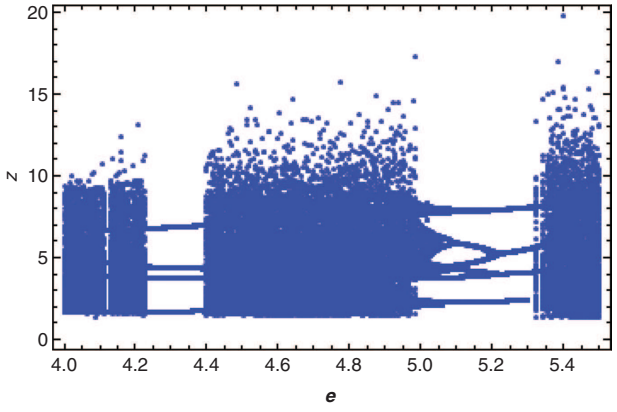

Figure 3: Z Bifurcation Diagram for Increasing ***e***, and Showing Limit Cycle Period Doubling.

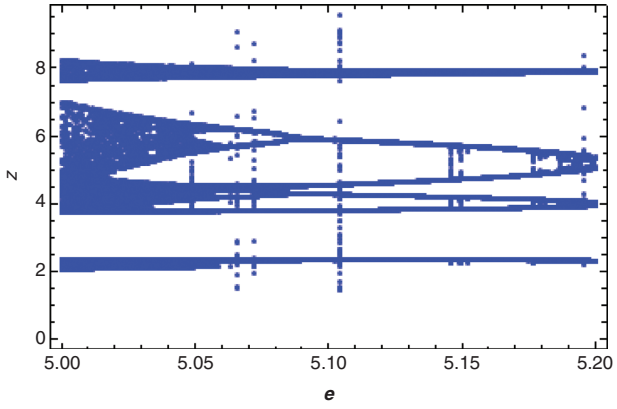

Figure 4: Zoomed in z Trajectory Diagram.
This zooms into the region of Figure 6.

area, giving a better view of the period doublings. This period doubling is a feature of many chaotic systems and has been observed in physical experiments.

3.4 Phase Portraits

Pick the parameters $a = 5$, $b = 8$, $c = 15$, $d = 4$, and $e = 3$; it appears that the new chaotic attractor exhibits a very interesting, complex and chaotic dynamical behavior. This nonlinear system exhibits the complex and abundant chaotic dynamic behaviors. The attractors of a novel system in three dimensions are show in Figure 5.

3.5 Waveform Analysis

The waveforms of system (1) for $(x(t), y(t), z(t))$ in time domain are shown in Figure 6. Obviously, the time domain waveform has a non-cyclic feature, which is one of the characteristics of a chaotic system.

3.6 Sensitivity to Initial Conditions

The long-term unpredictability is one of the chaotic system's characteristics because of sensitive dependence on initial conditions, such that if a small change happened between two initial conditions, they will become widely separated and the way in which the system is evaluated cannot be predicted [16]. Figure 7 demonstrates that the evolution of the chaotic trajectories has high sensitivity towards the initial conditions. Here, the initial values of system (1) are $x(0) = 0.1$, $y(0) = 5$, $z(0) = 10$ for the solid line and $x(0) = -0.1$, $y(0) = 5$, $z(0) = 10.00000001$ for the dashed line.

4 The Proposed Algorithm

In this section, the new algorithm is described. First, the parameters a, b, c, d, and e as well as the initial conditions $x(0)$, $y(0)$, and $z(0)$ are selected to fulfill the chaotic behavior described in the preceding sections.

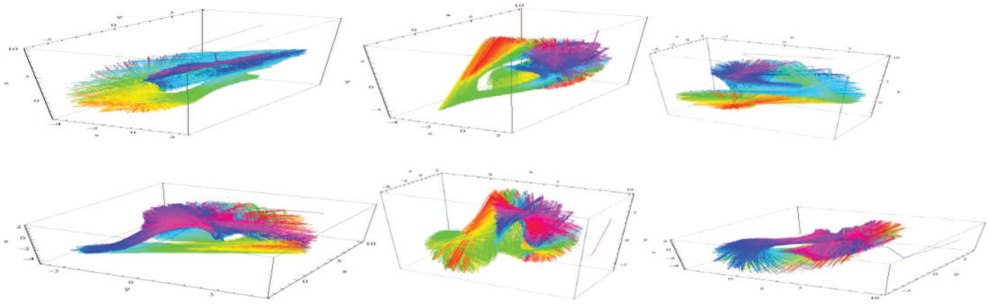

Figure 5: Chaotic Attractors of a Novel System, Three-Dimensional View.

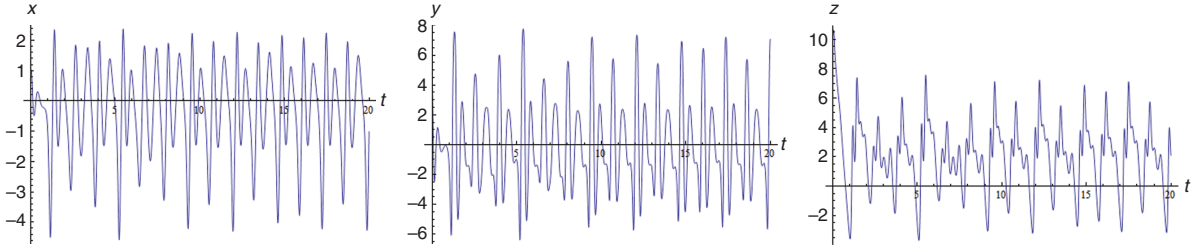

Figure 6: Time versus (x, y, z) of the Novel Chaotic System.

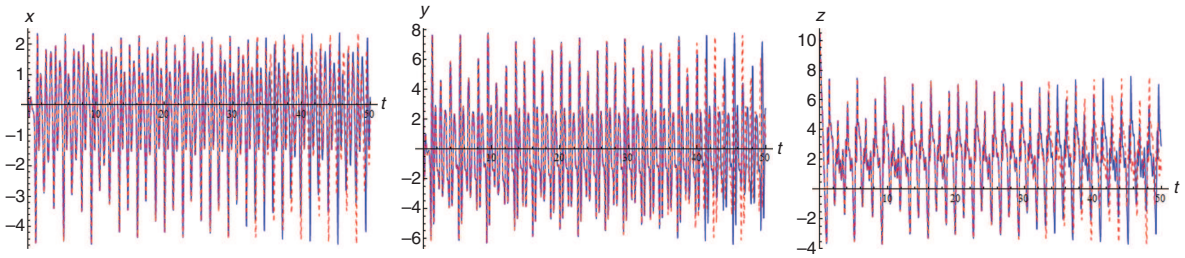

Figure 7: Sensitivity Tests of the Novel System ($x(t)$, $y(t)$, $z(t)$).

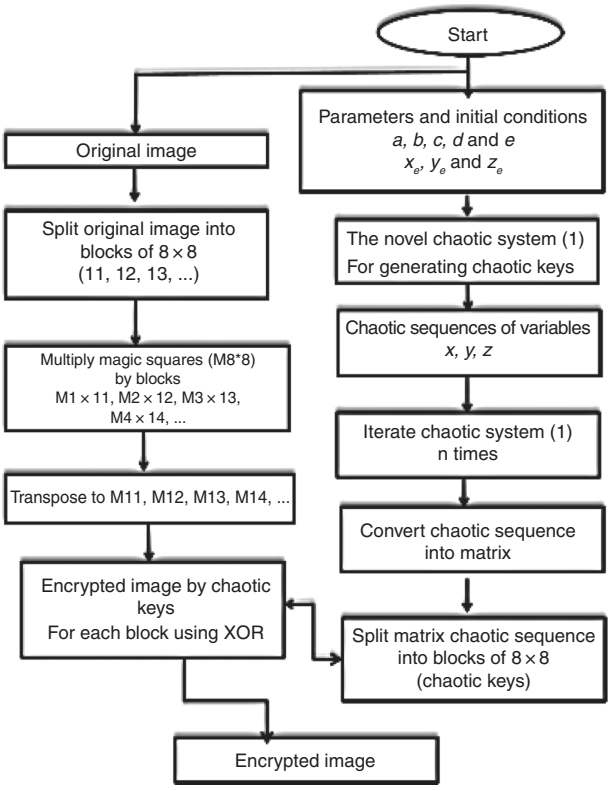

Figure 8: Proposed Algorithm Diagram of the Chaotic Encryption System.

These initial conditions are applied using the proposed chaotic system to generate the chaotic keys. Using this method, the chaotic sequences of the variables X, Y, and Z are produced n times. These n chaotic keys are then arranged into a matrix, and the matrix is divided into non-overlapped blocks represented by {C1, C2, C3, ...}.

The original-image is divided into a set of non-overlapped blocks represented by {I1, I2, I3, ...} and then multiplied by the magic squares of the same size to produce submatrices represented by {M1 × I1, M2 × I2, M3 × I3, ...}. The transpose of these blocks are then calculated and represented by {MI1, MI2, MI3, MI4, ...}. The image can be encrypted using the XOR operation between the blocks {C1, C2, C3, ...} and {MI1, MI2, MI3, MI4, ...}. The decryption process is the same as the encryption but with reverse steps. Figure 8 shows the block diagram of the chaotic encryption algorithm.

5 Experimental Results and Analysis

The proposed algorithm presented in this paper has been applied to a number of images. Figure 9 shows a number of sample images of the set invoked to test this algorithm. All images used in this test are of size

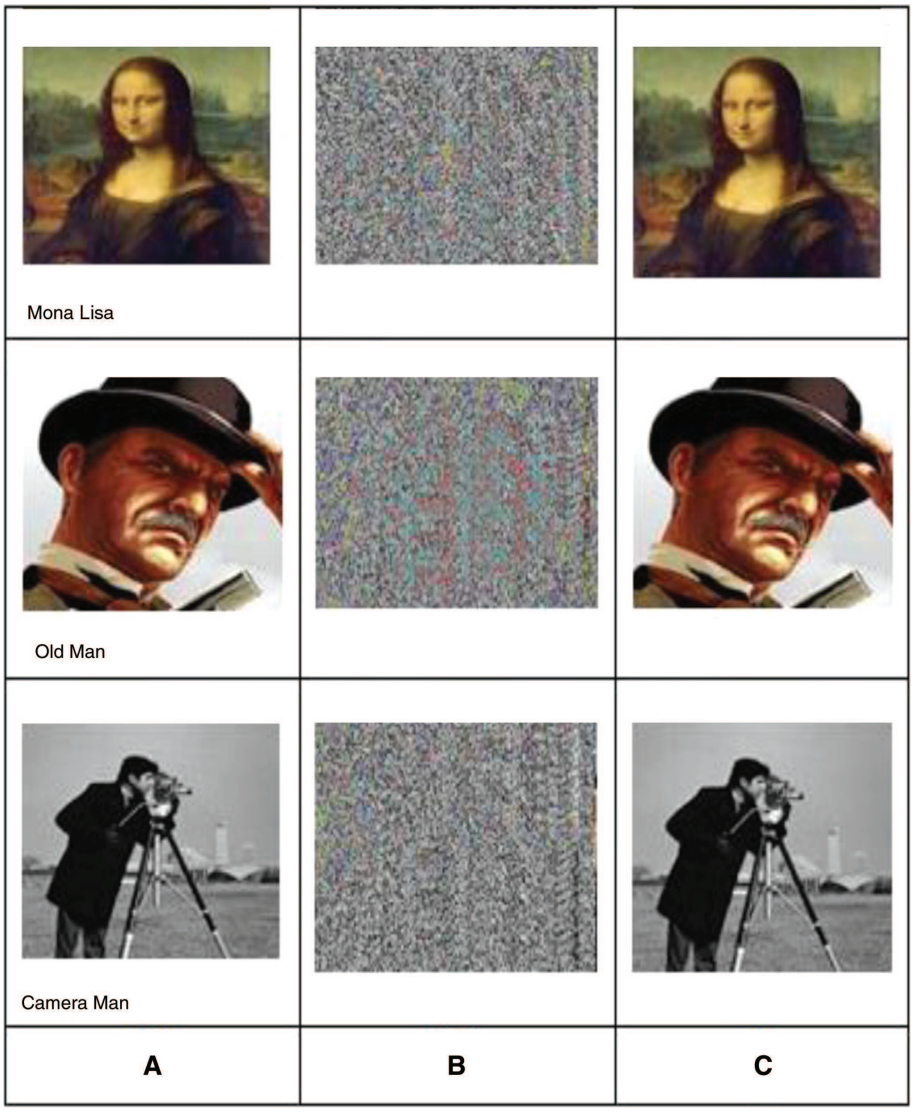

Figure 9: Experimental Result of Encryption and Decryption Image.
(A) Original Images, (B) Encrypted Images, and (C) Decrypted Images.

256 × 256 pixels. However, the proposed algorithm can be applied to any image of completely different size. In the following subsections, the proposed algorithm will be tested for security and statistical analysis, and effectiveness of this algorithm will be demonstrated. To prove the security of the encryption algorithm, the secret key must be very sensitive, and also the length of the key space should be greater than 2^{128} to avoid brute force attack. To demonstrate that the proposed algorithm is very powerful against statistical attack, analyses such as the histogram, the information entropy, and the correlation analysis of the encrypted image are performed.

5.1 Security Analysis

5.1.1 Key Space Analysis

To thwart the threat of brute force attack and make it infeasible, the size of key space must be large enough, where key space means that all possible and different keys can be utilized in the encryption process. Therefore, the minimum key size must be at least 2^{128} (bits) to withstand brute force attack [11]. In the proposed

encryption algorithm, the secret key is the initial conditions and parameters: (x_0, y_0, z_0, a, b, c, d, e). Since the precision for each parameter is 10^{-14}, the key space is calculated as $10^{112} \approx 2^{370}$, which is large enough and has thwarted any brute-force attack.

5.1.2 Sensitivity Analysis

An ideal image encryption procedure should be sensitive to the cipher key. In order to test the sensitivity, Mona Lisa is selected to be the original image. Keep other parameters as they are and employ the cipher key $z_0 = 10$ to decrypt the encrypted image. The results are illustrated in Figure 10. By comparing the two decrypted images, we can find that even with a tiny difference of 10–14, the attacker cannot decrypt the original image correctly. The proposed algorithm has good key sensitivity and ability to resist exhaustive attack.

5.2 Statistical Analysis

5.2.1 Histogram Analysis

In order to prevent the attacker from revealing any information from the original image, any statistical relationship or similarities between the original image and the ciphered image must be avoided. The statistical properties of an image can be deduced from histogram analysis of that image. In order to prevent the attacker from extracting any information from the original image, the statistical characteristics of original image and the ciphered image must be completely different [6]. Figure 11 shows that the histograms of the encrypted image in the red, green, and blue channels are fairly uniform due to the robust proposed encryption scheme, and there is not any statistical similarity between the histograms of the original image and the ciphered image.

5.2.2 Correlation Coefficient Analysis

One of the basic characteristics of any image is the high correlation between adjacent pixels. Correlation is a measure of the level of likeness between two pixels. Any encryption scheme must reduce the correlation among adjacent pixels to prevent the attacker from speculating on the values of the neighbor pixels. The proposed encryption scheme tries to make this correlation close to 0 to avoid any statistical attacks with respect to the original image. The correlation coefficients of vertically, horizontally, and diagonally adjacent pixels are computed and analyzed for the original image and its corresponding encrypted image. Figures 12–14 depict the correlation among the vertically, horizontally, and diagonally allocated pixels for the original and the encrypted images. High correlation between two adjacent pixels for the original image appear, while correlation of the encrypted image is very small and around 0. Table 1 shows the values of correlation for two contiguous pixels in the original image and the encrypted image.

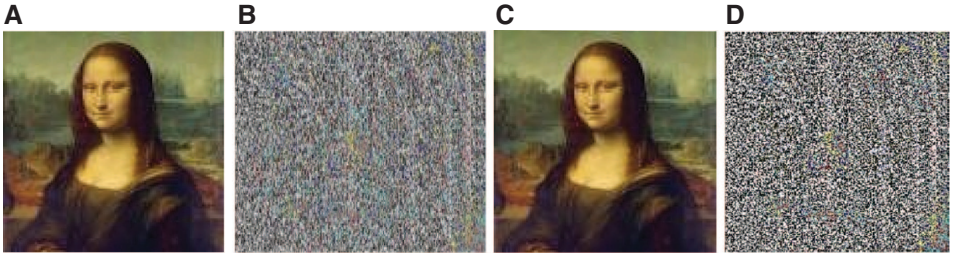

Figure 10: Results of Sensitivity Test.
(A) Original image of "Mona Lisa". (B) The encrypted image of (A). (C) The decrypted image of (A) with the correct key. (D) The decrypted image of (A) with a change in key z_0 ($z_0 = 10.0000001$).

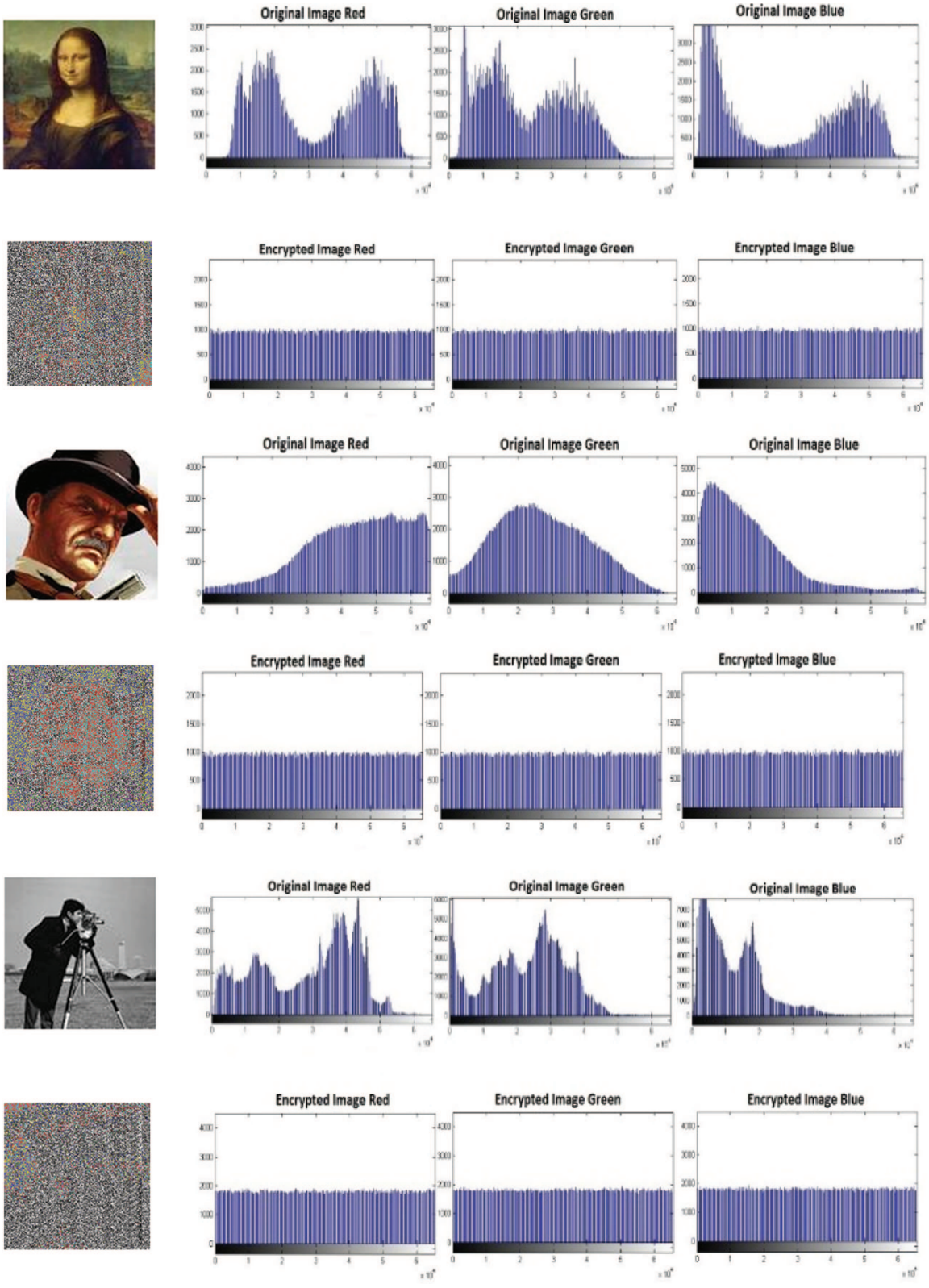

Figure 11: Histogram for Original Images and its Encryption.

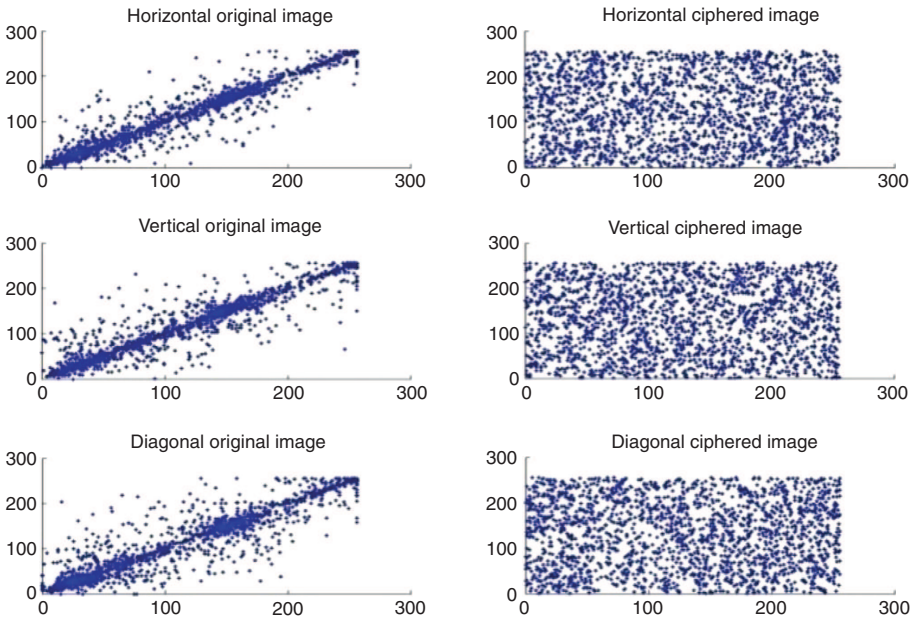

Figure 12: Correlation Horizontally, Vertically and Diagonally for Two Adjacent Pixels in Plain and Encrypted "Mona Lisa" Image.

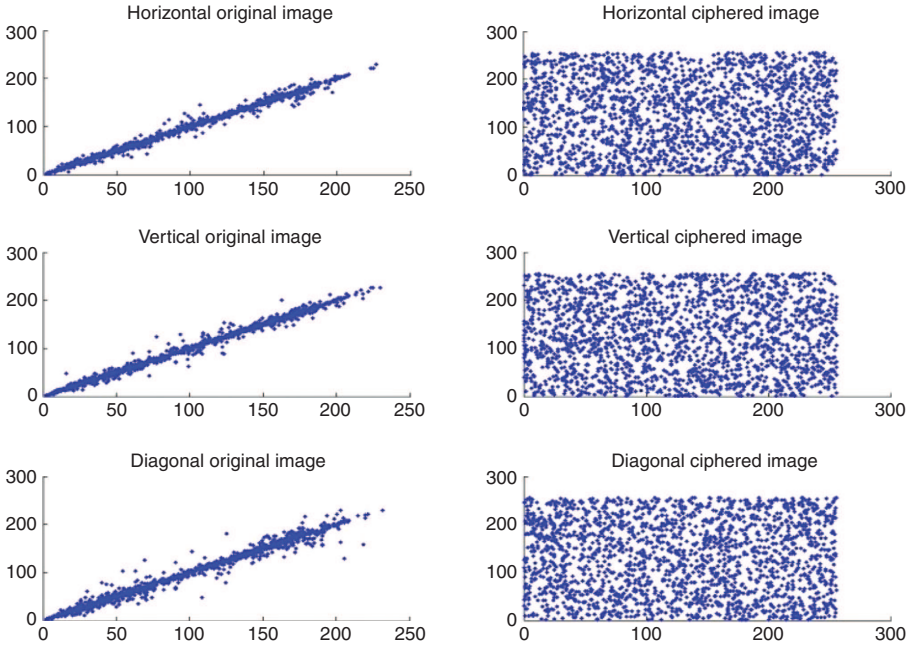

Figure 13: Plot Describes Correlation Horizontally, Vertically and Diagonally for Two Adjacent Pixels in Plain and Encrypted "Old Man" Image.

5.2.3 Information Entropy Analysis

Entropy is the most important characteristic of randomness or unpredictability in information theory. The entropy of perfect randomly source emitting 2^8 symbols is $H(\mathrm{m}) = 8$. From Table 2, the entropy values of cipher test images are between 7.92 and 7.99. This means that the ciphered image has better random characteristic than the original image and the proposed scheme for encryption is highly secure and more resistant against entropy attack. Values depicted in Table 2 show high security against entropy attack with less degree of predictability that threatens the security.

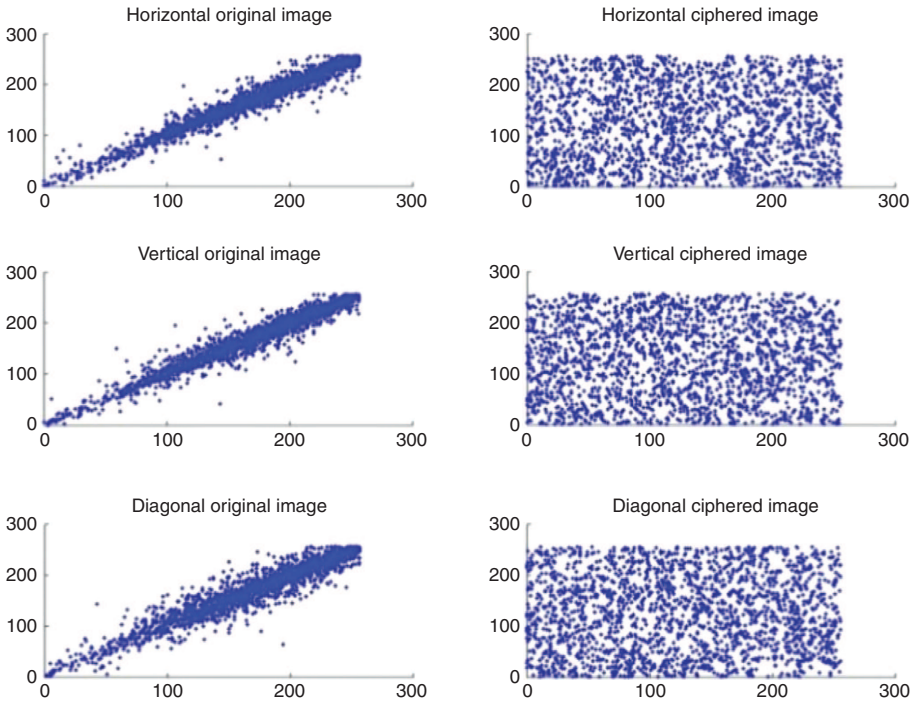

Figure 14: Plot Describes Correlation Horizontally, Vertically and Diagonally for Two Adjacent Pixels in Plain and Encrypted Camera Man Image.

Table 1: Correlation Coefficient Values for Original Images and their Corresponding Ciphered Images.

Image	Vertical	Horizontal	Diagonal
Mona Lisa original	0.9637	0.9686	0.9648
Mona Lisa encrypted	−0.0006	−0.0013	0.00017
Old Man original	0.9965	0.9956	0.9945
Old Man encrypted	0.0013	−0.0004	0.0001
Camera Man original	0.9935	0.9731	0.9819
Camera Man encrypted	−0.0014	0.0001	0.0005

5.3 Differential Attack

A good encryption scheme must have the ability to withstand differential attacks. The test for a differential attack includes encrypted two plain images P1 and P2 with very small difference of 1 bit, and the impact of that difference on the resulting cipher images is evaluated. Two important measures are used, namely, the number of pixels change rate (NPCR) and unified average changing intensity (UACI), where NPCR measures the percentage of various pixels between two ciphered images, C1 and C2, and can be expressed by the following formula:

$$D(i,j) = \begin{cases} 0, & \text{if } C^1(i,j) = C^2(i,j) \\ 1, & \text{if } C^1(i,j) \neq C^2(i,j) \end{cases} \tag{3}$$

$$\text{NPCR: } N\left(C^1, C^2\right) = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \tag{4}$$

UACI is used to measure the average intensity of various pixels between the two ciphered images, and it is expressed by

$$\text{UACI: } U\left(C^1, C^2\right) = \frac{\sum_{i,j} \left|C^1(i,j) - C^2(i,j)\right|}{F \times T} \times 100\% \tag{5}$$

Table 2: Information Entropy for Original and Cipher Images.

Image	Image size	Original/Encrypted	Red plane	Green plane	Blue plane
	256 × 256	Original	7.9286	7.9065	7.9649
		Encrypted	7.9317	7.9924	7.9980
	256 × 256	Original	7.9336	7.9864	7.9609
		Encrypted	7.9113	7.9121	7.9978
	256 × 256	Original	7.8197	7.9470	7.9263
		Encrypted	7.9033	7.9152	7.9980

Table 3 depicts the NPCR and UACI values for the three test images, namely, Mona Lisa, Old Man, and Camera Man.

From Table 3 and in comparison with theoretical values in [6], the resulting values for NPCR are between 99.9981 and 99.9993 and pass the test, while the resulting values for UACI are between 33.3789 and 33.7996, and some of these values pass the test where others are close to the theoretical values. Therefore, it can be concluded that the proposed encryption algorithm has high ability to frustrate the differential attacks.

5.4 Speed Performance

The speed of the proposed cryptosystem is a very important factor to measure the efficiency. The proposed scheme was tested using a personal computer Intel(R) Core(TM) i7 @ 2.67GHz CPU with 4 GB RAM, and Table 4 presents encryption and decryption speeds. According to this table, the time of encryption and decryption of the proposed algorithm is very short.

Table 3: The NPCR and UACI Result Values.

Image	NPCR	UACI
Mona Lisa	99.9981	33.3789
Old Man	99.9993	33.7996
Camera Man	99.9982	33.7802

Table 4: Encryption and Decryption Speed.

Image	Encryption time (s)	Decryption time (s)
Mona Lisa	0.4544	0.3544
Old Man	0.5822	0.4822
Camera Man	0.5468	0.512

6 Conclusion

This paper presented an image encryption model based on the chaotic technique. The chaotic technique is used to change the position and modify the values of the image pixels. Different tests are used to identify to what extent that the encryption algorithm can be applied. The results show that the technique highly rebuts the statistical attacks, such as histogram analysis in which the encrypted image has a completely uniform histogram. Test results have also shown that the correlation values for the encrypted image are tiny (close to zero); nonetheless, the encrypted image entropy values are selected to be close enough to the theoretical values. In addition, the encryption technique shows high resistance against different attacks. The space domain is very large (about 2^{370}), which, in some ways, can be frustrating for the brute-force attack. Finally, the encryption technique has fair sensitivity to the key changing, and the time for both image encryption and decryption is very short.

Bibliography

[1] D. G. Amalarethinam and J. S. Geetha, Image encryption and decryption in public key cryptography based on MR, in: *2015 International Conference on Computing and Communications Technologies (ICCCT)*, pp. 133–138, IEEE, Chennai, India, February 2015.

[2] H. Broer and F. Takens, *Dynamical systems and chaos*, vol. 172, Springer Science and Business Media, New York, Dordrecht, Heidelbeg, London, 2010.

[3] E. Brown, Magic squares, finite planes, and points of inflection on elliptic curves, *Coll. Math. J.* **32** (2001), 260–267.

[4] A. W. Grogono, A mini-history of magic squares [online], 2004. http://www.grogono.com/magic/history.php.

[5] Z. H. Guan, F. Huang and W. Guan, Chaos-based image encryption algorithm, *Phys. Lett. A* **346** (2005), 153–157.

[6] A. A. Hattab and S. A. Mehdi, A novel steganography method based on 4 dominations standard chaotic map in spatial domain, *J. Theor. Appl. Inform. Technol*. **96** (2018), 16.

[7] B. L. Kaul and R. Singh, Generalization of magic square (numerical logic) 3×3 and its multiples $(3 \times 3) \times (3 \times 3)$, *Int. J. Intell. Syst. Appl.* **1** (2013), 90–97.

[8] Q. A. Kester, Image encryption based on the RGB pixel transposition and shuffling, *Int. J. Comput. Network Inform. Sec.* **5** (2013), 43–50.

[9] J. Lu, G. Chen, X. Yu and H. Leung, Design and analysis of multiscroll chaotic attractors from saturated function series, *IEEE Trans. Circuits Syst. I: Regular Papers* **51** (2004), 2476–2490.

[10] S. A. Mehdi and R. S. Kareem, Using fourth-order Runge-Kutta method to solve Lü chaotic system, *Am. J. Eng. Res*. **6** (2017), 72–77.

[11] S. A. Mehdi and H. A. Qasim, Analysis of a new hyper chaotic system with six cross-product nonlinearities terms, *Am. J. Eng. Res*. **6** (2017), 248–252.

[12] K. Sakthidasan and B. V. S. Krishna, A new chaotic algorithm for image encryption and decryption of digital color images, *Int. J. Inform. Educ. Technol*. **1** (2011), 137–141.

[13] X. Wang and D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, *Commun. Nonlinear Sci. Numer. Simul.* **18** (2013), 3075–3085.

[14] X. Wang, J. Li and J. Fang, Si'lnikov chaos of a 3-D quadratic autonomous system with a four-wing chaotic attractor, in: *Control Conference (CCC), 2011 30th Chinese*, pp. 561–565, IEEE, July 2011.

[15] F. You, H. Dehlinger and J. M. Wang, *Generative art: aesthetic events from experiments with lines and squares*, Lingnan Art Publishing House, Guangzhou, China, 2010.

[16] Y. Zhang, P. Xu and L. Xiang, Research of image encryption algorithm based on chaotic magic square, in: *Advances in Electronic Commerce, Web Application and Communication*, pp. 103–109, Springer, Berlin, Heidelberg, 2012.