

A novel chaos based steganography application with a chaotic system without equilibrium points [☆]

Akif Akgul^a, Irene M. Moroz^b, Ali Durdu^c

*Department of Electrical and Electronics Engineering
Faculty of Technology, Sakarya University of Applied Sciences
54050, Sakarya, TURKEY*

*Mathematical Institute, University of Oxford
Andrew Wiles Building, ROQ, Oxford OX2 6GG, UK*

*Faculty of Political Sciences
Social Sciences University of Ankara, Ankara, TURKEY*

^a*aakgul@sakarya.edu.tr*

^b*moroz@maths.ox.ac.uk*

^c*ali.durdu@asbu.edu.tr*

Abstract

In this article, we investigate how special is the choice of parameter values in the three dimensional nonlinear system, proposed by Akgul and Pehlivan (2016), in producing a system, which exhibits chaos but has no real equilibrium states. Also, a steganography application with a three dimensional chaotic system without equilibrium point, developed by Akgul and Pehlivan, is realized. Numerous encryption studies have recently been made as chaos based. Encryption processes that are used with chaos bring about some security deficiencies in some cases. Steganography, unlike encryption studies, helps communicating the secret data by hiding it in an innocent-looking cover in order to avoid being detected by third parties at first glance. In this work, a novel chaos based steganography method that hides an image with a different color into color images is proposed. Via the proposed method, data is hidden in bit space with the help of the chaotic random number generator (RNG). The generated random numbers are found with a chaotic system without equilibrium point which is new in the literature. Shilnikov method cannot be applied to find whether the system is chaotic or not because they cannot have homoclinic or heteroclinic orbits. Thus, it can be useful in several engineering applications, especially in chaos based cryptology and coding information. In the study, bits are hidden in pixels indicated by numbers generated by RNG. As the order of the hiding process is made randomly on chaotic level, it has made data hiding algorithm stronger. The proposed method hides the data in cover image in such a way that it cannot be easily detected. Furthermore, proposed method has been evaluated with steganalysis methods and image distortion measurement method PSNR. The chaos based steganography method realized here has produced more best results in image distortion measurement method PSNR than other studies in the literature.

Keywords:

June 21, 2019

1. Introduction

The study of chaos is the most complicated decisive behavior of dynamical systems known. It is a field of science that is helpful in explaining nonlinear activities. In other words, chaos, in short terms, is the order of disorder. Every day there are more and more studies about chaos and chaotic systems. Among the most solid examples of these are chaos based applications and new chaotic systems [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. The general classification in the literature includes chaotic systems such as 1 saddle and 2 unstable saddle-foci, like the Liu system [14], having 2 unstable saddle-foci, like DLS [15], chaotic attractors with one saddle and two stable node-foci, with two stable node-foci, like introduced by Yang and Chen [16], Pehlivan and Uyaroglu [17] and Yang et al. [18], all of which have different features. In addition to, so far many different kinds of attractors have been proposed such as multistability, antimonotonicity attractors etc [19, 20, 21, 22, 23, 24].

Recently, chaotic systems without equilibrium points have become more popular [1, 25, 26, 27]. Chaotic system without equilibrium points is named as chaotic system with hidden attractor [28, 29]. As they don't have homoclinic or heteroclinic orbits, some analysis methods like the Shilnikov method [30] cannot be run on chaotic systems without equilibrium points. That is why, they have been preferred more and more in some studies where security like encryption and data hiding are the biggest concerns.

Studies on steganography come into prominence in encryption as data to be encrypted, or hidden in other words, can directly be seen by third parties. Steganography aims to hide secret data in an innocent-looking environment in an undetectable manner. Its main advantage over encryption is that here the presence of the secret information is not openly exhibited. This is the reason why it cannot be understood that the observable object hides secret information. A novel steganography method that hides data into images by means of chaotic random number generator (RNG) is proposed. There are many studies already available on the field of steganography. In the study by Mielikainen, data was hidden into a still image via matching method [31]. The proposed method hides data with the help of a function. In this method, 2-bit data is hidden into two consecutive pixels. Chan improved Mielikainen's study and proposed a new method [32]. The method proposed by Chan makes use of XOR gate as function. For cover image, Tian proposed a data hiding method which has low distortion, high capacity and which is also reversible [33]. Alattar advanced the method proposed by Tian; he doubled the difference between four pixels and was able to hide the 3-bit data into this area [34].

The literature of the field includes a very small number of studies regarding the use of steganography together with chaos. In their study, Anees et al. made use of chaotic maps and managed to

hide data into images. Based on this, they hid data into pixels according to the location they gathered from chaotic maps [35]. In his study, Dogan performed data hiding via genetic algorithm with the help of chaotic maps. Gauss found out that logistic and tent maps are faster than random hiding method [36]. In their studies, Ghasemi and Broumandnia proposed a chaos matching based method that hides text data for images [37]. Kumar et al. encrypted secret data via chaos and managed to hide data into DCT coefficients of the image [38]. Charan et al. hid data with two leveled encryption method [39]. Secret data was encrypted with ceaser encryption technique and with chaos on the first level and second level, respectively. Then, data was hidden with LSB method.

In the first part of this article, a new three-dimensional chaotic system without equilibrium points is discussed. Phase portraits of the chaotic system without equilibrium points and also time series results are given and then some basic analyses are made. In the second part, RNG design is performed with the used chaotic system without equilibrium points and NIST-800-22 statistical tests, which have the internationally highest standards, are made. In the fourth part, the steganography method in this study is explained. The experimental results are covered in the next part. The last part includes the results and evaluations.

2. The used chaotic system and its dynamical analysis

As a steganography application, in this study, a new chaotic system without equilibrium points is employed, unlike the ones in the literature. The proposed 3D continuous time chaotic system [1] introduced in this paper is described as the following differential equations:

$$\begin{cases} \dot{x} = ay - x + zy \\ \dot{y} = -bxz - cx + yz + d \\ \dot{z} = e - fxy - x^2 \end{cases} \quad (1)$$

In the chaotic system, initial values are $x(0)=0$, $y(0)=0$, $z(0)=0$. The system has six constant parameters (a , b , c , d , e and f). Substituting $a=2.8$, $b=0.2$, $c=1.4$, $d=1$, $e=10$ and $f=2$. The system can be described by the following Eq. (2):

$$\begin{cases} \dot{x} = 2.8y - x + zy \\ \dot{y} = -0.2xz - 1.4x + yz + 1 \\ \dot{z} = 10 - 2xy - x^2 \end{cases} \quad (2)$$

Phase portrait, time series and frequency spectrum analyses of the system introduced above are given below. Among dynamic analyses, Figure 1 first shows phase portrait outputs belonging to x - y , x - z and y - z of the chaotic system. Results have been gathered via Matlab odesolve program. Figure 1 clearly exhibits the complex structure of the chaotic system introduced.

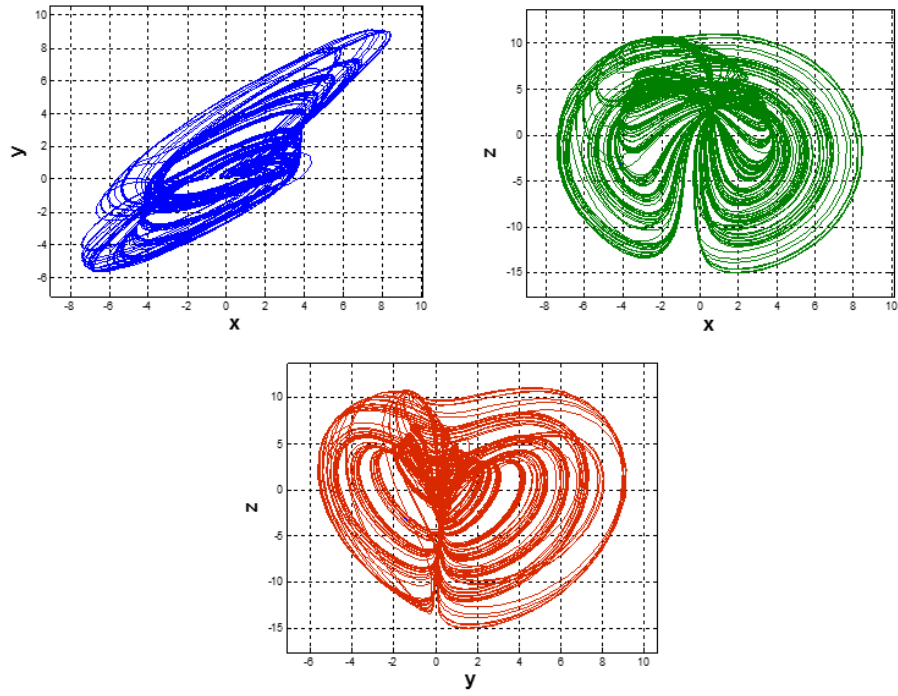


Figure 1: Phase portraits of the introduced chaotic system for $x - y$ phase plane, $x - z$ phase plane, and $y - z$ phase plane

Figure 2 shows time series graphs for the system without equilibrium points. As can be gathered from time series analysis, the system exhibits a chaotic behavior.

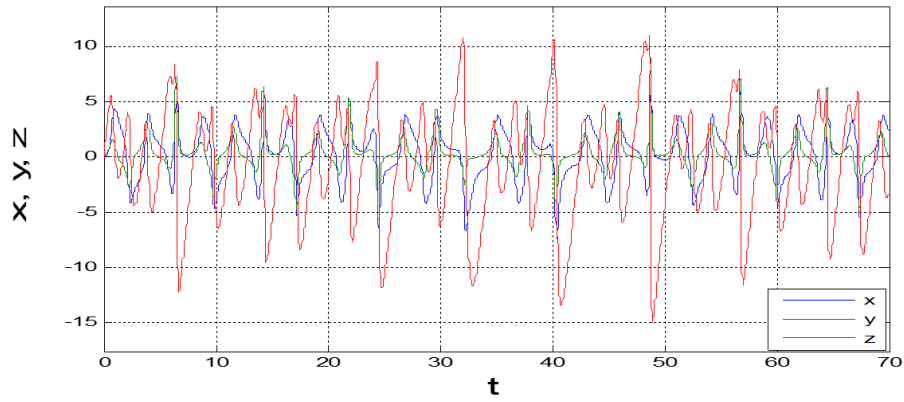


Figure 2: Time series diagram for 3D chaotic attractor in x , y and z

Figure 3 shows the frequency spectrum of chaotic system without equilibrium points and also complex structure of chaotic system. The frequency spectrum is between around 0 kHz and 5 kHz. The wide range of the distribution of frequency spectrum can be observed from the Figure 3. This range is a significant advantage for nonlinear systems. Simple dynamic analyses performed here have proved that the system without equilibrium points is a chaotic system. In addition, it has been shown, with the high frequency conversion of state variables, complexity and sensitivity features, that it is very suitable to be used in studies like encryption and data hiding. That the system doesn't have an equilibrium point has already been proved by Akgul and Pehlivan in their previous studies [1], so it is not included in this study.

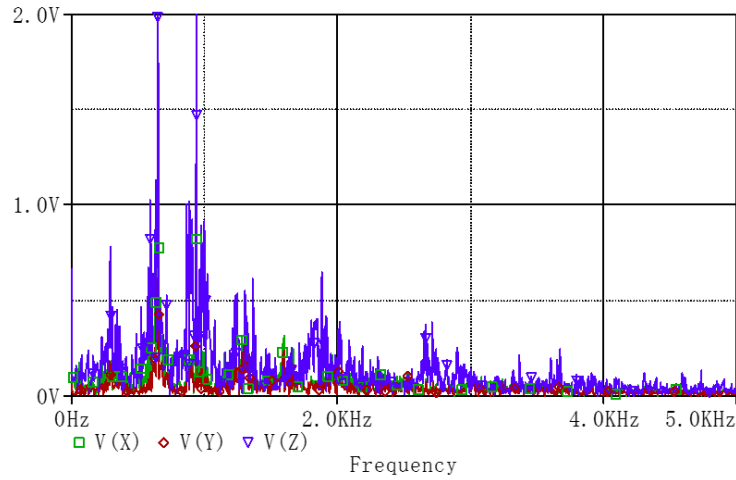


Figure 3: The frequency spectrum of the chaotic signals without equilibrium points.

In introducing the new three dimensional chaotic system, Akgul and Pehlivan (2016) chose parameter values of $(a, b, c, d, e, f,) = (2.8, 0.2, 1.4, 1, 10, 2)$. For these parameter values, only complex equilibrium states exist. It is of interest, therefore, to determine just how special is this choice of parameters, in order to assess just how special is both the hidden chaotic attractor and the steganographic application, proposed in the current paper. This is the objective of this section. We accomplish this by discussing the character of the equilibria of system (1) as we vary each of the six parameters in turn, identifying where there exist real equilibrium points, where there exist both real and complex equilibria, and where there exist only complex equilibria. These ranges are then compared with corresponding bifurcation transition diagrams for the maximum value of y over each cycle. We took the final values for (x, y, z) to be the initial data for the next increment of the parameter.

We can derive a quartic equation for the equilibrium states of (1), by eliminating y and z . Writing the equilibrium point $x_e = X$, we obtain:

$$A_4 X^4 + A_3 X^3 + A_2 X^2 + A_1 X + A_0 = 0, \quad (3)$$

where

$$A_4 = a + f(1 + ab + bf - c), \quad A_3 = fd, \quad (4a)$$

$$A_2 = e(cf - 2a - abf - f), \quad A_1 = -def, \quad A_0 = ae^2. \quad (4b)$$

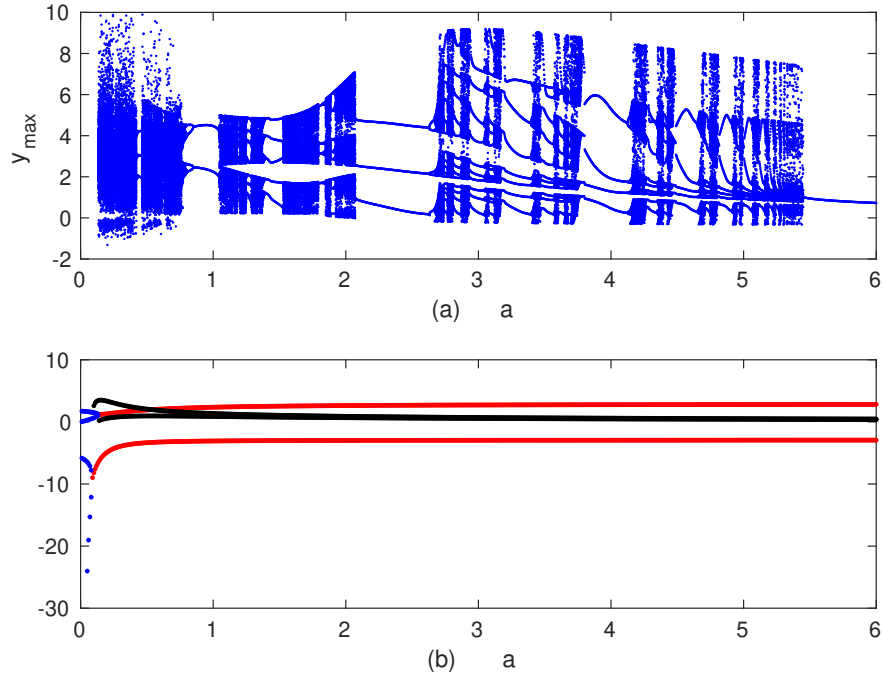


Figure 4: The upper figure shows the bifurcation transition diagram as parameter a varies, in terms of the maximum value of y over each cycle. The lower figure shows the real equilibrium points (blue), the real parts of the complex equilibria (red) and the imaginary parts for X .

As a increases from $a = 0$, there are four real equilibria, one of which comes in from $-\infty$. These four equilibria exist in $0 \leq a \leq 0.09$, when two equilibria coalesce to form a pair of complex conjugate equilibria. The remaining two equilibria merge when $a = 0.14$. Thereafter for $a \geq 0.14$, there are only complex equilibrium states, over the range of existence of both chaotic and periodic solutions, which includes $a = 2.8$.

Figure 5 of Akgul and Pehlivan (2016) shows the bifurcation transition diagram as b increases. The next figure shows the corresponding plot of X vs b .

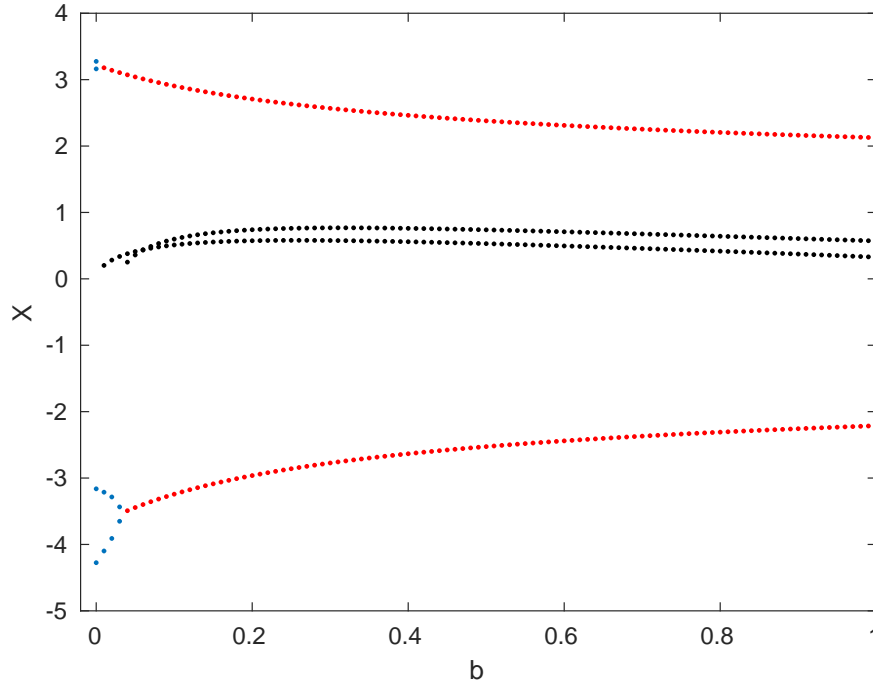


Figure 5: The real equilibrium points (blue), the real parts of the complex equilibria (red) and the imaginary parts for X .

When $b = 0$, there are four real equilibria, all unstable (so we have a stable periodic state). For $0.01 \leq b \leq 0.03$, two of the equilibria have coalesced, to create two complex equilibria. For $b \geq 0.04$, we only find four complex equilibrium states, including for $b = 0.2$.

The corresponding plots as the parameter c varies are shown in the next figure. As c increases from $c = 0$, there is a pair of real equilibrium states and a pair of complex conjugate equilibria. One of the real equilibrium states is stable for $0 \leq c < 0.46$. When $c = 0.46$, the two real equilibria merge to give four complex equilibrium states. This coincides with the appearance of multiple branches in the (c, y_{max}) plot. When $c = 2.84$ two of the complex equilibria become real. This pair continues to exist as c increases. When $c = 3.26$, the other two complex equilibrium states become real, and we now have four real equilibria until $c = 3.39$, when two of the real equilibria become complex. The coefficient A_4 in the quartic equation for X vanishes when $c = 3.36$, indicating that one of the roots becomes infinite. $c = 1.4$ falls within the chaotic region.

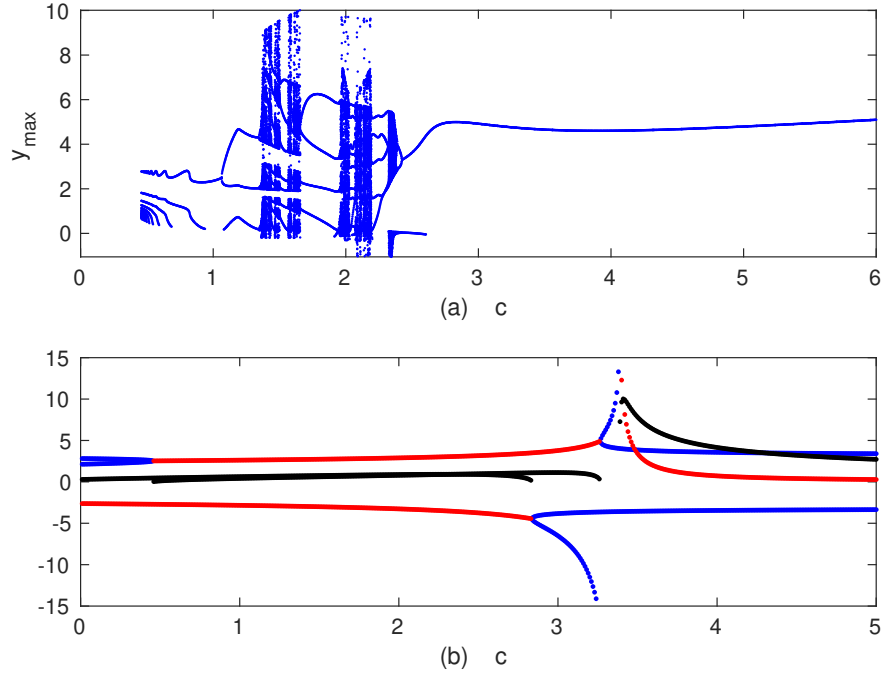


Figure 6: The upper figure shows the bifurcation transition diagram as parameter c varies, in terms of the maximum value of y over each cycle. The lower figure shows the real equilibrium points (blue), the real parts of the complex equilibria (red) and the imaginary parts for X .

When we increased d from $d = 0$, we found no real equilibria until $d = 0.37$, where a pair of complex equilibria become real. Referring to the bifurcation transition plot for d , this value coincides with the loss of chaotic or periodic behaviour, and the establishment of stable steady state solutions.

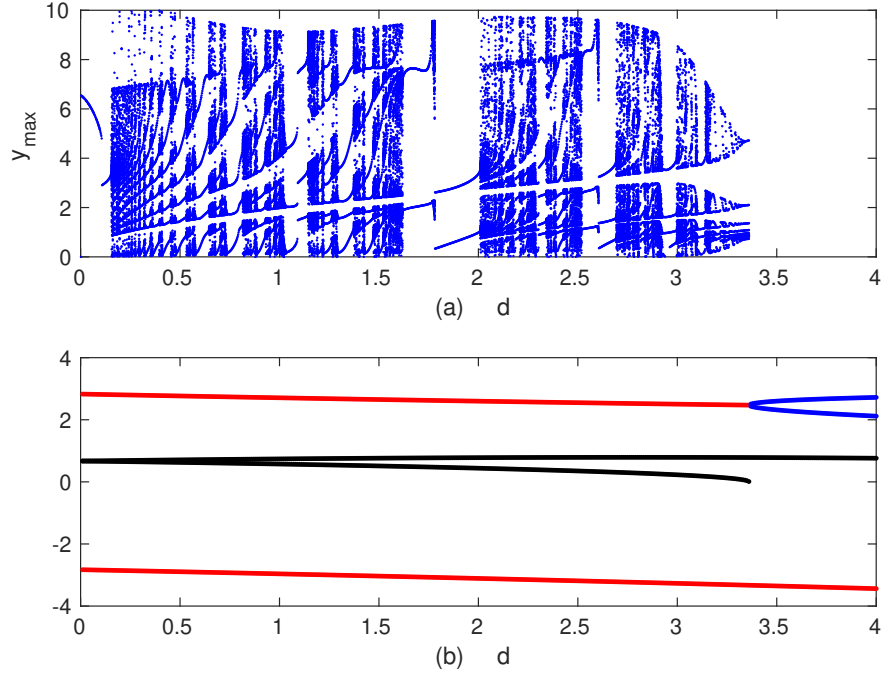


Figure 7: The upper figure shows the bifurcation transition diagram as parameter d varies, in terms of the maximum value of y over each cycle. The lower figure shows the real equilibrium points (blue), the real parts of the complex equilibria (red) and the imaginary parts for X .

As e is increased, for $0 \leq e < 0.2$ there are four real equilibria, one of which is a stable steady state. For $0.21 < e < 0.88$, there are two complex equilibria and two real equilibria. For $e > 0.89$, there are only complex equilibrium states. $e = 10$ falls within the chaotic regime, where there is a range of no real equilibrium points.

Finally, we varied the parameter f . Only for the value of $f = 0$ does there exist four real equilibrium states. Indeed when $f = 0$, the quartic for X simplifies to give the roots $X = \pm\sqrt{e}$ (twice). For $f > 0$, there are always four complex roots, at least for $f \leq 10$.

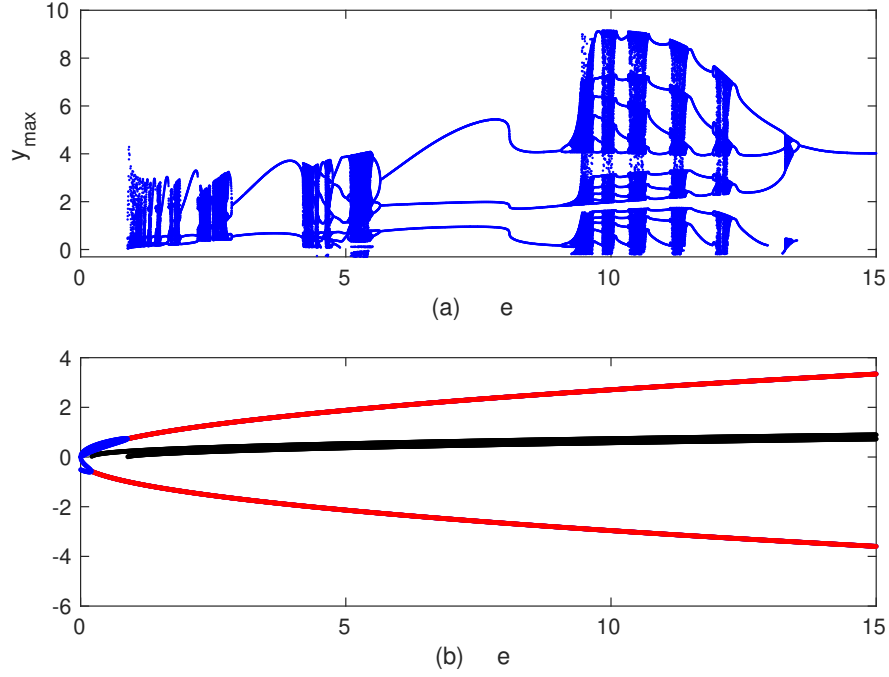


Figure 8: The upper figure shows the bifurcation transition diagram as parameter e varies, in terms of the maximum value of y over each cycle. The lower figure shows the real equilibrium points (blue), the real parts of the complex equilibria (red) and the imaginary parts for X .

3. RNG design with a chaotic system without equilibrium points and its NIST test results

Random Number Generators (RNG) are used in many scientific and engineering fields like the science of encryption where random number series are required. In recent years, numerous studies on RNG have been carried out [3, 6, 4, 40, 41, 42, 43, 44]. In applications like encryption and data hiding in which security is of utmost importance, keys must be random. Number of chaos based studies has recently been on the rise as they properly offer features of complexity and sensitivity. By means of RNG created with chaotic systems, studies such as chaos based encryption and data hiding can be carried out in a more secure, complex and sensitive manner in many fields.

In this paper, for RNG design, a chaotic system without equilibrium points has been used. Since certain analysis methods like Shilnikov method cannot be applied to a system without equilibrium points, such systems are harder to detect by analysis. As it is almost impossible to uncover hidden data without chaotic system, it can be argued that the chaotic system without equilibrium points, used in this study, is more reliable to utilize than other chaotic systems. The design and tests of chaos based RNG which will form the basis of data hiding algorithm for the article have been

made. For RNG design, steps given on the block diagram on Figure 9 have been followed.

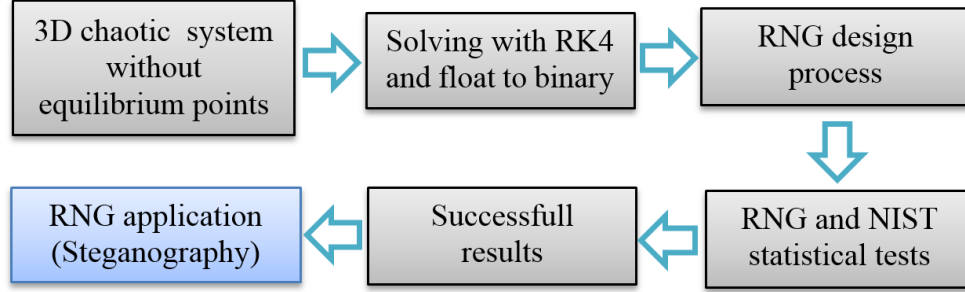


Figure 9: Random number generator design steps with the proposed 3D chaotic system without equilibrium points

For RNG design, since the chaotic system without equilibrium points used for RNG design is a continuous time system, discretization has been made with RK4 algorithm on the first stage. So firstly, the parameter and initial values of chaotic system are needed. These values are very important to obtain the same random numbers. Any change in these values will result in generation of different numbers. After entering initial and parameter values, time step is determined in order to discretize time series of the chaotic system without equilibrium points.

After discretization process, float numbers are obtained. Float numbers, created for the steganography method applied in this study, have been converted to binary number system. The conversion has produced a 32-bit binary number system for each float number. Suitable bits from the 32 bit binary numbers have been picked and number series consisting of '0's and '1's have been created. In this study, last 16 bits, the from 32^{nd} to 17^{nd} ones that are more complex have been picked for RNG design.

In order to measure randomness performance of the binary numbers created via the design, NIST-800-22 statistical tests, which have the internationally highest standards, have been used. NIST-800-22 tests are made up of 16 different tests and a number series with minimum 1 Mbit '0' and '1's is needed for this test. Provided that the bit series fails in one or more of the NIST-800-22 tests, it needs to be re-generated and tests must be made. A bit series that passes all of these tests is considered successful in NIST-800-22 test.

In NIST-800-22 test, results found are interpreted according to the defined P-value. If P-value is defined as 0.001, P-value must be bigger than 0.001 for the test to be considered successful. In this study, the bit series created with chaotic system without equilibrium points have passed all NIST-800-22 statistical tests. Since the chaotic system is 3 dimensional, 3 different bit series (x, y, z) can be found through the RNG design processes here. Tests, in this study, have been made with only random numbers gathered from 'x' output and results are given on Table 1.

As can be seen from the results on Table 1, all P values are bigger than 0.001 and that is why all test results are successful. Since random numbers employed in encryption or very hiding applications have a direct influence on security, they are of vital significance for such applications.

Once generated random numbers pass NIST-800-22 randomness tests, they can safely be used in applications like encryption and data hiding.

Table 1: RNG NIST-800-22 tests with 3D chaotic system without equilibrium points

Statistical Tests	P-value (x)	Result
Frequency (Monobit) Test	0.6326	Successful
Block-Frequency Test	0.4965	Successful
Cumulative-Sums Test	0.6356	Successful
Runs Tes	0.0684	Successful
Longest-Run Test	0.8196	Successful
Binary Matrix Rank Test	0.1178	Successful
Discrete Fourier Transform Test	0.7342	Successful
Non-Overlapping Templates Test	0.0053	Successful
Overlapping Templates Test	0.2708	Successful
Maurer's Universal Statistical Test	0.2039	Successful
Approximate Entropy Test	0.6650	Successful
Random-Excursions Test	0.4787	Successful
Random-Excursions Variant Test	0.6745	Successful
Serial Test-1	0.5894	Successful
Serial Test-2	0.6463	Successful
Linear-Complexity Test	0.3089	Successful

In this paper, the generated random numbers are obtained with a chaotic system without equilibrium point as different from RNGs in literature. Shilnikov method cannot be applied to find whether the system is chaotic or not. Also, the random bit series obtained from chaos based random number generator (RNG) design are successfully passed all the NIST-800-22 tests which is the most commonly employed tests to evaluate randomness of number series. In some studies, not all the results of the tests are successful [45, 46]. Furthermore, in the design process of RNG, there is no logical operator in the bit series which successfully passed all the NIST tests.

In some studies in the literature, to obtain bit series which pass all the NIST tests logic operators such as XOR, AND or OR are employed [47, 48, 49]. However, these logical operators cause a loss of time. For example, use of one logical operation in RNG design doubles random number generation time. Moreover, in the design process the last 16 bits of the random numbers in 32 bit binary format are used for x output. Hence the random number generation speed increases. For example, to generate a 1,000,000 bit series a 62,500 iteration of the chaotic system suffices since there is no logical operator in random number generation process. In some studies, only the least

1-2 bits of the random numbers in 32 bit binary are used [47, 50, 51, 52]. Thus, it can be useful in several engineering applications, especially in chaos based cryptology and coding information.

4. The chaos based steganography method proposed with chaotic system without equilibrium points

In this article, data hiding is performed with the help of chaotic system and by hiding data into cover environment in a random manner with least significant bit (LSB) technique. Via this technique, data can be hidden into image, audio, video and text files, independently from the environment. Image hiding into 24 bit color/black and white image has been carried out with the proposed method. The capacity of the proposed method is the same with conventional LSB methods. In this method, random numbers gathered from chaotic system are utilized for data hiding. Data is hidden into byte locations of the numbers, generated by random number generator, in the cover image. The hidden data can be restored without any loss. In the method employed here, data is hidden with LSB technique and thus a 50 percent of change occurs in the last bits of cover image. During the restoration of data, the same chaotic system is needed on the clients side. That is why, it is necessary to know all parameter and initial values belonging to the chaotic system.

According to the proposed method, numbers as many as the bits of the data to be hidden are generated and hiding is made in the location indicated by the numbers generated by chaotic system. Sizes of the file to be hidden and the cover file are calculated and it is checked whether there is enough space for the data to be hidden. In LSB method, data can be hidden in 1/8 of cover file. If the size of the message to be hidden exceeds this limit, hiding cannot occur.

Figure 10 shows the operating principle of the proposed data hiding method. Based on Figure 10, random numbers were generated via chaotic system according to the size (N) of the message to be hidden, and then N-sized RNG Array was created. According to this, the process starts with the first number of RNG series. The pixel value shown by number value in the cover file is found. The proposed method enables hiding in colored images. Figure 10, primarily, 105th pixel has Red (157), Green (201) and Blue (212) data content. The three bit data to be hidden (110) is placed into LSB bits of the 105th pixel. At the end of the process, data content of the 105th pixel is converted to R (157), G (201) and B (246). As a result of the hiding process, only the content of Blue byte was changed by 1 bit. No change occurred in other bytes. These procedures were performed in the same manner for the 357th and 15th pixel, respectively and then 9 bit hidden message (110 100 010) was hidden, as seen on Figure 10. Bytes that experienced a change were shown as black rectangles on Figure 10. For a N-sized hidden message, these processes are repeated N times. Since the hiding process is carried out via random numbers indicated by RNG series, the chaotic system that makes up the RNG number system need to be known in order to acquire the hidden message.

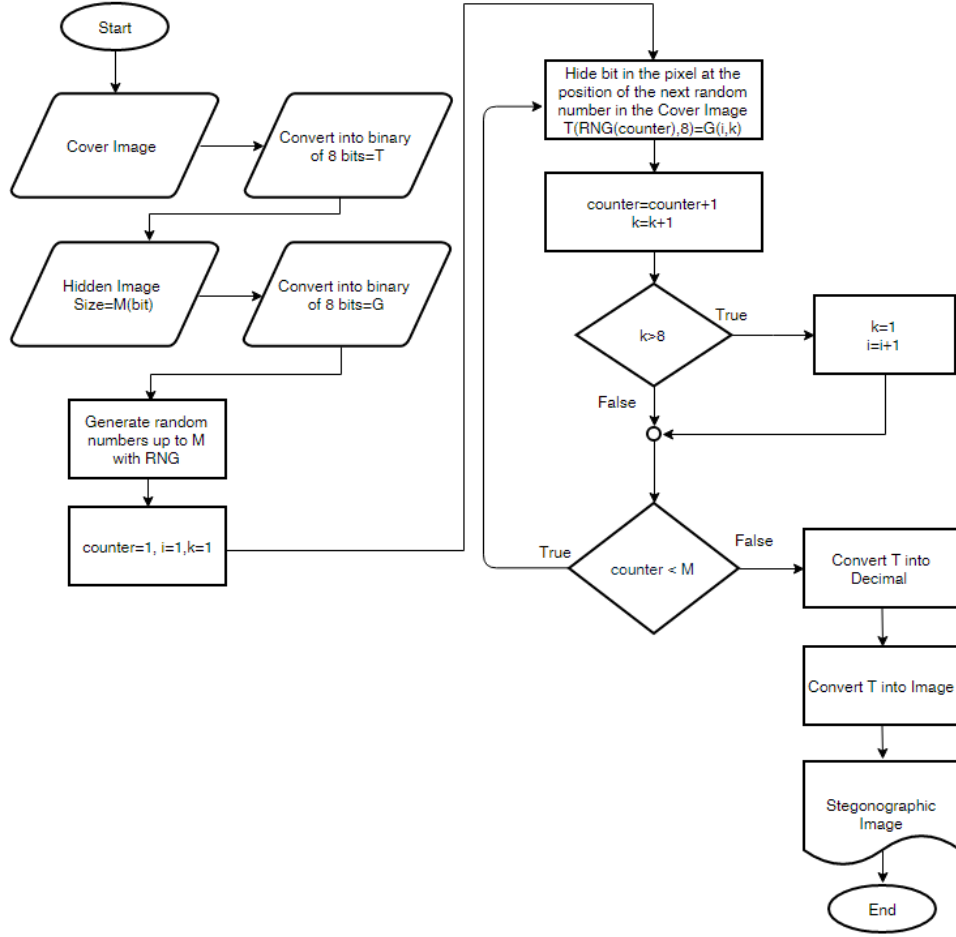


Figure 11: Block diagram for the proposed chaos based data hiding method

cover image. This operation continues until all bits are hidden.

Once all the hiding is completed, 8-bit cover information (T) is converted to decimal. Following this, conversion to image is carried out and stego image is created. As secret bits are hidden into cover image in a random manner, steganography algorithm is stronger than steganalysis methods. Thanks to random locator created with chaotic system, it becomes hard to locate hidden bits. RNG random number generator can be generated in repeating numbers. This is the reason why repeating numbers are discretized.

For data extraction, steps in data hiding are repeated in the same manner. Here, unlike data hiding, LSB bits of pixels indicated by RNG series are combined according to RNG series order and that is how the hidden message is found.

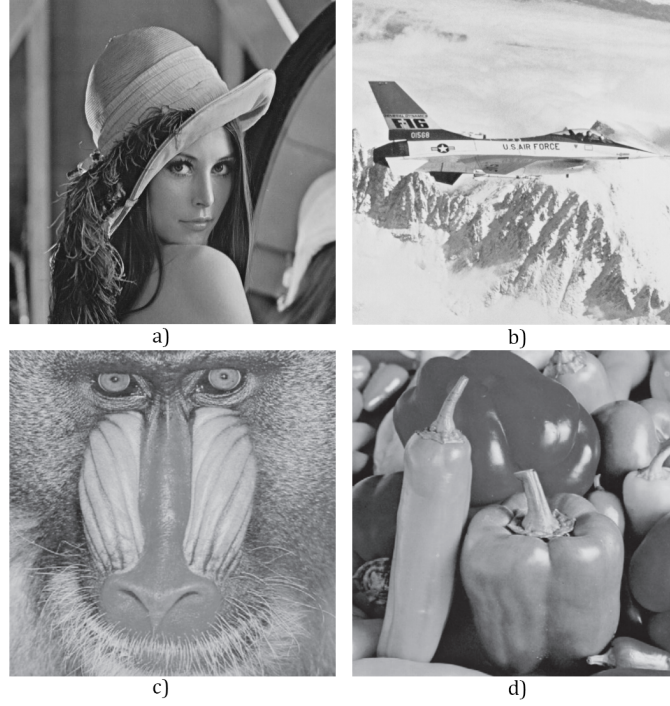


Figure 12: Original test images a)Lena b)Airplane c)Baboon d) Peppers

5. Experimental results

The algorithms were implemented in Matlab2014a on a PC with Intel Core i7 2.8 GHz CPU, 8096 MB RAM, and 64-bit Windows 10 system. Lena, Airplane, Baboon and Peppers images, used in experimental results, were taken from USC-SIPI image database [53]. Performance results of the proposed method were compared with the help of the same test images in Zhang and Wang's, Ni et al.'s, Kim et al.'s and Mielikainen's methods [54, 55, 56, 31]. 4 test images in 512x512 pixel size, given on Figure 12, were used as Lena, Airplane, Baboon and Peppers cover images, respectively. 256x256 bits data was hidden into each image.

A good data hiding method is, primarily, supposed not to cause any observable distortion on the cover image after data hiding. Figure 13 shows cover images prior to and following the data hiding with the proposed method on the left and right columns, respectively. Figure 13 (a), (c), and (e) show enlarged and cropped forms of original cover images Lena, Baboon and Pepper. Figure 13 (b), (d), and (f), on the other hand, exhibit images containing data hidden via the proposed method. An examination of images on the left and right, respectively, shows no visually observable difference.

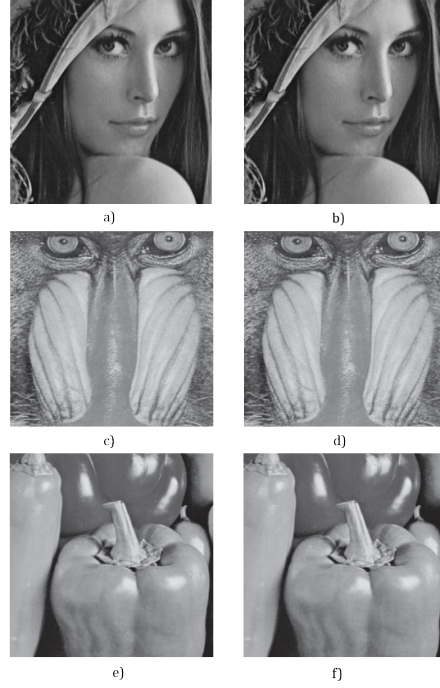


Figure 13: Original and stego images as cropped and enlarged

Figure 14 exhibits histogram graphs of the original test images and the stego images with 64 KB hidden data via the proposed method. The histogram of the image in which data was hidden according to histogram method is supposed to be different from the histogram of the original image. As can be seen on Figure 14, however, no change can be observed in any of the four test image histograms. These results are enough proof for the reliability of the proposed method.

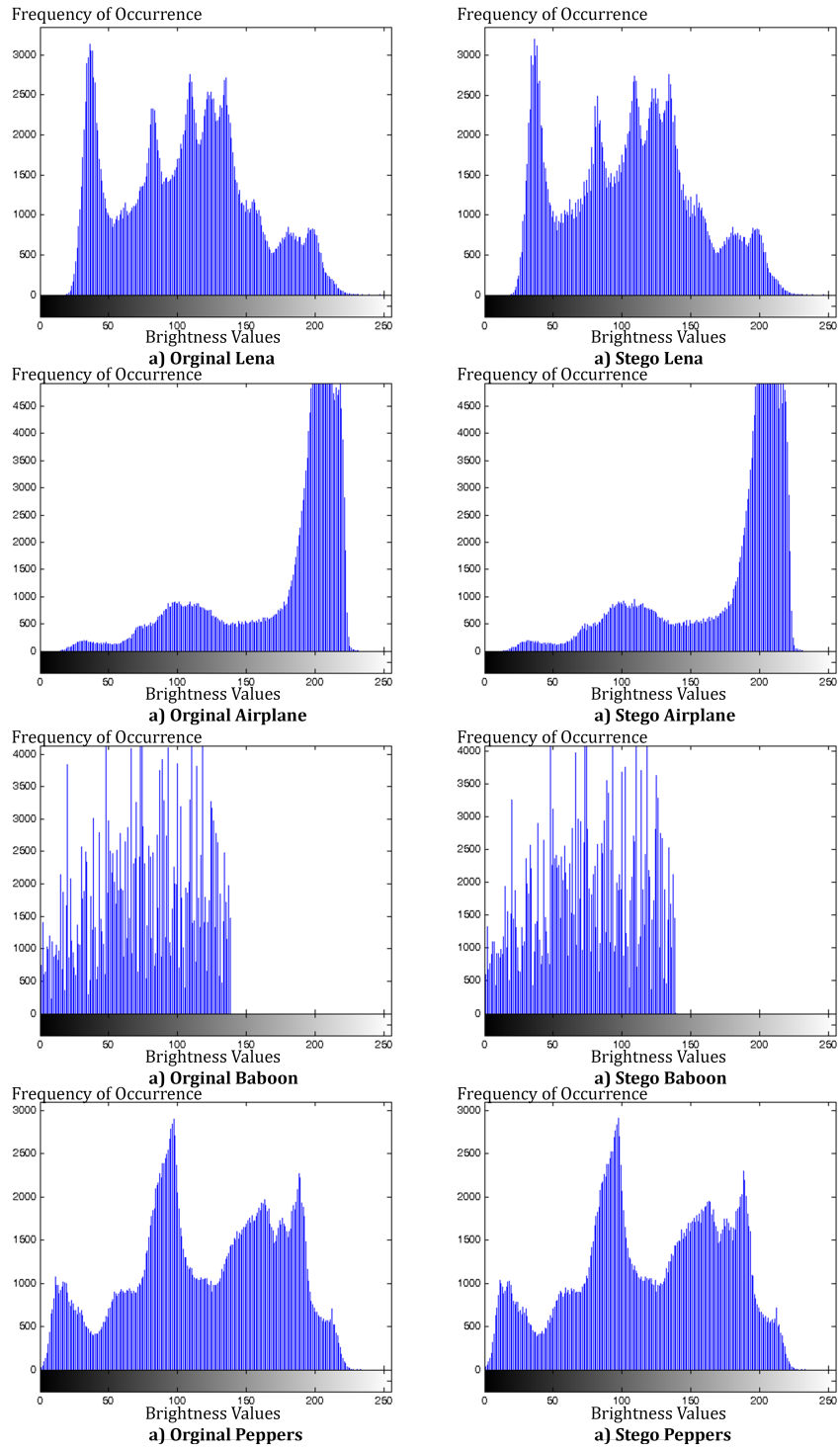


Figure 14: Histograms of the original and stego test images with 64 KB hidden data



Figure 15: Original and stego test images with hidden 64 KB data, following the LSB bit attack

So as to test the robustness of the proposed method, LSB bit attack was run on the original test images and the stego images with 64 KB hidden data via the proposed method. In LSB bit attack, LSB bit information of the image is destroyed. Distortions in the stego image with hidden data, as a result of the attack, are expected. Attack results are given in Figure 15. As a result of the attack, Figure 15 (d), (h) stego images exhibited no visual distortions, like in the original image. For Baboon image, as it is obvious from Figure 15, the original image has a black vision while the stego has a clear vision. Yet, no distortion on the image due to data hiding occurs. The results of the attack validate the strength of the proposed method.

Another crucial factor for the security of the method is that data hiding method operation must not be detected by steganalysis methods as well. For the measurement of distortions on cover images, two quality measures, namely mean squared error (MSE), given in Equation (5), and peak signal noise rate (PSNR), given in Equation (6), both of which are very commonly preferred in the literature, have been used.

$$\left\{ \begin{aligned} MSE &= \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [O(i, j) - S(i, j)]^2 \end{aligned} \right. \quad (5)$$

$$\left\{ \begin{aligned} PSNR &= 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \end{aligned} \right. \quad (6)$$

In Equation (5), m and n represent row and column information of the image; O represents original cover image; S represents hidden image. After MSE value is calculated, the next is the PSNR calculation. PSNR is an image criterion that assesses the similarity rate between cover image and hidden image. MAX in Equation (6) represents the maximum value for a pixel and it is usually 255.

Bit data in different amounts were hidden into 512x512 sized 5 gray images with four different methods in the literature and the proposed method and PSNR results of the stego images were compared on Table 2. The reason why black and white images were used as test images is that the studies used for comparison here were carried out with black and white images. Otherwise, a fair comparison would not be possible. In the proposed method, Zhang and Wang's and Mielkainen's method, 65.536 bit was hidden into the all pictures. In Ni et al. and Kim et al.s methods, on the other hand, bit data in different amounts were hidden. In Table 2, maximum data capacity to be hidden with the methods and also the amount of the data hidden were given as bits. Maximum capacity of data was hidden into all images with the help of all the methods. PSNR quality criteria scores that compare the original image with the stego image, following the hiding, are also given. It is clear that PSNR measurement results of the proposed method are more successful than other methods in all the test images. The proposed method produced the best score, 57,19 dB PSNR, in Airplane image. The average PSNR score of the proposed method is 57,17 dB. The second best result by Mielkainen's method is 52.39 dB. Kim et al's method offered 56,93 dB, the highest PSNR score, with 34.552 bit hiding while the proposed method offered hid 65.536 bit and scored 57.19

dB PSNR. Furthermore, data hiding capacity of the proposed method is higher than those of Ni et al. and Kim et al.'s methods. Proposed method's PSNR values are successful, which is related to the fact that the method hide data in the cover image in such a way that it cannot be discovered randomly.

Table 2: Comparison of PSNR values of the proposed method and the methods in the literature

Cover	Zhang and Wang		Ni et al.		Kim et al.		Mielkainen		Proposed Method	
	Embed(bit) Capacity	PSNR	Embed(bit) Capacity	PSNR	Embed(bit) Capacity	PSNR	Embed(bit) Capacity	PSNR	Embed(bit) Capacity	PSNR
Lena	65.536	52,12	5.414	48,13	53.883	55,00	65.536	52,38	65.536	57,16
Airplane	65.536	52,11	12.625	48,13	34.552	56,93	65.536	52,39	65.536	57,19
Baboon	65.536	52,11	3.567	51,20	19.473	59,42	65.536	52,39	65.536	57,16
Peppers	65.536	52,12	6.576	48,13	38.387	56,47	65.536	52,38	65.536	57,16
Average	65.536	52,11	7.045	48,89	36.573	56,95	65.536	52,39	65.536	57,17

6. Conclusions

A new approach to steganography methods, which are among secure communication techniques, is introduced in this article. A chaotic system without equilibrium points has been used with the proposed method and a RNG has been designed and a different steganograph application has been performed with the generated random numbers. Even if the existence of hidden data is detected in steganography method, chaotic RNG or the employed chaotic system is required in order to find the data because the order of the data is random. Since the realized application is chaos based and thus provides confusion and sensitivity, it is challenging for third parties to uncover hidden data. The steganalysis made here has shown the performance of the application. The proposed method has produced better results than studies in the literature in image criteria used for detection of distortion after hiding. It has also proven more successful than steganalysis methods. That the chaotic system used here has no equilibrium points makes some chaotic system analyses (Shilnikov method, etc.) difficult and thus it gets difficult for third parties to reach hidden data.

References

- [1] Akif Akgul and Ihsan Pehlivan. A New Three-Dimensional Chaotic System Without Equilibrium Points, Its Dynamical Analyses and Electronic Circuit Application. *Technical Gazette*, 23(1):209–2014, 2016.
- [2] Chunbiao Li, Ihsan Pehlivan, Julien Clinton Sprott, and Akif Akgul. A novel four-wing strange attractor born in bistability. *IEICE Electronics Express*, 12(4):20141116–20141116, 2015.
- [3] Akif Akgul, Haris Calgan, Ismail Koyuncu, Ihsan Pehlivan, and Ayhan Istanbulu. Chaos-based engineering applications with a 3D chaotic system without equilibrium points. *Nonlinear Dynamics*, 84(2):481–495, apr 2016.
- [4] Akif Akgul, Irene Moroz, Ihsan Pehlivan, and Sundarapandian Vaidyanathan. A new four-scroll chaotic attractor and its engineering applications. *Optik - International Journal for Light and Electron Optics*, 127(13):5491–5499, 2016.
- [5] Akif Akgul, Shafqat Hussain, and Ihsan Pehlivan. A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications. *Optik - International Journal for Light and Electron Optics*, 127(18):7062–7071, 2016.
- [6] Unal Cavusoglu, Akif Akgul, Sezgin Kacar, Ihsan Pehlivan, and Ahmet Zengin. A novel chaos-based encryption algorithm over TCP data packet for secure communication. *Security and Communication Networks*, 9(11):1285–1296, jul 2016.
- [7] J C. Sprott. A new class of chaotic circuit. *Physics Letters A*, 266(1):19–23, 2000.
- [8] Chunbiao Li, Ihsan Pehlivan, and Julien Clinton Sprott. Amplitude-phase control of a novel chaotic attractor. *Turkish Journal of Electrical Engineering and Computer Sciences*, 24:1–11, 2016.
- [9] J C Sprott. Simple chaotic systems and circuits. *American Journal of Physics*, 68:758–763, 2000.
- [10] Wajdi M. Ahmad and J.C. Sprott. Chaos in fractional-order autonomous nonlinear systems. *Chaos, Solitons & Fractals*, 16(2):339–351, 2003.
- [11] Jessica R Piper and J C Sprott. Simple Autonomous Chaotic Circuits. *IEEE Transactions On Circuits And SystemsII Express Briefs*, 57(9):730–734, 2010.
- [12] Guanrong Chen and Tetsushi Ueta. Yet another chaotic attractor. *International Journal of Bifurcation and Chaos*, 09(07):1465–1466, jul 1999.
- [13] Ali Durdu, Ahmet Turan Ozcerit, and Yilmaz Uyaroglu. A novel chaotic system for secure communication applications. *Information Technology and Control*, 44(3):271–278, 2015.

- [14] Chongxin Liu, Tao Liu, Ling Liu, and Kai Liu. A new chaotic attractor coined. *Chaos, Solitons and Fractals*, 12:659–661, 2004.
- [15] Gerard van der Schrier and Leo R.M. Maas. The diffusionless Lorenz equations; Shil’nikov bifurcations and reduction to an explicit map. *Physica D: Nonlinear Phenomena*, 141(1):19–36, 2000.
- [16] Qigui Yang and Guanrong Chen. A chaotic system with one saddle and two stable node-foci. *International Journal of Bifurcation and Chaos*, 18(05):1393–1414, may 2008.
- [17] Ihsan Pehlivan and Ylmaz Uyaroglu. A new chaotic attractor from general Lorenz system family and its electronic experimental implementation. *Turkish Journal of Electrical Engineering and Computer Sciences*, 18(2):171–184, 2010.
- [18] Qigui Yang, Zhouchao Wei, and Guanrong Chen. An unusual 3D autonomous quadratic chaotic system with two stable node-foci. *International Journal of Bifurcation and Chaos*, 20(04):1061–1083, 2010.
- [19] Karthikeyan Rajagopal, Sajad Jafari, Viet-Thanh Pham, Zhouchao Wei, Durairaj Premraj, Kathamuthu Thamilmaran, and Anitha Karthikeyan. Antimonotonicity, bifurcation and multistability in the vallis model for el niño. *International Journal of Bifurcation and Chaos*, 29(03):1950032, 2019.
- [20] Karthikeyan Rajagopal, Chunbiao Li, Fahimeh Nazarimehr, Anitha Karthikeyan, Prakash Duraisamy, and Sajad Jafari. Chaotic dynamics of modified wien bridge oscillator with fractional order memristor. *Radioengineering*, 28(1):165–174, 2019.
- [21] Atiyeh Bayani, Karthikeyan Rajagopal, Abdul Jalil M Khalaf, Sajad Jafari, GD Leutcho, and J Kengne. Dynamical analysis of a new multistable chaotic system with hidden attractor: Antimonotonicity, coexisting multiple attractors, and offset boosting. *Physics Letters A*, 2019.
- [22] Karthikeyan Rajagopal, Viet-Thanh Pham, Fawaz E Alsaadi, Fuad E Alsaadi, Anitha Karthikeyan, and Prakash Duraisamy. Multistability and coexisting attractors in a fractional order coronary artery system. *The European Physical Journal Special Topics*, 227(7-9):837–850, 2018.
- [23] Karthikeyan Rajagopal, Sundaram Arun, Anitha Karthikeyan, Prakash Duraisamy, and Ashokkumar Srinivasan. A hyperchaotic memristor system with exponential and discontinuous memductance function. *AEU-International Journal of Electronics and Communications*, 95:249–255, 2018.
- [24] Karthikeyan Rajagopal, Akif Akgul, Sajad Jafari, Anitha Karthikeyan, and Ismail Koyuncu. Chaotic chameleon: Dynamic analyses, circuit implementation, fpga design and fractional-order form with basic analyses. *Chaos, Solitons & Fractals*, 103:476–487, 2017.

- [25] Sajad Jafari, J.C. Sprott, and S. Mohammad Reza Hashemi Golpayegani. Elementary quadratic chaotic flows with no equilibria. *Physics Letters A*, 377(9):699–702, 2013.
- [26] Zhouchao Wei. Dynamical behaviors of a chaotic system with no equilibria. *Physics Letters A*, 376(2):102–108, 2011.
- [27] Zenghui Wang, Shijian Cang, Elisha Oketch Ochola, and Yanxia Sun. A hyperchaotic system without equilibrium. *Nonlinear Dynamics*, 69(1-2):531–537, jul 2012.
- [28] G.A. Leonov, N.V. Kuznetsov, and V.I. Vagaitsev. Localization of hidden Chuas attractors. *Physics Letters A*, 375(23):2230–2233, 2011.
- [29] G.A. Leonov, N.V. Kuznetsov, and V.I. Vagaitsev. Hidden attractor in smooth Chua systems. *Physica D: Nonlinear Phenomena*, 241(18):1482–1486, 2012.
- [30] Leonid P Shilnikov, Andrey L Shilnikov, Dmitry V Turaev, and Leon O Chua. *Methods of Qualitative Theory in Nonlinear Dynamics Part I*, volume 4 of *World Scientific Series on Nonlinear Science Series A*. World Scientific, sep 1998.
- [31] Jarno Mielikainen. LSB matching revisited. *IEEE Signal Processing Letters*, 13(5):285–287, 2006.
- [32] Chi-shiang Chan. On Using LSB Matching Function for Data Hiding in Pixels. 96:49–59, 2009.
- [33] Jun Tian. Reversible Data Embedding Using a Difference Expansion. *IEEE Transactions on Circuits and Systems*, 13(8):890–896, 2003.
- [34] Adnan M. Alattar. Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing*, 13(8):1147–1156, 2004.
- [35] Amir Anees, Adil Masood, Jameel Ahmed, and Iqtadar Hussain. A technique for digital steganography using chaotic maps. pages 807–816, 2014.
- [36] Sengul Dogan. A new data hiding method based on chaos embedded genetic algorithm for color image. *Artificial Intelligence Review*, 46(1):129–143, jun 2016.
- [37] Elnaz Ghasemi and A Broumandnia. Text steganography in digital images by chaos-based mapping, 2016.
- [38] S. S. V. Nithin Kumar, Gunda Sai Charan, B. Karthikeyan, V. Vaithiyanathan, and M. Rajasekhar Reddy. A Hybrid Approach for Data Hiding Through Chaos Theory and Reversible Integer Mapping, 2016.

- [39] Gunda Sai Charan, V Kumar, Nithin S. S., B. Karthikeyan, V. Vaithiyanathan, and Divya K. Lakshmi. A Novel LSB Based Image Steganography With Multi-Level Encryption. In *2015 International Conference On Innovations In Information, Embedded And Communication Systems (ICIIECS)*, 2015.
- [40] H. Nejati, A. Beirami, and W.H. Ali. Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. *Electronics Letters*, 48(24):1537–1538, 2012.
- [41] Liang Zhao, Xiaofeng Liao, Di Xiao, Tao Xiang, Qing Zhou, and Shukai Duan. True random number generation from mobile telephone photo based on chaotic cryptography. *Chaos, Solitons & Fractals*, 42(3):1692–1699, nov 2009.
- [42] Salih Ergun and Serdar Ozoguz. Truly random number generators based on a non-autonomous chaotic oscillator. *AEU - International Journal of Electronics and Communications*, 61(4):235–242, 2007.
- [43] Qingdu Li, Qifeng Liu, and Junli Niu. Chaotic oscillator with potentials in TRNG and ADC. In *2012 35th International Conference on Telecommunications and Signal Processing (TSP)*, pages 397–400. IEEE, jul 2012.
- [44] Karthikeyan Rajagopal, Akif Akgul, Sajad Jafari, and Burak Aricioglu. A chaotic memcapacitor oscillator with two unstable equilibriums and its fractional form with engineering applications. *Nonlinear Dynamics*, 91(2):957–974, 2018.
- [45] Ihsan Cicek, Ali Emre Pusane, and Gunhan Dundar. A novel design method for discrete time chaos based true random number generators. *INTEGRATION, the VLSI journal*, 47(1):38–47, 2014.
- [46] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti. A fast chaos-based true random number generator for cryptographic applications. In *Solid-State Circuits Conference, 2006. ESSCIRC 2006. Proceedings of the 32nd European*, pages 130–133. IEEE, 2006.
- [47] İsmail Koyuncu and Ahmet Turan Özcerit. The design and realization of a new high speed fpga-based chaotic true random number generator. *Computers & Electrical Engineering*, 2016.
- [48] Erdiñç Avaroğlu, İsmail Koyuncu, A Bedri Özer, and Mustafa Türk. Hybrid pseudo-random number generator for cryptographic systems. *Nonlinear Dynamics*, 82(1-2):239–248, 2015.
- [49] Michael François, Thomas Grosge, Dominique Barchiesi, and Robert Erra. Pseudo-random number generator based on mixing of three chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 19(4):887–895, 2014.
- [50] İsmail Koyuncu, Ahmet Turan Ozcerit, and Ihsan Pehlivan. Implementation of fpga-based real time novel chaotic oscillator. *Nonlinear Dynamics*, 77(1-2):49–59, 2014.

- [51] Christos Volos, Akif Akgul, Viet-Thanh Pham, Ioannis Stouboulos, and Ioannis Kyprianidis. A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme. *Nonlinear Dynamics*, pages 1–15, 2017.
- [52] Mohammad Ali Jafari, Ezzedine Mliki, Akif Akgul, Viet-Thanh Pham, Sifeu Takougang Kingni, Xiong Wang, and Sajad Jafari. Chameleon: the most hidden chaotic flow. *Nonlinear Dynamics*, pages 1–15, 2017.
- [53] Allan G. Weber. The USC-SIPI Image Data Base. Technical report, 1993.
- [54] Xinpeng Zhang and Shuozhong Wang. Efficient Steganographic Embedding by Exploiting Modification Direction. *IEEE Communications Letters*, 10(11):781–783, nov 2006.
- [55] Zhicheng Ni, Yun Q Shi, Nirwan Ansari, and Wei Su. Reversible Data Hiding. *IEEE Communications Letters*, 10(11):1–3, 2006.
- [56] Dae-Soo Kim, Gil-Je Lee, and Kee-Young Yoo. Reversible Image Hiding Scheme for High Quality Based on Histogram Shifting. In *2013 10th International Conference on Information Technology: New Generations*, pages 392–397. IEEE, apr 2013.