ISSN: 0067-2904

Key Generator to Encryption Images Based on Chaotic Maps

Ahmed Yousif*, Ali H. Kashmar
Department of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq

Abstract

It is known that images differ from texts in many aspects, such as high repetition and correlation, local structure, capacitance characteristics and frequency. As a result, traditional encryption methods can not be applied to images. In this paper we present a method for designing a simple and efficient messy system using a difference in the output sequence. To meet the requirements of image encryption, we create a new coding system for linear and nonlinear structures based on the generation of a new key based on chaotic maps.

The design uses a kind of chaotic maps including the Chebyshev 1D map, depending on the parameters, for a good random appearance. The output is a test in several measurements, including the complexity of the standard balance and time execution.

The results show that any change in input will change the output and the time required for the application requires only parts of the minute.

The output is passed through the exponential function [exp (X))] to obtain a wide range of input. The result is then set to machine words to fit the desired range of multicast used.

The next step is the output of machine words that will be used as input to the array that we have structured to generate the key. The key is converted to a sequential element into an element with an ordinary image to produce the encrypted image. Furthermore, keystream succeeded by passing tests (NIST statistical package tests for random). Finally, the real-time image encoding of the corresponding algorithm was applied; preliminary results show that the proposed algorithm has good coding strength with added benefit that resists security analysis.

Keywords: Cryptography, Symmetric key, Chaotic Maps, Image encryption, NIST.

توليد مفتاح لتشفير الصور بالاعتماد على الدوال الفوضوية

احمد يوسف*، علي حبيب
قسم الرياضيات، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

من المعروف أن الصور تختلف عن النصوص في العديد من الجوانب ، مثل التكرار الشديد والارتباط ، والبنية المحلية وخصائص السعة والتكرار. ونتيجة لذلك، لا يمكن تطبيق طرق التشفير التقليدية على الصور. نقدم في هذا البحث طريقة لتصميم نظام فوضوي بسيط وفعال باستخدام اختلاف في تسلسل المخرجات . لتحقيق متطلبات تشفير الصور، نوجد نظام تشفير جديد للبنية الخطية و غير الخطية على أساس توليد مفتاح جديد يعتمد على الخرائط الفوضوية.

يستخدم التصميم نوع من خرائط الفوضى بما في ذلك، خريطة Chebyshev 1D ، اعتمادا على المعلمات ، لظهور عشوائية جيدة. يمثل المخرج اختباراً في عدة قياسات، بما في ذلك تعقيد التوازن المعياري

Email: math.ahmedyousif@gmail.com

والتنفيذ الزمني. تظهر النتائج أن أي تغيير في المدخلات سوف يغير الناتج والوقت اللازم لتطبيقه يتطلب اجزء من الدقيقه فقط. يتم تمرير الإخراج من خلال الدالة الأسية [exp (X)] الحصول على نطاق واسع من الإدخال. ثم يتم تعيين النتيجة إلى machine words لتلائم النطاق المطلوب من تعدد الإرسال المستخدم. المرحلة التالية مخرجات machine words سوف تستعمل كمدخلات الى الصفوفة التي قمنا بهيكلتها لتوليد المفتاح. يتم تحويل المفتاح إلى عنصر متسلسل إلى عنصر مع صورة عادية لإنتاج الصورة المشفرة. علاوة على ذلك، نجح keystream من خلال اجتياز اختبارات NIST (اختبارات حزمة إحصائية لعشوائية). وأخيرًا، تم تطبيق تشفير الصور في الوقت الفعلي للخوارزمية المقابلة؛ تظهر النتائج الأولية أن الخوارزمية المقترحة لديها قوة تشفير جيدة مع الفائدة المضافة التي تقاوم التحليل الأمني.

1. Introduction

The detailed investigation and analysis of nonlinear dynamical system based on the developing of chaotic functions has been much interesting in a period of past ten years. Chaotic functions become larger for different applications such as information technology, digital communications and cryptography either theory or practice. The fundamental truth of sensitively dependence on its initial condition is the most significant feature of the chaotic system; Prof Lorenz is the first researcher who illustrated this properly. In the course of a search, he discovered that a bit changed the initial conditions in the system of differential equations could completely change the resulting after short period [1], such particular feature of chaos has been supported by many researchers [2, 3].

Uncorrelated number, Random-looking sequences and reproducible singles can be generating based on the principle of the sensitive dependence of chaotic systems on their initial conditions. Due to the deterministically and disguising modulation property, chaotic dynamical system can be easily made as noise based on its random-like behaviour [4]. Many advantages have been provided by the application of chaotic sequence over conventional binary sequences, particularly Pseudorandom Number Generators (PRNGs) sequences that frequently employed in cryptography and digital communications [5]. The consideration of conventional systems is not a good choice of transmitting message with efficient way, thus employing chaotic maps become necessary in the design of a secure cryptosystem. Diffusion and confusion, the two basic structure of symmetric key encryption can be modeled well by chaos theory [6], moreover the coupled between chaos theory and DNA, offered efficient method to encrypt information [7].

The focus of the paper is heavy built upon the theory of chaos. The application of the theory of chaos to cryptography is the main objective of this research.

The eligible chaotic PRNG was created, based on the equations and derived from nonlinear dynamical system capable of exhibiting chaos,

$$x_{n+1} = r x_n (1 - x_n) , \quad (1.1)$$

For each use, a different initial condition was assigning, stars the chaotic map with the initial condition of the intended receiver and repeatedly generated points of the orbit. Sensitively depending on its initial values x_0, for these values of r, the orbit will be great numbers which are noise-like, random-like and reproducible. Therefore, cipher system based on chaotic PRNG resistance against security attack [8].

This paper outlines the work of the author's investigation into the generation of new keystream dependent on hybrid chaotic maps. Many crypto systems depended chaotic maps have been proposed in the past [9-13]. However, the effecting of these researches made rather marginal on modern cryptography for many reasons; chaos-based cryptographic algorithms in general employ a dynamical system defined on a set of real numbers so that it is hard for application, implement slow and weak keystream generation and do not provide security.

A new method to Key Generator to Encryption Images Based on Chaotic Maps for symmetrical algorithms will be presented. In the next section, the chaotic map in cryptography was briefly introduced. A central part of the paper describes the construction of new. In the following two sections, the paper gives the significant properties of propose algorithm as well as results and discussions**.** Finally, the paper contributes some conclusions.

2. Related Works

Shannon in his classic 1949 first mathematical paper on cryptography proposed chaotic maps as models - mechanisms for symmetric key encryption, before the development of Chaos Theory [14]. Hopf based this remarkable intuition on the use of the Baker's map in 1934 as a simple deterministic mixing model with statistical regularity [15].

Over the past twenty years, nonlinear chaotic systems have been used in the design of digital data encryption and transmission systems. The similarities between the chaotic maps and the cryptographic systems are the main motivation for the design of chaos based cryptographic algorithms. Hundreds cryptosystems designed based on chaos and nonlinear dynamic systems including, PRNGs, block and stream ciphers, hash functions, public-key ciphers, image encryptions, steganography and watermarking [16]. They emerged as a new promising candidate for cryptography because many chaos fundamental characteristics such as a broadband spectrum, periodicity and high sensitivity to initial conditions are directly connection as well as two basic properties of good ciphers, confusion and diffusion [17].

Generally, the low costs and speed make chaotic system more efficient than traditional methods for image encryption [18]. In this section, the briefly consideration of some significant improvements on image encryption methods using chaotic system will be provided. First, Matthew [19] introduced a new encryption algorithm based on a logistic map, then, Fridrich [20] followed him, proposed a new architecture for image encryption with two stages permutation and diffusion utilized 1D and 2D chaotic maps. Additionally, Guan et al.[21] has been used both of permutation /diffusion for the image encrypting applied 3D Arnolad's catmap and Chen chaos system. After that, Pareeka et al.[22] suggested 8 various kinds of operations utilized with 80-bit key to accomplish the encryption process based on two logistic map. In [23] a new method was introduced depending on the use multi-chaotic functions with Rossler attractor to generate the key for permutation all image pixels. [24] Introducing two general tent chaotic maps to increase the degrees of freedom and produce a versatile response that can fit many cipher applications. [25] proposing a novel image encryption algorithm based on two pseudorandom bit generators; Chebyshev map for permutation and rotation equation for substitution operations. [26] An image encryption algorithm based on Ikeda and Henon chaotic maps is presented. [27] Proposing a novel image encryption scheme based on the chaotic tent map, to generate key stream by a 1D chaotic tent map, that is more suitable for image encryption. Finally, [28] discussing and presenting an image encryption and decryption approach using Gauss iterated map.

3. The Proposed System Construction

The structure design of propose algorithm, as illustrated in Figure-1 below, shows that, it is modern technique based on Chebyshev map.

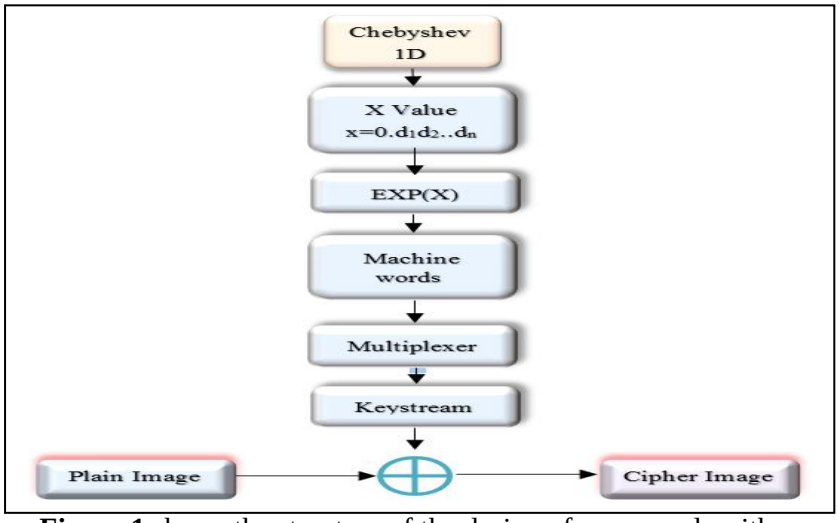

Figure 1 shows the structure of the design of propose algorithm.

As demonstrated in Figure-1, the algorithm depends on several steps:

Step 1: Use the chaotic map

- Chebyshev: $f(x_{n+1}) = cos(karccos(x_n))$.

Where, $-1 \leq x_n \leq 1, n = 1, 2, 3,$

Step 2: Enter the initial parameters values.

Step 3: Apply the chebyshev map to generate a sequence of new values of x, which are real numbers between 0 and 1.

Step 4: Find the Exponential to generate the extended values Exp(x).

Step 5: Find the Floating-Point Representation group of random numbers.

Step 6: Find the Random Keystream based on the random Matrix Table.

Step 7: Utilize the key for the encryption and decryption processes.

4. The Test Vectors for Executing Propose System

This section is dedicating for the design and implementation of the proposed digital image encryption system. Generally, the proposed system encrypted a colored squared digital image using the advantage of chaotic maps properties to make the encryption more secure and robust against security attacks. In the following subsections, test vectors show the results of implementing propose algorithm for the key generation steps and encryption/decryption processes.

4.1 Key Generation Steps

As shown in Figure-1, the key generation is presenting by the following steps:

1. Enter the parameters of Chebyshev (1D) Map to get a good randomness , as shown in Figure-2.

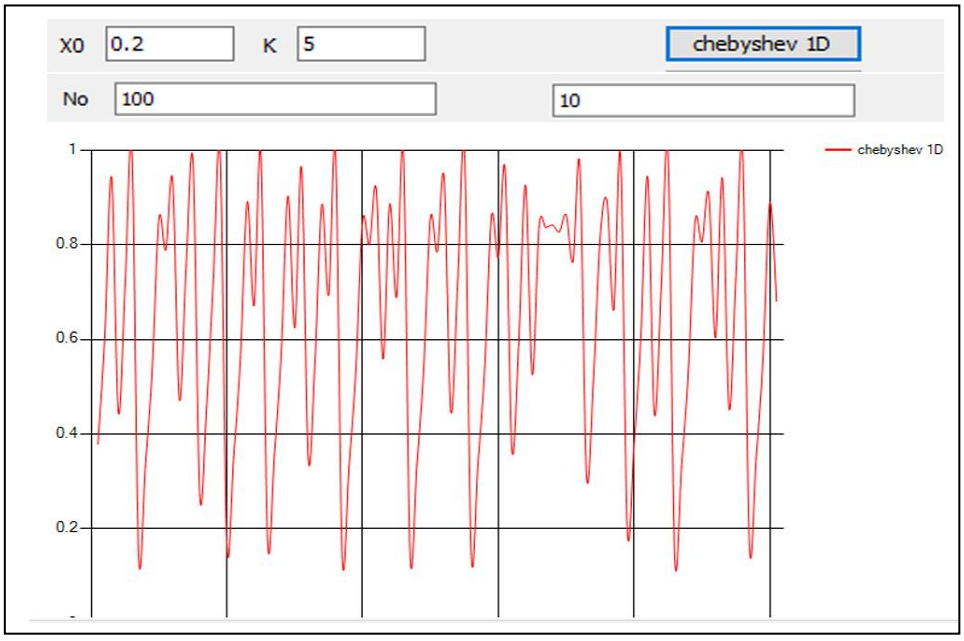

Figure 2 -Show the parameter chebychev map

2. The output of Chebyshev map is passing through the exponential function [exp(x)] to get wide range of input as shown in Figure-3.
3. Then the result of step 2 is mapping into words to fit the required domain of the used multiplexed.

No	X	Exp(x)	Machine Words
0	0.378286738313747	1.4597814581445	401485D0635B18
1	0.604907566120297	1.83108294696228	40152E58A1887490
2	0.942699401149351	2.56690117050383	4018CE3CC928003C
3	0.446447899221967	1.56275126487814	4014CCBA4BB22C18
4	0.71332552526167	2.04076660751219	401BB52BEA7B73
5	0.999042637777578	2.71568069343945	4019045CF566EB24
6	0.143701165915936	1.15453904135163	4015C1C48EEC7F
7	0.332850639597567	1.39493893426892	40148FAD8DF43B30
8	0.5372317106248	1.71126302780316	401502C1880BAE70
9	0.855583954498669	2.35274787721323	4018805434C441AC

Figure 3 -Shown the Exp(x) and machine words steps.

4. The next stage is passing the dictionary words into the multiplexer to produce the secret keystream. The multiplexer stage works to find the random keystream based on the random Matrix Table(10×6), as shown in Figure-4 , generation such keystream represented as a main goal of the proposed algorithm such that the input machine words to get the random keystream .

	A	B	C	D	E	F
0	1093	1073	1047	1126	1027	844
1	1096	1021	1138	1130	1115	1069
2	1144	827	1108	887	1132	1064
3	1006	993	1140	1111	1031	667
4	1089	1019	1135	1131	1113	1067
5	1145	879	1074	1128	1143	1070
6	1081	962	1041	944	1112	1141
7	1084	942	1050	1133	905	1142
8	1085	826	1063	1129	1028	866
9	1094	1020	1139	1134	1117	1068

Figure 4-Shown the Random Matrix Table

5. The cipher image after applied encryption process shown in Figure-5.

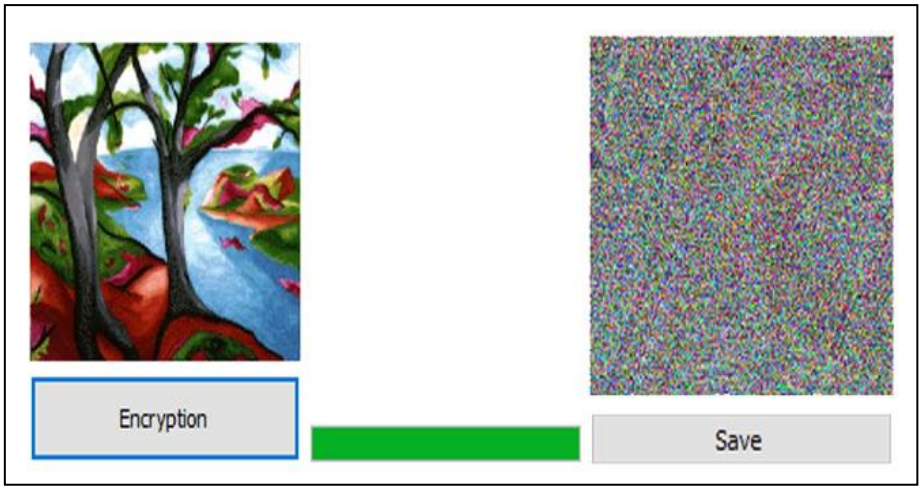

Figure 5-Shown the cipher image after encryption.

4.2 Decryption Process

For decryption process, as shown in Figure-6, the receiver employs the output of stream generator is xor'ed sequentially item to item with cipher image to produce the plain image.

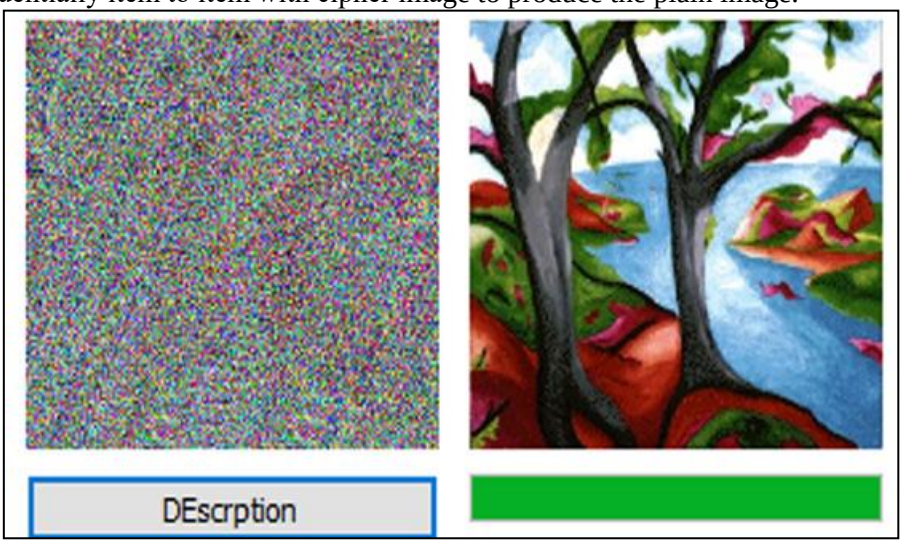

Figure 6-Shown the plain image after decryption

6. Results and Discussions

Histogram analyses for cipher image consider important tools for evaluating the proposed system. The most important thing here is the distribution of the histogram graph for the encrypted image should hide the redundancy of the plain image and looks like as uniformed as possible. This test is applied on the standard test images and their encrypted images and the results are listed in the Figure-7 o show the difference between them.

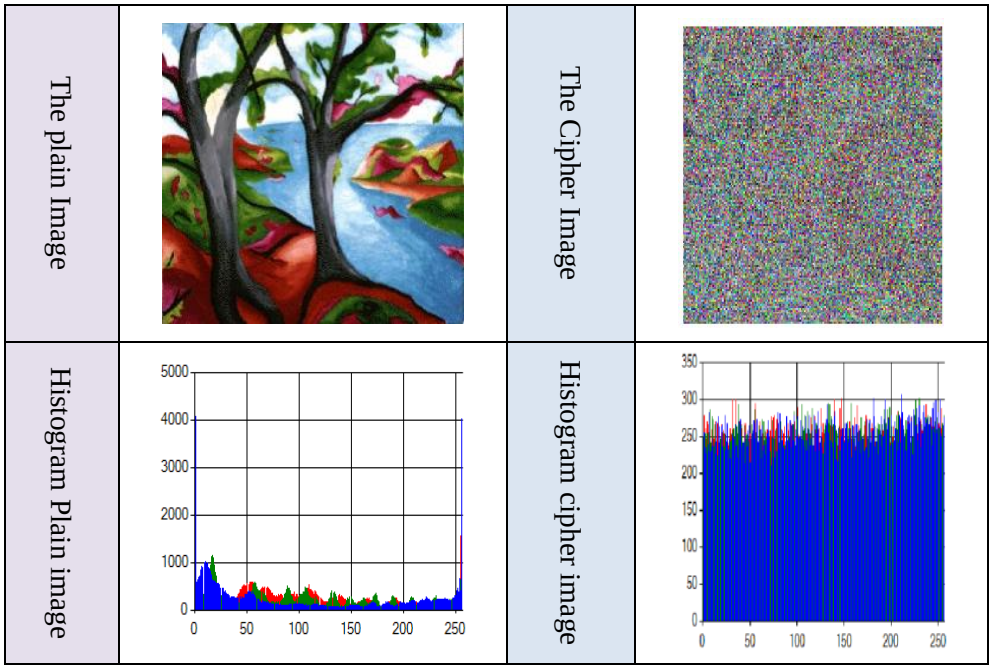

Figure 7-The Histogram for the Plain Image and Cipher Image

Furthermore, the keystream pass statistical tests for randomness as shown in Table-1.

Table 1-The Results of NIST Statistical Suite Tests for the key stream

Statistical Tests	*P*- Values	Result
Frequency	0.511369	SUCCESS
Block Frequency (128)	0.515017	SUCCESS
Runs	0.544917	SUCCESS
Long Runs of Ones (10000)	1.000000	SUCCESS
Rank	0.000000	SUCCESS
Spectral DFT	0.381350	SUCCESS
Non-Overlapping Templates	1.000000	SUCCESS
Overlapping Templates (9)	1.000000	SUCCESS
Universal (7)	0.600640	SUCCESS
Linear Complexity (500)	1.000000	SUCCESS
Serial 1 (16)	0.498961	SUCCESS
Serial 2 (16)	0.498531	SUCCESS
Approximate Entropy (10)	1.000000	SUCCESS
Cumulative – sums Fwd	0.528055	SUCCESS
Cumulative – sums Rev	0.536731	SUCCESS
Random Excursions	0.941084	SUCCESS
Random Excursions Variant	0.983947	SUCCESS

6.Peak signal-to-noise ratio analysis

A general requirement for all image encryption schemes is that the encrypted image should be greatly different from its original form. In our work, we use a similarity measurement metric—Peak Signal-to-Noise Ratio (*PSNR*) to measure the difference between the original image and the encrypted image. *PSNR* is mathematically defined as

$$\begin{cases} PSNR = 2\log_{10}\left(255/\sqrt{MSE}\right) \\ MSE = \dfrac{1}{M \times N}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(P_0(i,j)-P_1(i,j)\right)^2 \end{cases} \quad (6.1)$$

where M and N are the width and the height of the test image, respectively. $P0(i, j)$ and $P1(i, j)$ are the pixel values of the original image and the encrypted one, respectively. *MSE* is the mean squared error between the original image and the encrypted image. The larger the *MSE* value, the smaller the *PSNR* value, the better the encryption security.

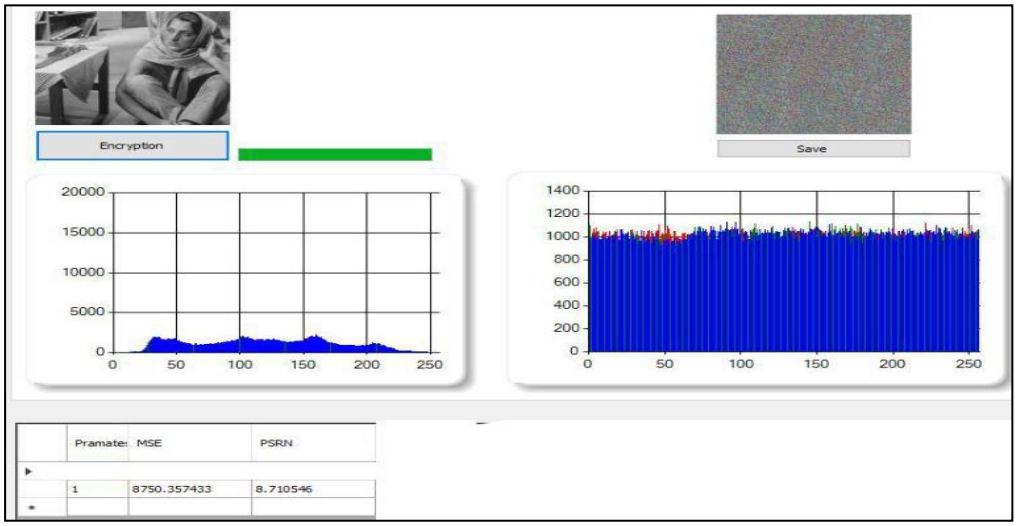

Figure 8-The Histogram , MSE and PSNR for the Plain Image and Cipher Image

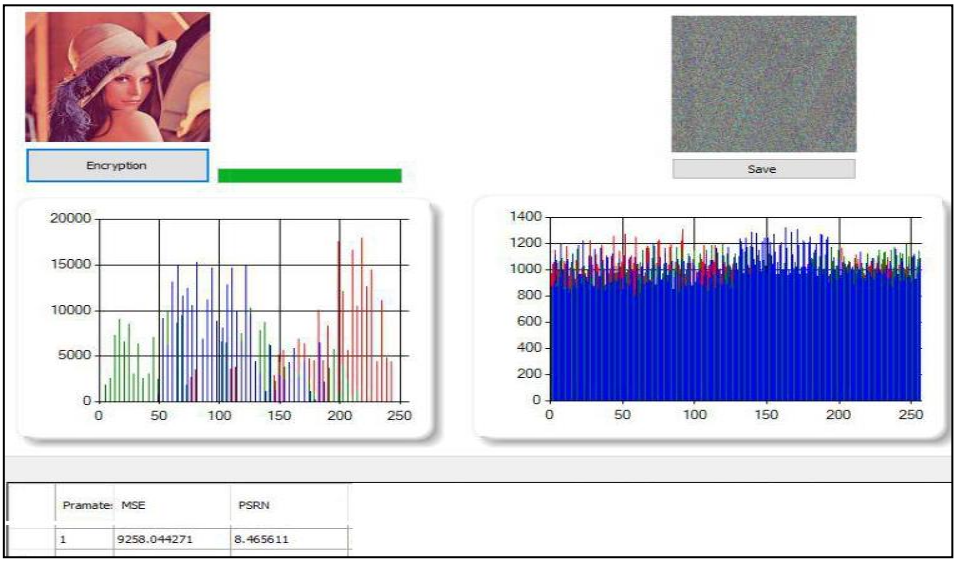

Figure 9-The Histogram , MSE and PSNR for the Plain

8. Conclusion

This paper presented a new method for introducing keystream generator mechanism called Key Generator to Encryption Images Based on Chaotic Maps. The design of our work depends on Chebyshev map. The output is test in several measurements represent including complexity, time execution and avalanche criterion balance; the results show that the keystream generation successfully passed through NIST. Finally, image encryption in real time for the corresponding algorithm was applied; preliminary results show that our proposed algorithm has good cryptographic strength with the added benefit that is resistant against security analysis.

References

1. Lorenz, Edward N. **1963.** "Deterministic Nonperiodic Flow". *Journal of the Atmospheric Sciences*. **20**(2): 130–141.
2. Lighthill, J. **1986.** "*The recently recognized failure of predictability in Newtonian dynamics*", Proc. Roy. Soc. London A407, 35-50
3. Devaney, R. **1992.** "*A First Course in Chaotic Dynamical Systems*", Perseus Books.
4. Vinod Patidar and Sud, K. K. **2009.** "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing" , *Informatica Journal*, **33**(2009): 441–452.
5. Piyush Kumar Shukla , Ankur Khare , Murtaza Abbas Rizvi , Shalini Stalin and Sanjay Kumar. **2015**. "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing", *Journal Entropy*, **17**: 1387-1410.
6. Wang, Xingyuan and Zhao, Jianfeng **2012.** "An improved key agreement protocol based on chaos". *Commun. Nonlinear Sci. Numer. Simul*. **15**(12): 4052–4057.
7. Babaei, Majid. **2013.** "A novel text and image encryption method based on chaos theory and DNA computing". *Natural Computing. An International Journal*. **12**(1): 101–107.
8. George Makris, G. and Ioannis Antoniou, L. **2012.** "*Cryptography with Chaos*", Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece, pp: 309-318.
9. Jakimoski, G. and Kocarev, L. **2001.** " Chaos and cryptography: block encryption ciphers based on chaotic maps, Circuits and Systems I: Fundamental Theory and Applications", *IEEE Transactions* on **48**(2) 309 (2001): 163–169.
10. Alvarez, G. and Li, S. **2006.** "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems". *International Journal of Bifurcation and Chaos*, World Scientific, **16**: 2129-2151.
11. Bogdan, C., Chargé, P. and Fournier-Purnaret, D. **2007.** "Behavior of Chaotic Sequences Under a Finite Representation and its Cryptographic Applications", IEEE Workshop on Nonlinear Maps and Applications (NOMA), Toulouse, 2007.

12. Amigó, J.M. **2009.** "*Chaos-Based Cryptography. In: Intelligent Computing Based on Chaos*", Springer, ISBN 978-3-540-95971-7, pp. 291-313, Berlin.
13. Alvarez, G., Amigó, J.M., Arroyo, D. and Li, S. **2011**. "Lessons Learnt from Cryptoanalysis of Chaos-based Ciphers, in Chaos-Based Cryptography. Theory, Algorithms and Applications". *Studies in Computational Intelligence*, **354**: 257-295.
14. Shannon, C. **1949.** "Communication Theory of Secrecy Systems". *Bell System Technical Journal*, **28**(4): 656–715.
15. Hopf, E. **1934.** "On Causality, Statistics and Probability", *J. Math. and Phys*. **13**: 51-102.
16. Akhavan, A., Samsudin, A. and Akhshani, A. **2011.** "A symmetric image encryption scheme based on combination of nonlinear chaotic maps". *Journal of the Franklin Institute*. **348**(8): 1797–1813.
17. Behnia, S., Akhshani. A., Mahmodi, H. and Akhavan, A. **2008.** "A novel algorithm for image encryption based on mixture of chaotic maps". *Chaos, Solitons & Fractals*. **35**(2): 408–419.
18. Wang, X., Teng, L. and Qin, X. **2012.** "A novel colour image encryption algorithm based on chaos". *Signal Processing*, 2012. **92**(4): 1101-1108.
19. Matthews, R. **1989.** "On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 1989. **13**(1): 29-42.
20. Fridrich, J. **1998**."Symmetric ciphers based on two-dimensional chaotic maps". *International Journal of Bifurcation and chaos*, 1998. **8**(06): 1259-1284.
21. Guan, Z.-H., Huang, F. and Guan, W. **2005.** "Chaos-based image encryption algorithm". *Physics Letters A*, 2005. **346**(1): 153-157.
22. Pareek, N.K., Patidar, V. and Sud, K.K. **2006.** "Image encryption using chaotic logistic map. Image and vision computing", 2006. **24**(9): 926-934.
23. Alsafasfeh, Q.H. and A.A. Arfoa, **2011**. "Image encryption based on the general approach for multiple chaotic systems". *J. Signal and Information Processing*, 2011. **2**(3): 238-244.
24. Salwa, K., Abd-El-Hafiz, Ahmed. G., Radwan, and Sherif H. AbdEl-Haleem, **2015.** "Encryption Applications of a Generalized Chaotic Map", *Appl. Math. Inf. Sci*. **9**(6): 3215-3233 (2015).
25. Borislav Stoyanov and Krasimir Kordov. 2015 "Image Encryption Using Chebyshev Map and Rotation Equation", Journal Entropy 2015, 17, pp:2117-2139.
26. Şekertekin, Y. and Atan, Ö. 2016 , "An image encryption algorithm using Ikeda and Henon chaotic maps" , 24th Telecommunications Forum (TELFOR). Belgrade, Serbia.
27. Chunhu Li, Guangchun Luo, Ke Qin and Chunbao Li., 2016. "An image encryption scheme based on chaotic tent map" Nonlinear Dynamics Journal; 87, 1; pp:127-133.
28. Sharma, M. C. and Sharma, P., 2017. "Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map" International Journal of Computer Applications, Volume 157 – No 3, pp: 18-23, January 2017.