

Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)

Rajaa Ahmed Ali* - Taha Mohammed Hasan** - Ebtisam K. Abdulah***
Ismael Salih Aref**

*University of Information Technology and Communication

** University of Diyala College of Science

*** University of Baghdad - College of administration and Economics

Received 21 February 2016 ; Accepted 28 April 2016

Abstract

Security is one of the significant challenges that people are faced over the entire world in every aspect of their lives. One of the methods used in security areas is cryptography. In this work we have investigated the possibility of using the multi logistic maps in the dynamical matrix for pseudo random number generator. Theoretical analysis and experimental show the sequences generated by the proposed random number generated possess many good properties. The proposed can be used in many applications requiring random binary sequences and also in the design of secure cryptosystems.

Keywords: Chaos, Logistic map, Cryptography.

مولد الأرقام العشوائية الديناميكي السريع مع تطبيقات في أنظمة التشفير

رجاء احمد علي* طه محمد حسن** ابتسام كاظم عبدالله*** اسماعيل صالح عارف**

*جامعة تكنولوجيا المعلومات والاتصالات

** جامعة ديالى - كلية العلوم

***جامعة بغداد - كلية الادارة والاقتصاد

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali

Taha Mohammed Hasan

Ebtisam K. Abdulah

Ismael Salih Aref

الخلاصة

الأمن هو احد التحديات الهامة التي تواجه الناس في جميع انحاء العالم في كل جانب من جوانب حياتهم. واحدى الطرق المستخدمة في حماية البيانات هو التشفير. في عملنا هذا تم تصميم مولد ارقام عشوائية ديناميكية سريع لتوليد متتابعة من الارقام العشوائية التي اجتازت الاختبارات الاحصائية وتم استخدامها في انظمة التشفير لتشفير نصوص وصور وكانت النتائج جيدة بعد اجراء الاختبارات على النصوص والصور المشفرة.

الكلمات المفتاحية: الفوضى، خريطة لوجستية، التشفير.

Introduction

With the rapid development of multimedia and network technologies, the security of multimedia becomes more and more important, since multimedia data are transmitted over open networks more and more frequently. Typically, reliable security in storage and transmission of digital speech data, images and videos is needed in many real applications, such as pay-TV, medical imaging systems, military image databases as well as confidential video conferences. In recent years, some consumer electronic devices, such as mobile phones, have also started to provide the function of saving and exchanging digital speech/music data, images and video clips under the support of multimedia messaging services over wireless networks, which is urgently demand for multimedia security. To meet the above needs in practice, some encryption algorithms are required to offer a sufficient level of security for different multimedia applications. Apparently, the simplest way to encrypt multimedia data is to consider the 1-D, 2-D or 3-D) multimedia bit-stream as a 1-D signal, and then to encrypt it with any available cipher [1]. In some multimedia applications, such a simple way may be enough. However, in many applications, especially when digital images and videos are involved, encryption schemes considering special features of the multimedia data, such as bulky size and large redundancy in uncompressed images/videos, are still required to achieve a better overall performance and to make the integration of the encryption scheme into the whole processing procedure easier. Since the 1990s, many different algorithms have been proposed to provide solutions to image encryption, video encryption and speech encryption [2]. Meanwhile, some cryptanalysis work has also been published and a number of multimedia encryption schemes have been found to be insecure from the cryptographical point of view [1]. On the whole, the

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

cryptanalytic work is still not enough now compared with cryptographic one, which is the main reason for publication of so much insecure encryption schemes. Due to the tight relationship between chaos theory and cryptography, a great number of multimedia and text encryption schemes use chaos as a mechanism to realize secret permutations of digital images/frames, or as a source to generate pseudo-random bits to control secret encryption operations [2].

As we well-known, cryptanalysis and cryptography are the two sides of cryptology which promote each other mutually. To accelerate the development of designing secure multimedia and text ciphers, we choose the security analysis (i.e., cryptanalysis) of some chaos related multimedia and text encryption schemes as the research topic of this thesis. In this paper, we evaluate the encryption quality of the robust chaotic block cipher. With the application of an encryption algorithm to an image and text, its pixels values change when compared with the original image. A good encryption algorithm must make these changes in an irregular manner and also maximize the difference in pixels values and text values between the original and the encrypted image and text.

Related Work

Image cryptography was not studied as normal cryptography or visual cryptography. It was used by [3], to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access. They proposed a version of digital image cryptography by using random phase mask for encrypting image. The authors consider image encoding as a new form of image encryption. They accomplish this using a transformation technique based on random phase masks. Their technique of encryption consists of four major steps. Fourier transform of initial image, phase modification, inverse Fourier transform and finally image conversion. It is a good concept but the weakest link lies in the use of steganography. Using image cryptography and steganography to increase security but they have not considered the use of image cryptography to disguise text cryptography which would provide enhanced privacy and confidentiality in cryptographic communication [3].

Partial encryption proposed a solution, in which a secure encryption algorithm is used to encrypt only part of the compressed data [4]. Computationally effect techniques for confidential storage and transmission of medical image data discuss [5].

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Chaos and Cryptography [6].

Chaos is one of the possible behaviors associated with evolution of a nonlinear dynamic system and occurs for specific values of system parameters. The chaotic behavior is a delicate behavior of a nonlinear system, which apparently looks random.

Chaos is an apparent fact that occurs in nonlinear definable systems sensitive to initial conditions and has pseudo-random action. Dynamic chaotic systems in case of Liapunov exponential equations meet will remain stable in chaos mode. It is the pseudo-random behavior that has caused this observable fact to take into account for many cryptographic systems. Due to pseudo-random character, the output of the vision system look like random in attackers' view, while in receiver's view, the system can be defined and decryption is possible. Several chaos based cryptographic algorithms are presented till now and some of them are somehow in use in the way that they are capable of image encryption as well as text encryption. An image encryption system must have suitable speed for image massive data ciphering. Text encryption methods are bad choice to be used for encryption of images. In practice, we require to transmit a sensible amount of information, which needs a large sample space and subsequently it implies a large amount of keys. The delivery of a large number of keys is responsible to cause awful management problems. So, one of the major advantages of chaotic system's comprehension is facilitated key management approach since this method only require to protect and secure transmission of secret key (parameters and initial values of chaotic system), which has a modest volume and as a result not only a small memory is desired to maintain it but also there is more assurance during its transfer. The illegal access to short length keys is notably less possible than the large length keys during data transmission through the insecure channel.

1. Logistic Map

Chaotic cryptography has been an important research area during the last two decades. The properties of chaotic systems have been used in very different ways to build new cryptosystems. All of those proposals can be classified into two big families, which are analog chaos-based cryptosystems and digital chaos-based cryptosystems [6]. Chaos in dynamical systems has been

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

investigated over a long period of time. With the advent of fast computers the numerical investigations on chaos have increased considerably over the last two decades and by now, a lot is known about chaotic systems. One of the simplest and most transparent systems exhibiting order to chaos transition is the logistic map. The logistic map is a discrete dynamical system defined by [7]. Logistic mapping is brought out by biologists R. May in 1976, and is a one-dimensional nonlinear iterative equation, the definition is as follows:

$$X_{n+1} = rX_n(1 - X_n) \quad n = 0,1,2, \dots, n \quad \dots\dots (1)$$

In this equation, X_n assumes a value in the interval $[0, 1]$. This signal, due to fact that the r parameter is divided into three different intervals, shows three different chaotic behaviors which, assuming that $X_0 = 0.3$, can be described as follows:

- 1- If $r \in [0, 3]$, then the signal behaves somewhat chaotically in the first 10 iterations and becomes stable after the tenth iteration [8] seeing Fig.1 (a).
- 2- If $r \in [3, 3.57]$, then the signal will behave somewhat chaotically in the first 20 iterations and, after the 20th iteration, varies between two stable values [8] seeing Fig. 1(b).
- 3- If $r \in [3.57, 4]$, then the behavior of the signal will generally be chaotic [8] seeing Fig. 1 (c).

Considering what has been said above, and because in this article a completely chaotic model is needed for hiding information , the chaotic signal Logistic Map with the initial values of $X_0 = 0.3$ and $r \in [3.57,4]$ is used[7].

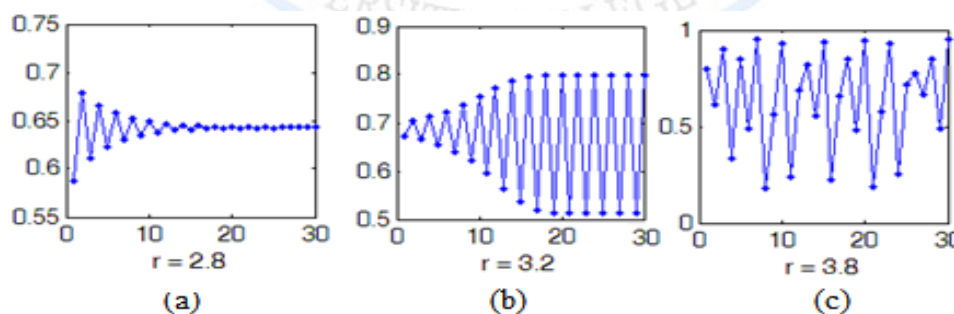


Figure (1): The chaotic behavior of the Logistic Map signal with $X_0= 0.3$. a) $r \in [0, 3]$, b) $r \in [3, 3.57]$, c) $r \in [3.57, 4]$

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Architecture of Logistic Text and Image Cryptosystem

A typical architecture of existing chaos-based text and image cryptosystems is shown in Figures (2). In this system will be generated key by logistic map and it is applied to text and digital color image encryption because of higher secrecy of high-dimension chaotic system. We divide the key to blocks; length of block is 24-bits such as each block apply on each pixel in plain image and text. The process of encryption and decryption consists of two levels, at first level will be using plain text or plain image and key generation then apply XOR operation to perform cipher text1 or cipher image1 (single level). The second step of the encryption process is to encrypt single level by apply feedback for single level to perform cipher text2 or cipher image2 (multilevel) that will be changing its pixel values based on dynamic chaotic systems. The decryption process applies the same steps as reverse steps.

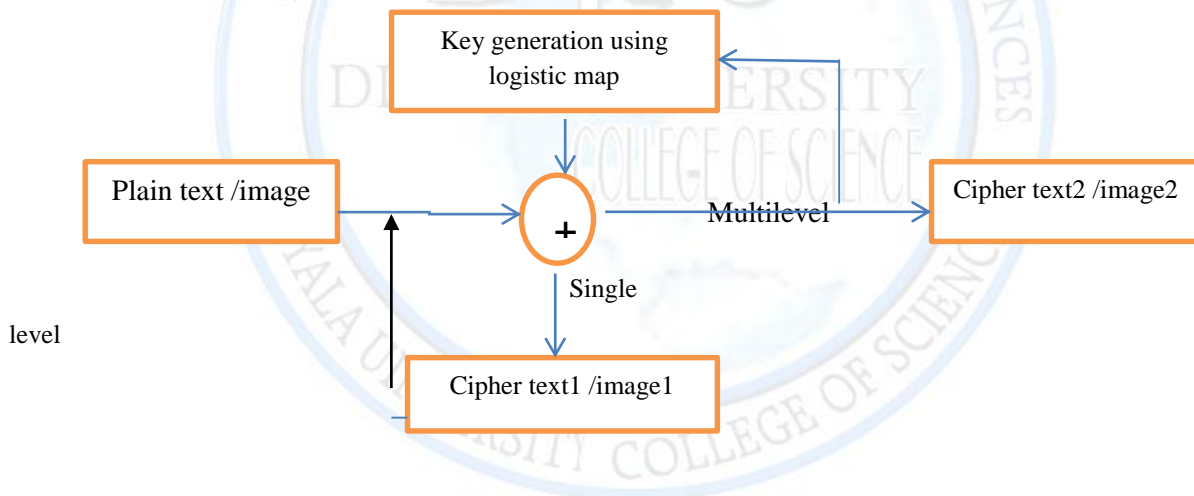


Figure (2): Typical Architecture of chaos- based text or image cryptosystem

The Proposed Algorithm

This paper is use the idea of logistic map to generate key by using equation (1) for encryption and decryption block of different massages and images using XOR operation. Algorithm (1) explains the steps of process and figure (3) show the key that generated by logistic map

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

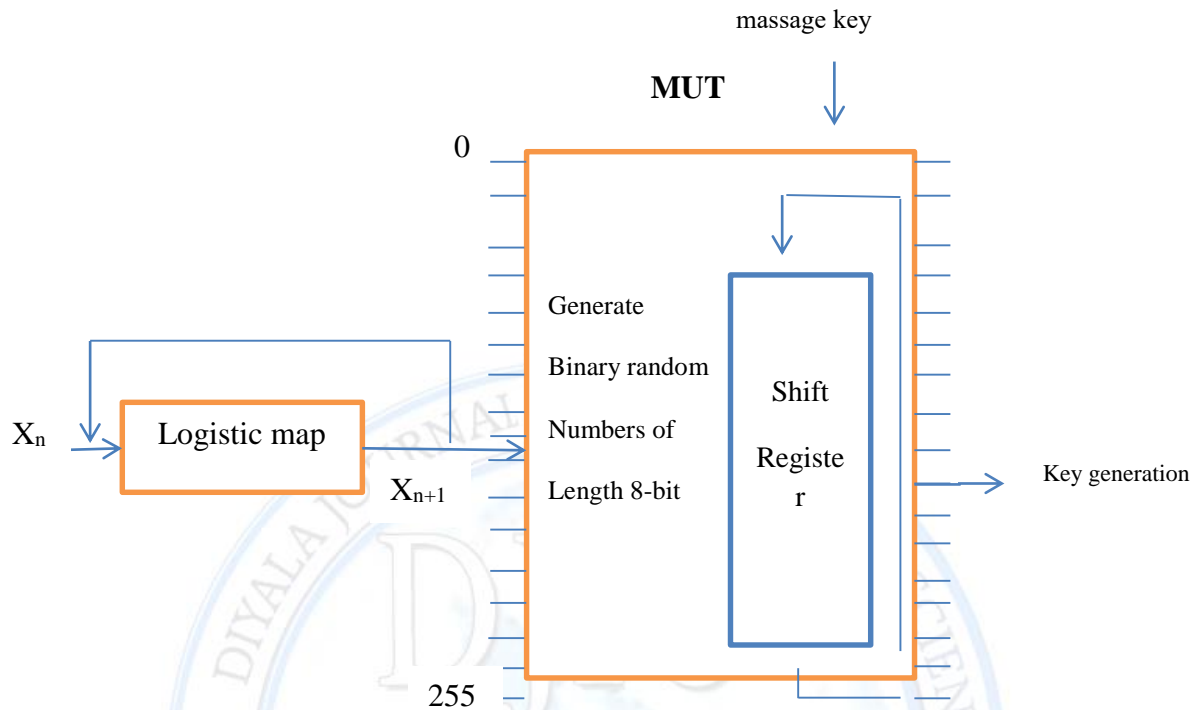


Figure (3): key that generated by logistic map

Using dynamic multiplexer and shift register during key generation to generate random numbers especially to multilevel and using message key as initial value between sender and reserve.

Algorithm (1): the proposed algorithm for multi cryptography

Input: text, an image, key generated by logistic map with parameters x, r and MUT.

Output: multi cipher text or cipher image.

- 1- Load plain text or plain image.
- 2- Enter key after generated as shown in below.
 - a- Using logistic map equation (1) to generate (255) random numbers and saving them in matrix S.

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

- b- Generate (255) binary random numbers, length of binary number is 8-bit and put them in a matrix B.
- c- Generate (255) random numbers between (0-1) using equation (2) and saving the numbers in matrix D.

$$\text{Random number} = (\text{loop from } 1 \text{ to } 255) | 255 \quad \dots\dots\dots (2)$$

- d- Compare each number generated by step(a) with all numbers generated by step(c), if it is equal or less than number that generated by step(c) we stop and will be take the binary number that contrast of step (b).
 - e- Apply XOR with last bit of generated number by step (d) with last binary number that generated by step (b) and shift the binary number by (1) using shift register with multiplexer.
- 3- Perform a bitwise XOR on plain text or plain image and key number that generated by step (2) to obtain cipher image1 (single level).
 - 4- Finally, repeat steps 2 and 3 to obtain cipher image2 (multilevel).

Results and Analysis

We have conducted some experiments to test check the encryption and decryption quality logistic map for application to text and digital images, which allow users to have confidentiality and security in transmission of the image and text. For apply those process, we use three messages of length (65) character and three images with format (.bmp) and it sizes (512*512) by applying the key that generated as above algorithm with different values of x and r using XOR operation. Table (1) shows the results of tests key with different length of the key.

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Table (1): Key Tests

Test Name	Key Length	Value Test	Result
Frequency test	800	213.21125	Pass
Serial Test	800	294.926298498122	Pass
Poker Test	800	52.4	Pass
Run test	800	11.1144424496815	Not Pass
Auto correlation	800	30.694	Not Pass
Frequency test	1000	170.569	Pass
Serial Test	1000	234.55084084084	Pass
Poker Test	1000	61.76	Pass
Run test	1000	22.0993845091088	Not Pass
Auto correlation	1000	45.940	Not Pass

1. Multi cipher and decipher

Below plain text and cipher text after apply secret key when $x=0.3$ and $r=1$ for single cipher and $x=0.7$ and $r=1$ for multilevel cipher. Table (2) show IC results of multi cipher and decipher text.

a- Stream Cipher program: this program using ABC method for encrypt.

Plain text

rjE•-z]eë—————óS7/çUD')|.Üì-□Lĩ-š' |yòÚ— ÜP'j•À±Bî-

Single level cipher text

q€ na ajhswoh xenpf pke oldno| spy }yna€ ww ~rerl ve|dni

Multilevel cipher text

b- The program for cipher text and image by using abc algorithm is excellent.

Plain text

qfq zgavira lp{ p}jagz dqdt qma bdra} jr fack□ frt cpiha |bbg a • esne□egy

Single level cipher text

te • upstdi ciz ec • xvy qiqb bfj • jagu fi uypdh qua qdcorbsm€ hr uhcakeael

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Multilevel cipher text

c- Computer department is a branch of science collage in university.

Plain text

2^δYÁ~f-'rš¥#KÙÑ•%B‡A—————J^wÁÔ%ú CEÍ p e[«•X{5PÍ,,Ò~%o

Single level cipher text

.š2mrŽ ° ÀÖ¶Pu†Ë • ÎãOÁEö~;âFC" -hÒ6Š“ó,,Ë\$KÎÂêËÚËŠFØÉ • ° ,c:

Multilevel cipher text

Table (2): IC of Multi Cipher and decipher text

No. of message	IC for plain Text	IC for Cipher Text1	IC for Cipher Text2
a	0.03697479	0.02689076	0.03381642
b	0.04915254	0.03446328	0.03224044
c	0.03647465	0.02394775	0.03233014


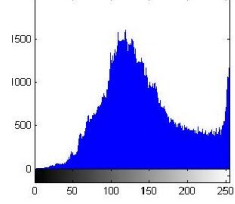

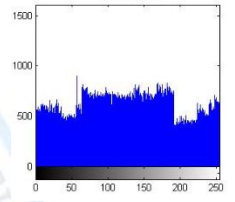
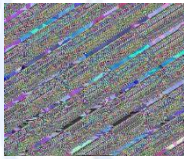
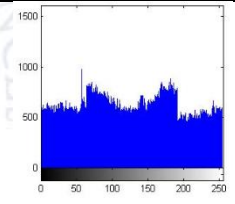

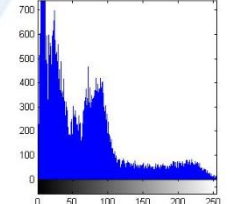
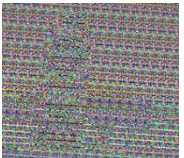
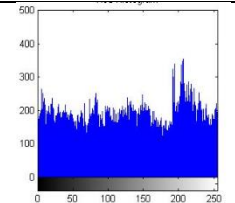
2. Multi image encryption and decryption

For multi-image encryption and decryption we apply secret key when $x= 0.3$ and $r=1$ for single level and $x=0.7$ and $r=1$ for multilevel , the results of correlation, entropy and histogram of them shown in table (3) .

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

Table (3): Multi image encryption and decryption

	Image	Correlation		Entropy	Histogram
		Horizontal	Vertical		
Image1		0.98582647	0.98836771	7.56418843	
Single image1		0.65252078	0.62954131	7.97661042	
Multilevel image 1		0.64639097	0.64999756	7.98307040	
Image2		0.95580514	0.95965978	6.84149806	
Single image2		0.62679821	0.62582916	7.976743366	

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali

Taha Mohammed Hasan

Ebtisam K. Abdulah

Ismael Salih Aref

Multilevel image 2		0.62444662	0.68624267	7.9718812	
Image3		0.95137593	0.91415032	7.3003151	
Single image3		0.62497300	0.95137593	7.982077553	
Multilevel image 3		0.61481652	0.57317908	7.976869068	

3. IC Test for text

The index of coincidence is a number that can help cryptanalysts guess the cryptographic system in use in a cipher text [8]. In [cryptography](#), coincidence counting is the technique (invented by [William F. Friedman](#)) of putting two texts side-by-side and counting the number of times that identical letters appear in the same position in both texts. This count, either as a

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

ratio of the total or normalized by dividing by the expected count for a random source model, is known as the index of coincidence, or IC for short .We can express the index of coincidence **IC** for a given letter-frequency distribution as a summation as shown in equation (2):

$$IC = \frac{\sum_{i=1}^c n_i(n_i-1)}{N(N-1)/c} \quad \dots\dots (2)$$

Where N is the length of the text and n_1 through n_c are the frequencies (as integers) of the c letters of the alphabet ($c = 26$ for mono case English). The sum of the n_i is necessarily N . The products $n(n-1)$ count the number of [combinations](#) of n elements taken two at a time. (Actually this counts each pair twice; the extra factors of 2 occur in both numerator and denominator of the formula and thus cancel out.) Each of the n_i occurrences of the i -th letter matches each of the remaining n_i-1 occurrences of the same letter. There are a total of $N(N-1)$ letter pairs in the entire text, and $1/c$ is the probability of a match for each pair[8].

4. Correlation Test

The correlation coefficient analysis indicates the relationship among pixels in the cipher image and determines the degree to which two variable's movements are associated. The correlation coefficient will vary from -1 to +1. A -1 indicates perfect negative correlation, and +1 indicates perfect positive correlation, a correlation of zero indicates that there is no linear relationship between the variables [9]. Equation is used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations. Where x and y are intensity values of two neighboring pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation [12].

$$r = \frac{\sum_{i=1}^n (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^n (X_i - \bar{X})^2} \sqrt{\sum_{i=1}^n (Y_i - \bar{Y})^2}} \quad \dots\dots (3)$$

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

5. Information Entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon (Stinson, 1995). Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics [7]. Entropy (more specifically, Shannon entropy) is the [expected value](#) (average) of the information contained in each message received. 'Messages' don't have to be text; in this context a 'message' is simply any flow of information. The entropy of the message is its amount of uncertainty; it increases when the message is closer to random, and decreases when it is less random [10]. To calculate the entropy $H(m)$ of a source m , we have:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad \text{bits,} \quad \dots \dots (4)$$

Where $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Suppose that the source emits 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, \dots, m_{2^8}\}$. After evaluating Eq. 4, we obtain its entropy $H(m) = 8$, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8, certain degree of predictability, which threatens its security [14]. We apply the entropy on cipher image encryption using the logistic map. The information entropy obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against entropy attack.

Conclusion

The paper designs a new secure random number generator based on the logistic maps. The proposed generator is a secure random number generator from the cryptographic point to view. A key stream generator should have the following important properties:

- 1- Output key features very high repeat.
- 2- Pass the statistical tests.
- 3- The generator has high linear complexity.

**Fast Dynamic Random Numbers Generator and Applications in
Cryptosystems (FDRNG)**

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

- 4- The randomness, the security, and the speed of the binary sequences generated by the random number generator are satisfactory.
- 5- When the key was used in texts and images encryption with good results after testing.

References

1. T.-J. Chuang and J.-C. Lin. "New Approach to Image Encryption", J. Electronic Imaging . Vol. 7, No. 2, PP. 350-356, 1998.
2. Y.Moa. G.Chen. and S.Lian. "A novel Fast Image Encryption Scheme based on 3 d Chaotic Baler Waps". International Journal of Bifurcation and Chaos, val.14, no. 10, PP. 3613-3624, 2004.
3. Zenon, H., Voloshynovskiy, S., Rytsar, Y. "Cryptography and Steganography of Video Information in Modern Communication", in Third TELSIS'97, Yugoslavia, pp. 115-125 , 1997.
4. [H. Cheng](#) ; [Xiaobo Li](#) "Partial encryption of compressed images and videos" , [IEEE Transactions on Signal Processing](#) (Volume:48 , [Issue: 8](#)), **Page(s):** 2439 – 2451 , 06 August 2002.
5. Norcen, R., Podesser, M., Pommer, A., Schmidt, H., Uhl, A., 2003. "Confidential Storage and Transmission of Medical Image Data". Computers in Biology and Medicine 33, 277–292.
6. David Arroyo¹, Gonzalo Alvarez¹, and Veronica Fernandez¹, " On the inadequacy of the logistic map for cryptographic applications", ACTAS DE LA X RECSI, SALAMANCA, 2008 ARROYO *et al.*: ON THE INADEQUACY OF THE LOGISTIC MAP ... 77.
7. [https://en.wikipedia.org/wiki/Entropy_\(information_theory\)](https://en.wikipedia.org/wiki/Entropy_(information_theory))
8. R. Hagnazar Koochaksaraei, V. Aghazarian, A. Haroonabadi, and A. Hedayati, "A Novel Data Hiding Method by Using Chaotic Map and Histogram ". International Journal of Innovation, Management and Technology, Vol. 3, No. 5, October 2012.

Fast Dynamic Random Numbers Generator and Applications in Cryptosystems (FDRNG)

Rajaa Ahmed Ali Taha Mohammed Hasan Ebtisam K. Abdulah Ismael Salih Aref

9. Alireza Jolfaei and Abdolrasoul Mirghadri, “**Image Encryption Using Chaos and Block Cipher**”. Faculty and Research Center of Communication and Information Technology, *ISSN 1913-8989 E-ISSN 1913-8997*, Vol. 4, No. 1; January 2011.
10. <http://www.thonky.com/kryptos/index-of-coincidence>
11. https://en.wikipedia.org/wiki/Index_of_coincidence
12. <http://www.investopedia.com/terms/c/correlationcoefficient.asp#ixzz3ljRx70iu>
13. Rajinder Kaur and Er. Kanwalpreet Singh,” **Comparative Analysis and Implementation of Image Encryption Algorithms**”. International Journal of Computer Science and Mobile Computing . A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IJCSMC, Vol. 2, Issue. 4, April 2013, pg.170 – 176 RESEARCH ARTICLE.
14. S. C. Phataka and S. Suresh Raob, “**Logistic Map: A Possible Random NumberGenerator**”. Institute of Physics, Bhubaneswar-751005, India, IP/BBSR/93-52.
15. <http://searchsecurity.techtarget.com/definition/encryption>