iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8258

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Light Weight Ciphers Primarily Based on Chaotic Map – LFSR Architectures

Suvarna S. Patil[1], Swapna[2]
[1]*Assistant Professor,* [2]*M. Tech Student*
Department of Electronics and Communication Engineering Rao Bahadur Y Mahabaleswarappa Engineering College, Ballari

Abstract: ***In this paper, we propose and analyze two different stream ciphers based on a Skew Tent Map and a Modified Logistic Map respectively. In order to improve the randomness of these systems, a single method for increasing the periodic length of the generated sequence has been applied. The results prove that the randomness of these systems can be severally increased by using this method, making these systems suitable for secure communications.***
Keywords: Secure communications; chaotic maps; logistic map; Skew tent map; Modified logistic map

I. INTRODUCTION

In the recent years it has become necessary to encrypt high amounts of data (Video) in real time for different applications. Usually, block ciphers or stream ciphers are used for private data encryption due to their high speed and low complexity. In cryptosystems Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. The chaos-based cryptosystems have an alternative to classical encryption since they could be able to achieve a good balance between speed and security. Most of these cryptosystems are based on one dimensional chaotic maps since they are the simplest systems that present a chaotic behavior. Specially, the logistic map has been used in many of the proposed cryptosystems due to its simplicity, high throughput and ergodic properties. Two different stream ciphers based on a Skew Tent Map and a Modified Logistic Map are proposed respectively. In order to improve the randomness of these systems, a single method for increasing the period length of the generated sequences has been applied. The results prove that the randomness of these systems can be severally increased by using this method, making these systems suitable for secure communications. Ciphers are a secret way of writing code. Linear feedback shift register is system which generates the output in form of sequence of bits. This paper incorporates the LFSR with skew tent map and Modified logistics map using encryption algorithms.

II. METHODOLOGY

The process of encryption is shown in below figure, first the sender sends a normal message that is human readable ie(plain text), this plain text is been converted into cipher text by using encryption algorithm. In encryption algorithm the plain text is been converted into Cipher text. Cipher text is the secret way writing code. The encryption key or key space is the one which holds the data in it, that data may be plain text, some additional bits are added to the key space so that it can be secure and hacker cannot hack the data ,if the encryption key is strong, hence encryption process is done,by converting plane text into cipher text .This cipher text is been decoded to get back the original plain text, during decoding the key space of both encryption and decryption shoud be of same length ,in case if the key space differs the original message cannot be retrived.

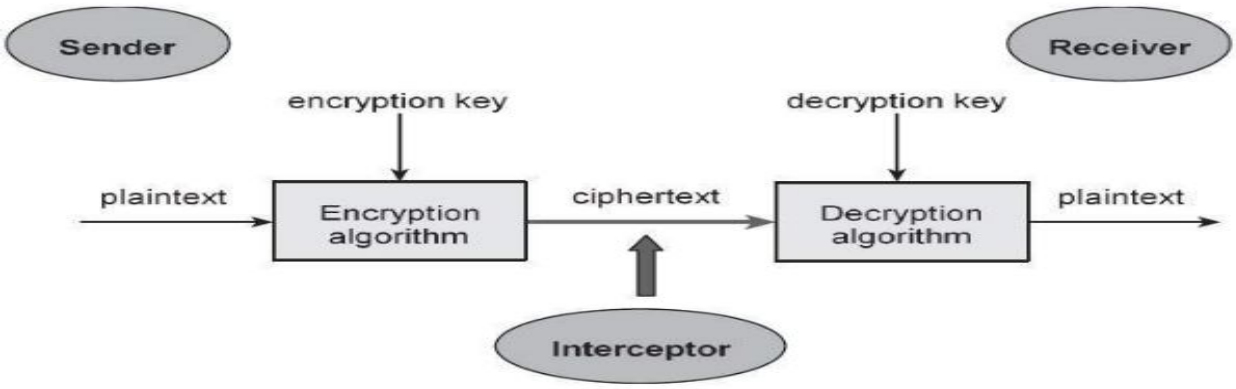


Fig.1 Process of encryption

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

III. EXISTING METHOD

There are two methods, which were used earlier for transmission of data namely Block ciphers and Stream ciphers. In Block ciphers the data transmission is done by sending a cunch or block of data(plain text) at a single transmission, hence transmission is done here by using key space and plain text is been converted into cipher text.In Stream ciphers the pain text is converted to cipher text by allowing bit by bit data transfer sequentially. The entire information may not been conveyed at once, eventually bit of information is been encrypted as stream ciphers.

Disadvantage of Stream and Block ciphers

Lack of security, Data is not transferred securely, Time consumption, in stream ciphers.

IV. PROPOSED SYSTEM

We propose and analyse two different tent maps namely skew tent map and modified logostic logistic map. These maps transfer data without any loss and mainly secure data transmission is done.

The fig.4. shows the 32-bit STM/MLM logistic map generator, at the input side either stm/mlm can be used, one bit is given from input side to the adder ,this bits are given here for key space ,from LFSR (linear frequency shift register)one more bit is added to the adder, here the shifting operation is done in 32bit format .These input bits are again added to next adder,where plain text(original message)is given and output is produced.

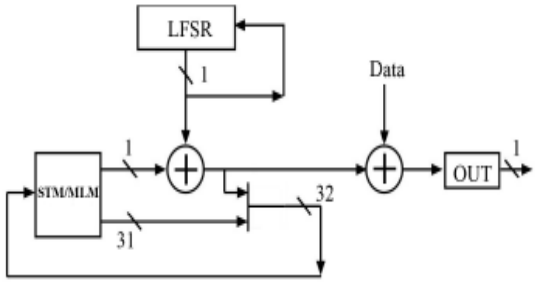


Fig.2 Skew /Modified Logistic map generator

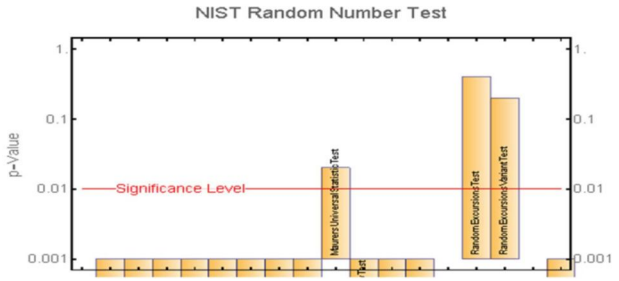


Fig.3 NIST tests occurs for a system made using only the STM

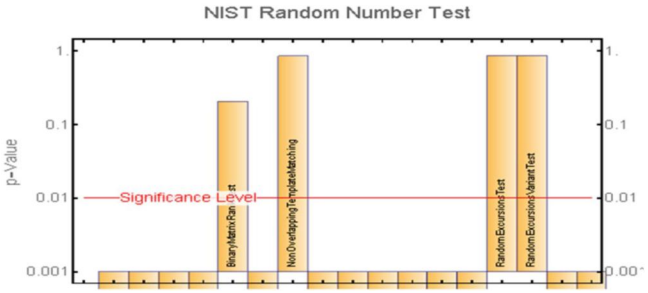


Fig.4 NIST tests occurs for a development made using only the MLM.

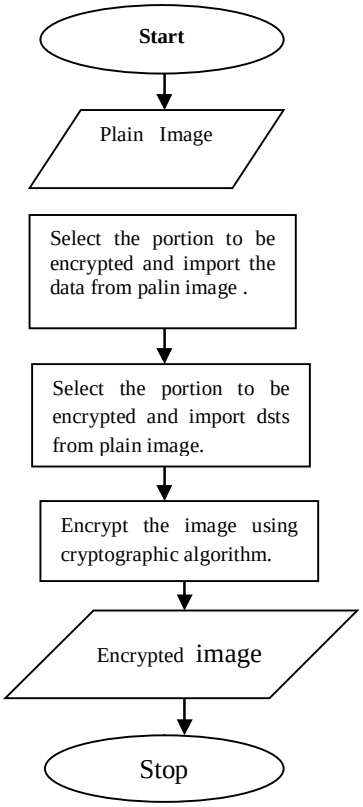
To analyse the security of these algorithms ,several sequences have been encrypted and subjected to NIST(National Institute of Standards and Technology).The sequences have been tested which have been generated by STM and MLM to verify our applications. Here the key size must be increased in order to prevent from Brute-force attack.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

V. FLOW CHART AND ENCRYPTION ANALYSIS

The flow chart diagram of encryption process explain ,how the image is been encrypted Firstly the plain image is been taken as input that is to be encrypted .In this encryption the whole image need not to be encrypted .we select the particular portion of image for encryption because of the security crisis ,by doing this the hackers cannot predict the original image it is difficult to encrypt the particular portion of image. Now the selected portion of image is been encrypted using cryptographic algorithms ,that is by using symmetric and asymmetric keys and private and public key structures .the periodic length of both the encryption and decryption should be strong enough so that the data loss shouldn't be a problem during encryption. The main aim of this process is high-security, by maintaining the periodic length in random it can be achieved, if the periodic length varies the process becomes unpredictable and complex. By maintaining proper periodic length and periodic window cryptography is achieved. By using encryption algorithms the image is been encrypted into particular RGB standards , this image format is been encrypted and the results are been in format of graphs. These are been represented in graphs to overcome the security attacks. The image in graph of RGB can only be understood by experts in cryptography .

.



VI. RESULTS AND DISCUSSION

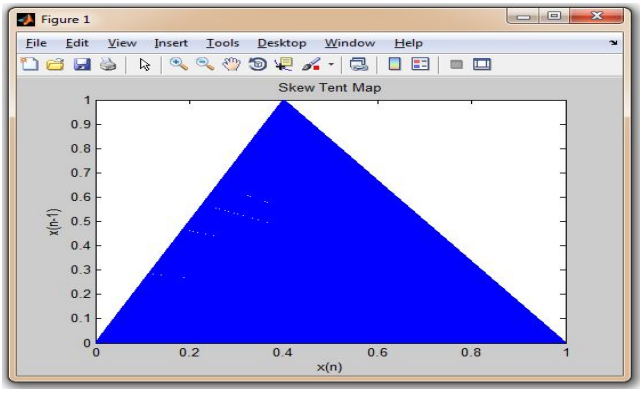


Fig.6 Skew Tent Map

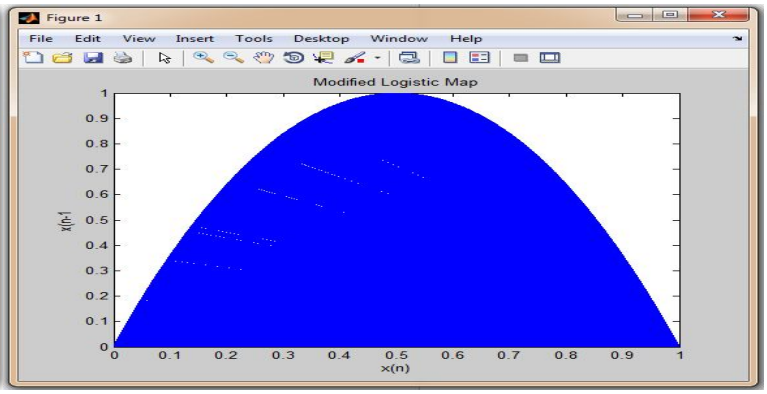


Fig .7. Modified Logistic Map

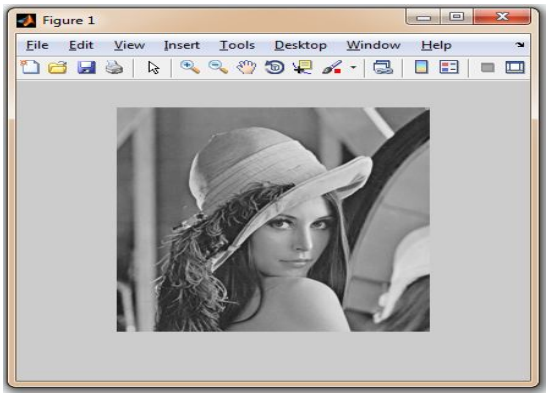


Fig.8 Image before Encryption

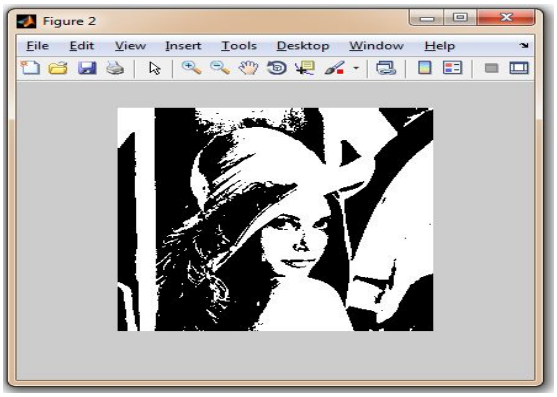


Fig.9 Image after Encryption

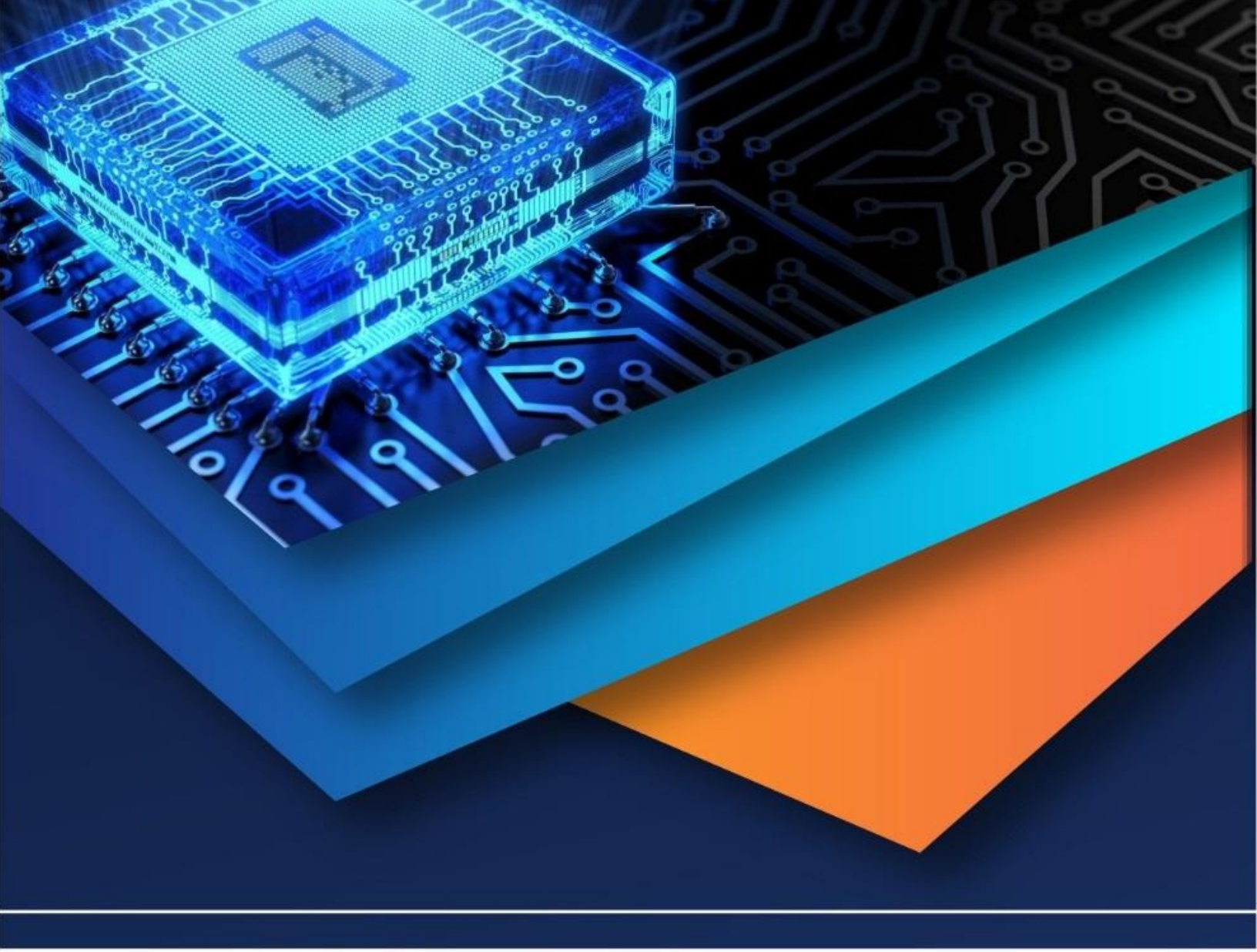
The skew tent and modified logistic maps are shown in fig 9.1 and 9.2 ,the tent map is based on γ **=0.04** value which is constant in skew tent map, if the value changes the skew tent map cannot be predicatble, it becomes more complex and data losses may occur .The binary sequence are also been generated by both skew and modified logistic map .The modified logostic map has been seen in log structure, and has some constant value, the log map is more advanced compared to skew map. Binary sequence are generated by using gray scaling in matlab software. From fig 9.3 system model shows how the image is been encrypted using black and white pixels. The input image is been given in system model that is to be encrypted using cryptanalysis mainataing constant periodic length and periodic window. The system mainly requires the high security for encryption so that the proper data can be regained .The process of encrypting images is shown in above and below figures.

VII. CONCLUSION

Two different stream ciphers have been proposed and analysed. Both of them have passed the NIST(National Institue of Standard Test) tests, providing the good randomness of the generated sequences. Furthermore a Cryptanalysis has been presented to prove that these systems are secure. However both Cryptosystems are similar, there are some differences that are worth noticing order to choose between them. Both systems could be suitable for applications that require both speed and security .However, it is difficult to determine which algorithm is better. In order to choose between them, the applications and the platform where it is going to be implemented should be considered.

REFERENCES

[1] J. Shah and V. Saxena, “Video Encryption: A Survey,” International Journal of Computer Science Issues, vol. 8, no. 2, pp. 525-534, March 2011.
[2] R. Hasimoto-Beltran, “High-performance multimedia encryption based on chaos,” Chaos: Interdisciplinary J. Nonlinear Sci., vol. 18, no. 2, pp. 023110-1 - 023110-8, 2008
[3] A. Baranovsky, and D. Daems, “Design of One-Dimensional Chaotic Maps with Prescribed Statistical Properties,” International Journal of Bifurcation and Chaos, vol. 5, no. 6, pp. 1585-1598, 1995.
[4] S.L. Chen, S.M. Chang, W.W. Lin, and T.Hwang, “Digital secure communication using robust hyper-chaotic systems,” International Journal of Bifurcation and Chaos, vol. 18, no. 11, pp. 3325-3339, 2008.
[5] L. Kocarev, and S. Lian, “Chaos-based cryptography”, Springer, 2009.
[6] NIST Special Publication 800-22 Rev.1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications (April 2010).
[7] ENISA, “Algorithms, key size and parameters report”, November 2014. <https://www.enisa.europa.eu/activities/identity-andtrust/ library/deliverables/algorithms-key-size-and-parameters-report- 2014>



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY