A REVIEW PAPER ABOUT “IMAGE ENCRYPTION USING TWO DIMENSIONAL MODIFIED SINE LOGISTIC MAP”

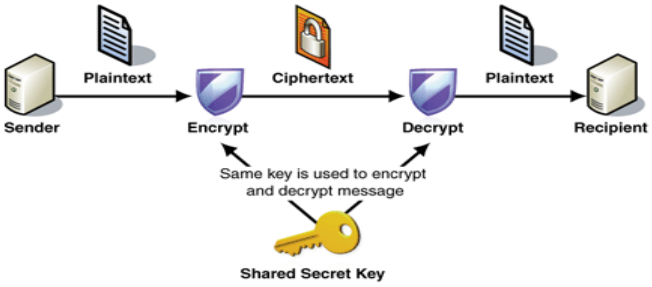
Ridwan Uz Zaman Pandit[1], Priyanka Mehta[2]
[1]Research Scholar, M.Tech (CSE), [2]Assistant Professor
Department of Computer Science and Engineering
Universal Institute of Engineering and Technology, Lalru, Chandigrah.

ABSTRACT: Advancement in the internet technology is enhancing day by day. The most dynamic field is the networking through which we can play different types of roles like multimedia technology, communication etc. The communication plays very important role in our day to day life. One of the most important topic in computer Networking is the Encryption of data, images and videos. Encryption means to convert the data or information in a secret form i.e. the information should be hidden from the third party. There are different types of techniques like DES,RSA and AES. These types of the techniques are not permissible in case of the encryption of images, having intrinsic property. Once the data or image is encrypted at one end is decrypted at the other end in order to obtain the original information. The decryption process is the reverse process of the encryption.. Cryptography and Steganography are the main two approaches that are used to undertake security issues. In case of cryptography data is piled up and sent in a specific form such that only specific user can understand it and process it. It does not hide the existence of data. But in case of Steganography, data is hidden in such a way that only authorized users have the knowledge of the existence of the data. In this research paper , using an algorithm known by coupled-map lattices and fractional-order chaotic system is proposed to increase the robustness and security of the encryption algorithms having permutation-diffusion structure. Chaotic maps are widely used in the application of security. Chaotic has excellent property of Unpredictability, ergodicity and sensitivity to their parameters and initial values. In this proposed work we introduce a new two-dimensional Sine modified Logistic modulation map, which is derived from the Logistic, and Sine maps. Compared with existing chaotic maps, it has the wider chaotic range, better ergodicity, and hyper chaotic property.

Keywords: Image cipher, chaotic cryptography, Logistic map, data encryption.

I. INTRODUCTION

Network security plays an important role during the encryption and decryption of data. When confidential data is transferred between two or more devices, security of information plays an important role. Cryptography and stenography plays an important role in network security in order to hide the information while transferring the data between two specific users. The data is piled and sent it in a specific manner so that only a particular user can understand it and process it during the cryptography. As, in case of the stenography, data is hidden in such a way only the authentic user have the acknowledgment of the particular data.. The result of encryption were used to substitute the phrased in addition to the alphabets in the nomenclature cipher. It is also known as cipher Mary. The modern cryptography focuses on developing the cryptographic algorithms that are hard to break by any adversary due to the computational hardness therefore could not be broken by a practical means. In modern cryptography, there are three types of cryptographic algorithms used called Symmetric key cryptography, public key cryptography and the hash functions. Symmetric key cryptography involves the encryption methods where both the sender and the receiver share the same key used to encrypt the data. In public key cryptography, two different but mathematically related keys are used. Hash functions does notuse key, instead they compute a fixed length hash value from the data. It is impossible to recover the length or the original plain text from this hash value. The modern stenography methods are called Digital stenography. These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the messages within video files, etc. Furthermore, network stenography is used in telecommunication networks. This includes technique like stenography(hiding a message in voice –over-IP conversations)and WLAN stenography(methods for transmitting stenograms in WIRELESS LOCAL AREA NETWORKS). The following figure shows the simplest form of encryption and decryption.



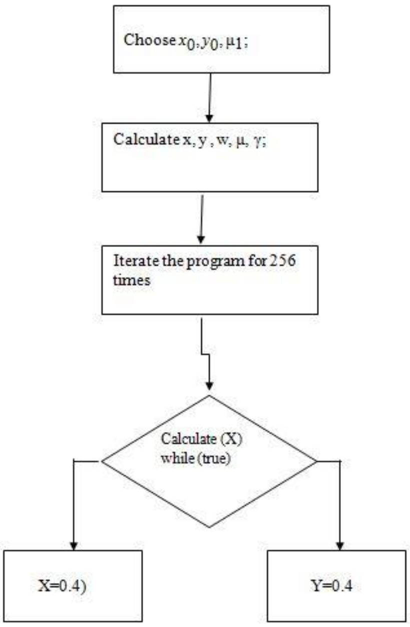
II. LITERATURE REVIEW

Due to enlargement of information and communication technology, the numerous applications have been increased in every aspects of daily routine as well in society. These applications have attractive features and easily understandable [1].Therefore numerous research groups are working in this domain because security of images is very important. Sensitivity and randomness fulfil the need for a better cryptographic system. Both randomness and sensitivity concern is better improved by the chaotic based encryption techniques. As chaotic based encryption technique firstly come into the effect in 1989 by Matthews. But randomness and sensitivity is still a big issue.Several research groups have made the significant contribution in the recent years to tackle these issues. Researchers introduced the complex chen system, complex Lorentz system[8],chaotic Logistic map, diffusion, permutation, XOR, three dimensional cat map system[9],fusion of maps[11] and some ancient algorithm. Xu, Li and Hua developed a technique using a bit level chaotic maps[1],Zhou et.al developed an image encryption technique using fusion of chaos and Line map [2],Zhang et.al developed encryption method using secret key for color images [3].

- Wang et.al (2007) developed an image encryption technique using two complex Chen systems. Each having advantages as well as drawbacks in this combined approach key space are not much larger than multidimensional.. Wang et.al introduced encryption algorithm based on exchange of pixels. It reduces the correlation that is good idea to resist the attacks [1].
- Leo Yu Zhang et.al, (2009)discussed about the chaotic image encryption. The per-mutation and diffusion structure is employed by the several round-based chaotic image encryption techniques. It becomes unconfidently when the value of iteration round is one and in this case it can be easily recovered. . Unambiguously, for the development of the several permutation sequences for several plain images firstly plaintext feedback technique is embedded in the permutation process after that secret key generated dynamically by employing plaintext or cipher text feedback for diffusion. This approach possesses large key space and it can repel the differential attack [2].
- Jun-xin Chen et.al, (2013)discussed the demand of real time secure image encryption i.e. chaos based image encryption.. Mostly are related to the architecture based upon permutation diffusion.But it contains two weaknesses i.e. according to first one, to encrypt one plain pixel at least two variables based on chaotic state are required in permutation as well as diffusion process. Chen further discussed how to tackle with this weakness with the help of a fast chaos based image encryption technique using a dynamic state variable mechanism to enhance security as well as efficiency [5].

III. PROPOSED ALGORITHM

In the proposed encryption algorithm we have used 232-bit secret key that is enough to fulfill the criteria of key space. Inspite of having larger key space, secret key must be very sensitive in both encryption and decryption process. It means that if we change even a single bit of secret key then ciphered image be totally different from the ciphered image generated from the correct key and decrypted image. With the help of chosen plaintext attack to encrypt the image and attacker analyse the cipher image or on the other hand with the help of ciphertext attack, attacker retrieve the original image. Finally attacker can easily find a relation between ciphertext and plaintext or even attacker can retrieve the secret key key if it is not secure enough. In modified sine logistic map specific structure is defined to resist the chosen plaintext and ciphertext attack.


Choose $x_0, y_0, \mu1$;
Calculate x, y , w, µ, γ;
Iterate the program for 256 times
Calculate (X) while (true)
X=0.4)
Y=0.4

Flow diagram to generate key

Algorithm 1 The generation of initial states for two-dimensional modified sine logistic map.
Input: Secret key K = 232 bits.
Output: Initial states (x_0, y_0, μ_1) and (x_0, y_0, μ_2).

1.$x=(^{52}\ K[i]\times2^{i-1})/2^{52}$; for i=1:52
In this step we are generating the value of key x. K is an array. It is iterated 1-52 times and finally we are getting value of x.

2. $y=(^{104}\ K[i]\times2^{i-53})/2^{52}$; for i=53:104
In this step we are generating the value of key y. K is an array. It is iterated 53-104 times and finally we are getting value of y.

3. $\mu=(^{156}\ K[i]\times2^{i-105})/2^{52}$; for i=105:156
In this step we are generating the value of key µ. K is an array. It is iterated 105-156 times and finally we are getting value of µ.

4. $w=(^{208}\ K[i]\times2^{i-157})/2^{52}$; for i=157:208
In this step we are generating the value of key *w*. K is an array. It is iterated 157-208 times and finally we are getting value of w.

5. $\gamma1 = {}^{220}\ K[i]\times2^{i-209}$; for i=209:220
In this step we are generating the value of key γ1. K is an array. It is iterated 208-220 times and finally we are getting value of γ1.

6. $\gamma2 = {}^{232}\ K[i]\times2^{i-221}$; for i=221:232
In this step we are generating the value of key γ2. K is an array. It is iterated 208-220 times and finally we are getting value of γ2.
7. for$i$=1to2do

In this step loop is iterated for two times.

8. x^i_0=(x_0+w×γ_i)mod1;

In this step further value of x0 is calculated using (x_0+w×γ_i) and mod is taken.

9. y^i_0=(y_0+w×γ_i)mod1;

In this step further value of y0 is calculated using (y_0+w×γ_i) and mod is taken.

10. μ_i= ((μ+w×γ_i) mod 0.4)+0.5;

In this step further value of $\mu_i$is calculated using ((μ+w×γ_i) mod 0.4)+0.5; and mod is taken after adding 0.5.

11. ifx^i_0=0then

if the calculated value is zero then the value is taken as 0.4.

12. x^i_0= 0 . 4 ;

13.end if

14. ify^i_0=0then

if the calculated value is zero then the value is taken as 0.4.

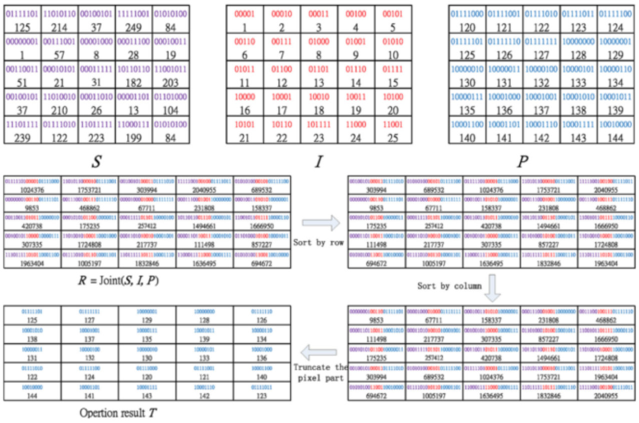
15. y^i_0= 0 . 4 ;

16. end if

17. end for

Finally this algorithm is completed.

As shown in the figure 4.2 pixel positions of the image are shuffled according to matrix generated by modified sine logistic map. As we can see that Sis the chaotic matrix generated by two-dimensional sine logistic.I is the index matrix that is generated by the pixels in matrix P. I is represented in the same way as in P. The binary values in the matrix S are replaced by the Most significant bit position. In confusion Process, pixel can be permuted at any position. It can be seen that shuffling of pixel after one time. R is the joint matrix of S, P and I. Then this matrix R is sorted by column. After that pixel is truncated and we finally get the result.



IV. OBJECTIVE / METHODOLOGY

The work presented in this report is focused on the logistic map based security techniques. The goal is to provide the effectiveness in terms of key and attacks. The whole work addresses the following key attributes:

To Survey the related research paper to identify the problem.

- To evaluating the performance in the case of image encryption and to explore the advantage and disadvantage in comparison to the existed approaches, providing the effective solution.
- To design and simulate the environment for the image encryption technique.
- To validate the results through Matlab.

Research methodology is the process to solve the research problem systematically. It is a science of studying how research is done scientifically. In this study the process defines the various steps that are generally adopted by a researcher in studying his/her research problem along with the logic behind them. The image Encryption in the logistic map is devoted to the design and development of Hybrid framework to Measure Quality and Risk score of component and select the best component from component repository by comparing the components on the basis of calculated risk score. Following Image methodology is used for achieving the objectives.

Proposed image methodology, which will be considered and followed step by step during the image Encryption and Decryption:

- Literature Survey: According Literature Survey to figure, first of all we did the literature survey an Image Encryption or Decryption processes.
- Cryptographic Algorithm: We studied different approaches and then find the research problem.
- MATLAB and Result outcomes: After that we firstly developed the algorithm for the existed technique.
- Result Analysis and comparison: After that we enhanced the cryptographic algorithm and implemented it into the matlab.
- Documentation: After that we compare the result generated by our algorithm with existing approach and reach the conclusion that proposed approach is better. Finally we did the documentation of the research work.

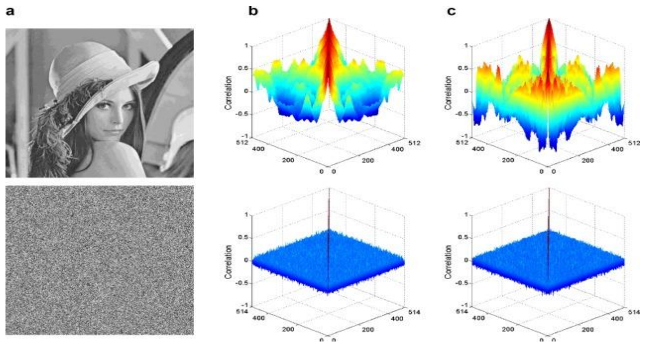
Modified two dimensional Sine Logistic Sine map

Mathematically two dimensional modified logistic sine maps is defined as below

xi+1= sin(π α(yi+xi + β)xi(1 − xi)),

yi+1=sin(πα(xi+1+yi+β)yi(1−yi))

Here the value of α is within the range of [0, 1] and value of β is fixed as 3. This modified two dimensional logistic map is formed using Sine and Logistic maps. Logistic equation is scaled by using α and then output is given to the input of sine logistic map. Modified two dimensional sine logistic map has more complicated output in comparison to the logistic map and sine map.



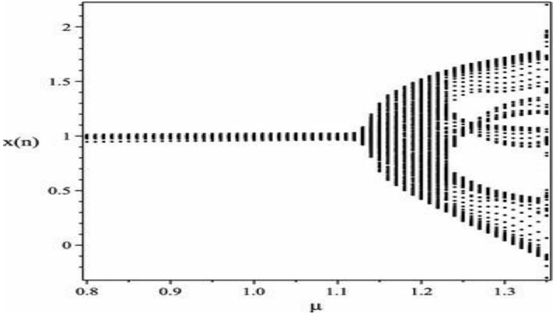
V. PROBLEM OUTLINE

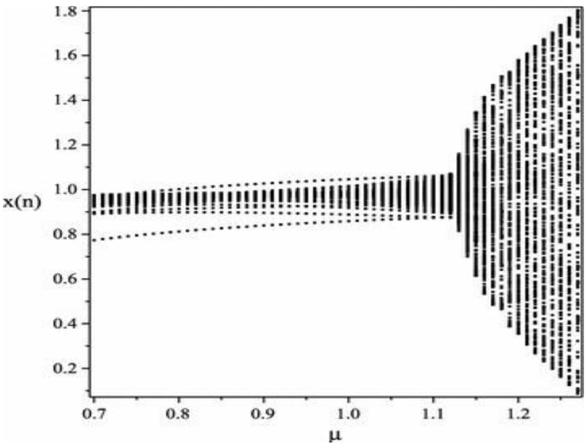
In recent years, a variety of chaos-based image cryptosystems have been proposed. An architecture of such kind of cryptosystems is composed of multiple rounds of substitution and diffusion. In the substitution stage, a two- or higher-dimensional chaotic map is employed to shuffle the image pixels for confusion purpose. In the diffusion process, the pixel values are altered sequentially so that the change made to a particular pixel depends on the accumulated effect of all the previous pixels. The design of this class of chaos-based image cryptosystems, together with the security evaluations

As we know that the cryptography helps us to dissolves the various problems, in order to perform the secure communication in between the network or two parties. Ciphers can dissolves the problem but not satisfactory. So the Sine and logistic map with combined approach helps us to provide the better result.Sine map and logistic with combined approach provide the better result because it increases more randomness because covered area is maximum in the hybrid approach.

VI. CONCLUSION

In the proposed work a new two-dimensional modified sine logistic map has been developed. It is developed with the help of logistic map and sine map. Then phase plane is extended from one dimension to two dimensions. Trajectory, Lyapunov exponent and Kolmogorov entropy were evaluated to prove the ergodity, extended chaotic range and unpredictability. Using two dimensional modified sine logistic maps, an image encryption technique is developed. It basically has three main steps i.e. addition of pixels, diffusion and confusion. The addition of pixels to the original image results into different ciphered image. Four times diffusion and confusion is applied to support the diffusion and confusion. Security analysis and simulation results proved that modified sine logistic map can encrypt several types of images into higher security level.





REFERENCES

[1] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn. 25 (1992) 567–581.

[2] Refregier, B Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.

[3] H.K.L. Chang, J.L. Liu, A linear quad tree compression scheme for image encryption, Signal Process. 10 (4) (1997) 279–290.

[4] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (6) (1998) 1259–1284.

[5] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (2) (1998) 318–325.

[6] J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999, pp. 430–437

[7] J.C. Yen, J.I. Guo, An efficient hierarchical chaotic image encryption algorithm and its VLSI realization, IEE Proc. Vis. Image Process. 147 (2000) 167–175.

[8] H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.

[9] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52

[10] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.

[11] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proceedings of the IEEE International. symposium on circuits and systems, Scottsdale, AZ, USA, 2002

[12] S. Li, X. Zheng, X. Mou, Y. Cai, Chaotic encryption scheme for real time digital video, Proceedings of the SPIE on electronic imaging, San Jose, CA, USA, 2002

[13] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, Chaos

Solitons Fractals 21 (2004) 749–761.

[14] N.K. Pareek, VinodPatidar, K.K. Sud, Discrete chaotic cryptography using external key, Phys. Lett. A 309 (2003) 75–82.

[15] N.K. Pareek, VinodPatidar, K.K. Sud, Cryptography using multiple one dimensional chaotic maps, Communication Nonlinear Sci. Numer. Simul. 10 (7) (2005) 715–723.