A Survey on Chaotic Image Encryption

Sneha P S
Department of Computer Science & Engineering
N.S.S. College of Engineering
Palakkad, Kerala, India
ahensofficial@gmail.com

Syam Sankar
Department of Computer Science & Engineering
N.S.S. College of Engineering
Palakkad, Kerala, India
syam.sankar8@gmail.com

Abstract — **The exchange of data over the internet and other mediums are rapidly increasing day by day. There is no security for those data which are transmitting. The data can be of any forms like text, image, audio, and video. The only way to keep the data unreachable to the irrelevant hands is to encrypt it. Most of the multimedia data in today's world contain images. Different encryption techniques were also used to conceal the original form of the images. AES, RSA, DES and so on were the encryption techniques used earlier. But on analysis, it shows a low resistance to different types of attacks and it was clear that the data can be lost. There arises a new idea of chaos in the field of cryptography which ensures more security and resistance towards attacks. The main reason why chaotic systems used in image encryption is that those parameters are very sensitive to the initial conditions. Several works have been done in the field of image encryption using chaos theory and in this survey paper, it is attempted to review some of the techniques and algorithms used for chaotic image encryption**

Keywords — **Image, cryptography, chaos, encryption, security**

I. INTRODUCTION

Data exchange is the very common way of communication and now there is no limit for the data which is shared and to whom it is shared. So there is a high risk of losing the confidentiality of sensitive information. There occurs chances of unauthorized access to the data which is shared over the electronic media like internet. That kind of breaches in security is one of the major issues to user's reputation and privacy. The data which is sharing may be of any kind like text, image, audio, video, etc… Each of these data has its own features and different methods are used to protect those data. Encryption is one of the main and better techniques used to encrypt those data especially image data. Cryptography is one of the major term to be discussed before encryption. Two inherent needs of human being from ages is to communicate and share information and also to communicate selectively. These needs give rise to an art of coding messages so that only the intended person could read it. Unauthorized person cannot do anything with those information even if it is available in their hands. So the science of concealing the message to introduce secrecy for it is known as cryptography. Two major subdivisions of cryptology are cryptography and cryptanalysis. Cryptography is the process of giving information more secrecy. The ciphertext is the encrypted or hidden version of original data and the original form is known as plain text. While talking about cryptanalysis, it is the process of breaking the ciphertext and finding out the original image. Confidentiality, Data integrity, authentication, Non-repudiation etc… are the main goals attained by cryptography. Main components of a cryptosystem are :

- **Plaintext**: Data to be protected during transmission.
- **Encryption algorithm**: The cryptographic algorithm which takes plaintext and key as input and produces ciphertext as output.
- **Ciphertext**: the Scrambled version of plaintext after applying the encryption algorithm.
- **Decryption algorithm**: the Cryptographic algorithm which takes ciphertext and decryption key as input and produces plaintext as output.
- **Encryption key**: Value known to the sender and which uses along with plaintext for encryption.
- **Decryption key**: Value known to the receiver and uses along with ciphertext for decryption.

Image encryption idea is to change an image into the 1-D data stream and encrypt that data using common cryptographic techniques. But it is not possible to encrypt images of all forms using this technique. There is no strict need that the decrypted image should be of same as the original image. Small distortions are allowed as the image size is high compared to the textual data.

II. CHAOS THEORY FOR CRYPTOGRAPHY

Chaos theory is the branch of mathematics focused on the behavior of dynamical systems which are highly sensitive to initial conditions. Chaos is an interdisciplinary theory which states that within the apparent randomness of chaotic complex systems, there are underlying patterns, constant feedback loops, repetition, self-similarity, fractals, self-organization, and reliance on programming at the initial point known as sensitive dependence on initial conditions. Small differences in initial conditions yield widely random outcomes for such dynamical systems. That response popularly referred to as the butterfly effect. This happens even though these systems are deterministic meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. This behavior is known as deterministic chaos, or simply chaos. The theory was summarized by Edward Lorenz [1]. So simply, chaos means: when the present determines the future, the approximate present does not approximately determine the future [2].

Chaos theory has been used for many years in cryptography. In the past few decades, chaos and nonlinear dynamics have been used in the design of hundreds of cryptographic primitives. These algorithms include image encryption algorithms, hash functions, secure pseudo-random number generators, stream ciphers, watermarking and steganography. The majority of these algorithms are based on uni-modal chaotic maps and a big portion of these algorithms use the control parameters and the initial condition of the chaotic maps as their keys. From a wider perspective, without loss of generality, the similarities between the chaotic maps and the cryptographic systems is the main motivation for the design of chaos-based cryptographic algorithms. One type of encryption, secret key or symmetric key, relies on diffusion and confusion, which is modeled well by chaos theory. Another type of computing, DNA computing, when paired with chaos theory, offers a way to encrypt images and other information.

There are two different ways to apply chaotic maps in a cipher system:

1) Generate pseudorandom key streams using chaotic maps.
2) Use plain text or secret keys as initial conditions and control parameters.

Finally, as we apply some iteration on chaotic maps we get the cipher image.

III. ARCHITECTURE OF CHAOS CRYPTOSYSTEM

Chaos cryptosystem architecture includes 2 stages: Confusion and Diffusion. In the confusion stage, permutation is actually done on the image pixels without changing the actual values and the original image will be unrecognizable. This permuted image can be broken by any kinds of attacks and for more security, the second stage called diffusion is applied. In this second stage of encryption, each pixel’s value has changed according to the chaotic map which depends on initial conditions and control parameters. That is, the pixel value modification is done by the sequence generated from the chaotic map. As the chaotic map sequences are highly random, the encrypted image should also be highly random in nature and in the form which cannot be recognizable or break by any of the attackers. These confusion diffusion stages repeat for a number of times and the entire image get encrypted for better security.

IV. IMAGE ENCRYPTION TECHNIQUES

Different image encryption approaches using different chaotic maps are discussed in this section. In [3] a simple and efficient algorithm using chaotic Logistic map is presented. Here two logistic maps and an external secret key of 80-bit is used. This key is used to found out the initial conditions for both logistic maps. In the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24. The initial condition of the second logistic map is modified from the numbers, generated by the first logistic map. By modifying the initial condition of the second logistic map in this way, its dynamics gets further randomized. In this encryption technique, eight different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the second logistic map. Thus, the second chaotic map further increases the confusion in the relationship between the encrypted and its original image. To make the cipher more robust against any attack, after each encryption of a block of sixteen pixels, the secret key is modified.

Another technique of chaotic image encryption is using Standard map [4]. All the previous works of this technique explain the confusion and diffusion stages separately and those processes contribute to the cipher image respectively. Apart from that approach here introduces some sort of pixel value modification in the confusion stage itself remaining the actual diffusion process by itself. Consequently, the pixel value mixing effect is done by two levels of diffusing operations: modified substitution process and original diffusion function. However, before the pixels get relocated, diffusion effect is applied by adding the current pixel value of the plain image to the previous permuted pixel and then performs a cyclic shift on their sum. Apart from addition, other simple logical operations such as XOR can be used, or the shift operation can be performed before addition. However, the add-and-shift combination leads to the best performance and so it becomes the choice in this cryptosystem. Although this leads to a longer processing time in a single round, the overall encryption time is reduced as fewer rounds are required.

In [5] an image encryption algorithm using two different chaotic systems are explained. One among the three different chaotic systems Lorenz, Chen, Lu is used for the confusion stage. So here the pixels are get permuted using one of the above chaotic maps. Diffusion stage comes next and here also one among those three systems is used to change the pixel value. After these two steps of encryption, we get the cipher image which is unrecognizable by the attacker. Similarly, the decryption process is explained in the reverse way of encryption. Complex chaotic maps are taken rather than simple ones to improve the complexity of the process and thereby enhancing the security.

Another approach of encryption here uses a nonlinear traverse on the plain image using dependent diffusion and reverse cat map [6]. Here two cryptosystems are designed, one makes use of dependent diffusion and reverse cat map. Here when the new location of a pixel is calculated that pixel gets diffused immediately before calculating the next pixel's location. And this ciphered pixel value get influenced by the other pixel's confusion and diffusion process. By doing this way only one traverse on every pixel is needed as both confusion and diffusion get completed in it. In the second cryptosystem, a modified mapping based on a 2-D chaotic map is adopted in the confusion phase and a simple diffusion is performed in the same phase. In the conventional confusion process, a mapping from an ordinary position to a pseudorandom position is defined. Take the cat map as an example, the input sequence to the map is the regular pixel position while the output sequence is considered as pseudorandom. Here a new kind of mapping which maps a pseudorandom position in the plain-image to another pseudorandom position in the cipher image. With the help of the new mapping operation and simple diffusion in the confusion phase, the confusion and diffusion effects cannot be separated using a plain-image with identical pixels.

In [7] describes an image encryption and decryption technique using key sequence k_i generated by sequence k_{1i} of logistic map and sequence of states k_{2i} of Linear Feedback Shift Register (LFSR). Initially, one-dimensional sequence is generated in the range of 0 to 1 using logistic map for the bifurcation parameter r and initial value x_0. The generated sequences are multiplied by 255 and bit by bit XOR operation employed on states of 8 bit LFSR to obtain final key sequence, k_i. So obtained key sequence k_i is XORed with 8-bit grayscale image pixels p_i to obtain the encrypted image. Two 8-bit grayscale images were chosen for performance analysis of this algorithm. This scheme is compared with image encryption scheme using logistic map method. The results show original and encrypted image is highly uncorrelated and perceptually different. The histogram plot of the encrypted image is fairly uniform compared to encryption using only logistic map. It is also shown that decryption with wrong key results completely different image. Correlation, Entropy, Mean Square Error between original and encrypted image computed for both this and logistic map method. It is observed that the encryption provides cryptographically better results than encryption using logistic map scheme and provides more security, secrecy to the image.

One of the similar approaches [8] explains an image encryption and decryption process. The scheme is divided into two modules such as Encryption and Decryption module. The scheme includes generation of single key sequence k_i using two separate key sequences of (i) Logistic map k_{1i} and (ii) Lozi map k_{2i}. The encryption module is used to convert the original image into an encrypted form using key sequence k_i generated by the proposed scheme. Here XOR operation is used for encryption of the Image. The same key sequence k_i which was used during encryption process is used to decrypt the image. The decrypted image is identical to original image. It is observed that performance with respect to Visual analysis, Histogram, Correlation, Entropy, MSE between the original and encrypted image of the proposed scheme is better than the Logistic map or Lozi map alone. Hence encryption using the combination of Logistic map and Lozi map achieves better image security and immunity against attacks compared logistic map or Lozi map alone.

The approach in [9] elaborates an algorithm based on cat map and hyperchaotic Lorenz system. Hyperchaotic systems have more complex dynamical behaviors and a number of system variables. Image data have strong correlations among adjacent pixels and in this work, Arnold cat map is used to erase such correlations by changing the pixels positions. Diffusion stage which is used to modify the pixel values is done using a hyperchaotic system. This system is obtained by adding a nonlinear quadratic controller to the second equation of the Lorenz chaotic system and is employed to generate the diffusion keystream. This cryptosystem has higher unpredictability and larger key space.

Another encryption approach [10] is using two complex chaotic systems. The encryption algorithm is comprised of three-step processes. In the permutation process, the pixels of the plain image is scrambled via two-dimensional and one-dimensional permutation processes among RGB channels individually. In the diffusion process, the exclusive-or (XOR) operation is applied to hide the pixel information. The final encryption step is to mix RGB channels with chaotic sequences. This encryption step process is called "Chaotic Ponytail" vividly for its process likes a ponytail. The boundaries among RGB channels may be broken with this method. Therefore, it totally becomes an impossible thing to decrypt the image beginning with one channel to another. Two chaotic systems used in this work are complex Chen system and complex Lorenz system.

A novel bit-level image encryption algorithm based on chaotic maps [11] is one of the different methods in chaotic encryption. It explains a bit-level image encryption algorithm based on cyclic shift, swapping and piecewise linear chaotic maps (PWLCM). First, the plain image is decomposed into eight bit-planes using BBD. Second, the bit-planes are arbitrarily divided into two groups equally. As an example, we choose the four higher bit planes as one group and the four lower bit planes as the other group. Then, it transforms the two groups into two binary sequences, A1 and A2. The elements of the bit planes are arranged in order from top to bottom, left to right and higher bit plane to lower bit plane, to form A_1 and A_2. In the diffusion phase, chaos, cyclic shifts, and the XOR operation are employed to change the bit value in A_1 and A_2, and then B_1 and B_2 are produced. In the confusion phase, we swap the binary elements in B_1 and B_2 by using the control from the chaotic map, and then we obtain C_1 and C_2. Finally, through transforming C_1 and C_2 into bit planes and combining all of the bit planes, there obtain the cipher image. Round n is used to further improve the security of this system. The initial parameters and conditions of the chaotic maps serve as the secret keys.

In the work [12] explains an algorithm which employs the discrete cosine transformation dictionary to sparsely represent the color image and then combines it with the encryption algorithm based on the hyper-chaotic system to achieve image compression and encryption simultaneously. The algorithm in the compression and encryption module of each channel takes the DCT dictionary to sparsely represent the image, embeds the encryption algorithm into the process of the compression from three aspects: (1) scramble the position information of the effective coefficients, which can destroy the relationship between atoms in DCT dictionary and effective coefficients. So the algorithm can eliminate relativity among pixels in the wrong reconstructed image blocks. It can also eliminate the vulnerability by which we can get the outline information with a wrong key. (2)Use a hyper-chaotic system to control the coefficients transformation to encrypt the coefficients. (3) Use the diffusion algorithm to encrypt the folded image, but not encrypt the information blocks, which can guarantee the security of image and do not destroy the data structure of the information block. Through three ways of encryption, the cipher image has high security. The algorithm can compress and encrypt the image based on the requirements of the quality of reconstructed images, with some flexibility.

In [13] explains a new 2D chaotic map, called the 2D Logistic-adjusted-Sine map (2D-LASM). It uses the Logistic map to adjust the input of the Sine map and then extends its phase plane from 1D to 2D. Performance evaluations show that 2D-LASM has a wider chaotic range, better ergodicity, and unpredictability than several existing chaotic maps. Using 2D-LASM, this work further designs a 2D-LASM-based image encryption scheme (LAS-IES). It performs confusion and diffusion operations at the bit level. An additional mechanism of adding random values to the plain-image is designed to ensure that each encrypted result is different. Simulation results and security analysis show that LAS-IES can encrypt different kinds of digital images into random-like ones, and it has strong capability against various attacks. It contains three main components, namely, adding surrounding pixels, bit manipulation confusion, and bit manipulation diffusion. The adding surrounding pixels is to add random values to the plain-image to ensure that each encrypted result is different. Multiple rounds of confusion and diffusion are performed at the bit level to fulfill the principle of confusion and diffusion.

Another mage encryption scheme using chaotic tent map [14] is explained next. Chaotic behaviors of the tent map are studied analytically throughout its chaotic region in terms of the invariant density and the power spectrum. As the height of the maximum is lowered, successive band-splitting transitions occur in the chaotic region and accumulate to the transition point into the non-chaotic region. The tent map is topologically conjugate, and thus the behaviors of the map are in this sense identical under iteration. Chaotic sequences generated using the mapping are with good statistical properties, but under the finite precision, they show certain periodicity. As the value of μ gets larger, the chaotic sequence exhibits periodicity. But with the value of μ becoming smaller, chaotic sequences exhibit strong randomness; however, after finite iterations, the output value of the chaotic sequence is zero. This is because: Using piecewise linear functions to generate a chaotic mapping, the precision of initial value is always limited; Because of the limitation of the computer precision, the closer to 1 the number of approximate will more likely by processed as 1. Therefore, the value of μ is close to 2. In the chaotic region, the tent map $f\ (xi,\mu)$ has a unique ergodic invariant measure which is absolutely continuous with respect to the Lebesgue measure. Iterate the chaotic tent map N times using the system, and obtain the key array x(n). Mix the original image components with the key array x(n).

One of the latest work among this category and as an enhancement of the scheme using chaotic tent map is now going to explain. In this work [15] an improved algorithm, which is based on a rectangular transform (RT)-enhanced CTM system, has been described. Actually, 2D-RT is an enhancement of Arnold map and can be used to permute non-square images. As the previous work has omitted the permutation phase here it had been added again. Apart from the permutation processing, this method generates key streams related to the plain image also. That is, even if the secret keys are same key streams will be different for different plain images. Because of this, the key sensitivity had been improved. And when encrypting color images, it encrypts the three channels of the plain image at the same time and these channel encryptions associate with each other.

V. CONCLUSION

Chaos in the field of image encryption has improved the security in transmitting data over networks and the cipher image is not easy to decrypt by the attacker as because the encryption is done using randomly generated sequence by chaotic maps. It has proven that the chaotic maps generate sequences which are highly random and so the encrypted images using those random sequences will also be highly random and cannot be identified easily. In this survey paper, the existing chaos-based image encryption schemes have been discussed and analyzed. To conclude, each and every encryption schemes are useful for real-time image encryption and each scheme is unique in its own way. Security can be enhanced by having multiple chaotic maps for image encryption. Hence from all the encryption techniques explained in this survey paper it is concluded that encryption is ever changing and fast growing and always exhibit a high rate of security.

REFERENCES

[1] Lorenz, E.N., 1963. Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2), pp.130-141.

[2] Boeing, G. (2016). "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction". Systems. 4 (4): 37

[3] Pareek, N.K., Patidar, V. and Sud, K.K.(2006), "Image encryption using chaotic logistic map." Image and vision computing, 24(9), pp.926-934.

[4] Y. Yang, C. L. Teo, H. Daume III, and Y. Aloimonos, “Corpus guided sentence generation of natural images,” in EMNLP, 2011.

[5] Sakthidasan, K. and Krishna, B.S., (2011), "A new chaotic algorithm for image encryption and decryption of digital color images." International Journal of Information and Education Technology, 1(2), p.137.

[6] 4 Zhang, W., Wong, K.W., Yu, H. and Zhu, Z.L.(2012), "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion." Communications in Nonlinear Science and Numerical Simulation, 18(8)

[7] Rohith, S., Bhat, K.H. and Sharma, A.N.(2014), " Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register" In Advances in Electronics, Computers and Communications (ICAECC), 2014 International Conference on (pp. 1-6). IEEE.

[8] Rohith, S. and Sujatha, B.K(2015), " Image encryption and decryption using combined key sequence of Logistic map and Lozi map." In Communications and Signal Processing (ICCSP), 2015 International Conference on (pp. 1053-1058). IEEE.

[9] Zhang, J.(2015), "An image encryption scheme based on cat map and hyperchaotic Lorenz system" In Computational Intelligence and Communication Technology (CICT), 2015 IEEE International Conference on (pp. 78-82). IEEE.

[10] Wang, L., Song, H. and Liu, P(2015), "A novel hybrid color image encryption algorithm using two complex chaotic systems" Optics and Lasers in Engineering, 77, pp.118-125.

[11] Xu, L., Li, Z., Li, J. and Hua, W.(2016), " A novel bit-level image encryption algorithm based on chaotic maps." Optics and Lasers in Engineering, 78, pp.17-25.

[12] Tong, X.J., Zhang, M., Wang, Z. and Ma, J.(2016), " A joint color image encryption and compression scheme based on hyper-chaotic system." Nonlinear Dynamics, 84(4), pp.2333-2356.

[13] Hua, Z. and Zhou, Y.(2016), " Image encryption using 2D Logistic-adjusted-Sine map." Information Sciences, 339, pp.237-253.

[14] Li, C., Luo, G., Qin, K. and Li, C.(2017), " An image encryption scheme based on chaotic tent map." Nonlinear Dynamics, 87(1), pp.127-133

[15] Wu, X., Zhu, B., Hu, Y. and Ran, Y.(2017), " A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps." IEEE Access, 5, pp.6429-6436.