International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 4, April 2017)

Survey on CHAOS Based Image Encryption Techniques

Shwetha Kamath

Student, Department of Information Science & Engineering, Nitte Mahalinga Adyanthaya Memorial Institute of Technology (NMAMIT), Karkala, Udupi, India

***Abstract*— Now a days exchange of data over the network is keep on increasing, we using the for data exchange like open networks and internet. In data exchange security of the data is one of the major concern. We can encrypt the data before exchange like we can secure the data. The data can be in the format of text, image, audio and video etc.. Most of the multimedia applications includes images. Earlier AES, DES, RSA etc image encryption techniques were used, it contains low level of security and others can attack easily and hack the data. This problem was overcome by chaos based cryptography. The chaotic systems are knew to be very sensitive to the initial conditions and it controls the parameters which make them to appropriate for the image encryption. Now a days most of the work has been done using the chaos based image encryption. In this survey paper I tried to made a review the aspects and approaches of the design used for image encryption.**

***Keywords*— Cryptography, Chaotic Maps, Image Encryption, Image Decryption, security.**

I. INTRODUCTION

Now a days data exchange over the network is increasing quickly, it is important to protect the confidential data from those who don't have the access to that confidential data. It will affect the user's privacy and reputation if the confidential data gets hacked. The data exchange can be in the form of text, image, video, audio etc.. Each format of data has its own features and used different techniques to protect the data. Encryption technique is used when data can be exchanged through open networks such as internet where the multimedia applications are growing continuously.

Cryptography is the technique used for secure communication in present days. Cryptography deals with encryption, authentication, key distribution are some of the techniques used here. Image encryption is one of the technique to convert the original image into an image which is difficult to understand. Now a days image encryption are used in military communication, multimedia systems, medical science, telemedicine, internet communication etc. Here the idea behind encryption image is to consider a 2D image as a 1D data stream and this data stream is encrypted with textual based crypto system.

This approach is called nave approach. The nave approach is suitable to send the small size audio, video, text file though fast dedicated channel. This encryption algorithm will not satisfy the formats like JPEG, BMP, PNG, etc. It is not good idea when image size is much greater than the textual data. And also decrypted text should be same as original size, for image data this requirement is not necessary. When image is decrypted it contains small distortion and it is acceptable because human have the ability to see this characteristics.

Image encryption techniques have divided into two methods one is chaos based methods and other one is non-chaos bases methods. Based on the approach one of the method will be used for the image encryption. Image encryption also classified like full encryption and partial encryption based on the percentage of the data has been encrypted. Using this method several reviews have been published where image and video encryption is used.

This paper is organized as follows: Section II describes the basics of chaos theory for encryption. Section III describes the architecture of chaos based image crypto system. Section IV describes the Literature survey on some of the chaos based image encryption techniques. Section V provides analysis of results presented in the particular papers. Section VI provides the conclusion of the paper.

II. CHAOS THEORY FOR ENCRYPTION

A chaotic system behavior cannot be predicted; thereby it has similar appearance as noise. The relationship between cryptography and chaos it makes a chaos cryptographic algorithm it makes natural candidate for secure communication and cryptography. Properties such as sensitivity to changes in the initial conditions and control parameters, pseudorandom behavior and unstable periodic orbits with long periods are the common between cryptographic algorithm and chaotic maps. Using the chaos, the image encryption have ability of make sequence of numbers that are random in nature. Some of the similarities and differences between chaos technique and cryptographic techniques are listed in Table 1.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 4, April 2017)

Table 1:
The similarities and differences between chaos technique and cryptographic techniques.

Chaotic Systems	Cryptographic algorithms
Encryption transformations are defined only for real numbers.	Encryption transformations are defined on finite sets of integers.
Runs on iterations	Runs on rounds
parameters that are equivalent to encryption key	Encryption key
Sensitive to initial conditions and parameters	Diffusion property

III. CHAOS BASED IMAGE CRYPTO SYSTEM

There are two stages in architecture of chaos based image cryptosystem one is confusion stage and diffusion stage. In confusion stage the position of the pixel of the images are scrambled over the image without effecting the values of the pixels. In this stage the image can't be recognised. Here the initial conditions and control parameters serve as the secret keys. This stage is not secure because it has only one permutation stage and it can be break at any attack. In diffusion stage, in this process the value of the each pixel in entire image will get change. This process is carried out through chaotic maps and it is completely dependent on initial conditions and control parameters. In this stage the value gets modify sequentially by the sequence generated from the chaotic system. To increase the security level the confusion-diffusion rounds will repeats as many number of times. For image encryption the randomness property which inherent from the chaotic maps which make more suitable. The architecture of chaos based image crypto system is shown in the following Figure 1.

IV. LITERATURE SURVEY

An external secret key of 80-bit and two chaotic logistic maps are used in the image encryption scheme presented by N. K. Pareek, V. Patidar, and K. K. Sud. By giving separate weightage to every one of its bits, using the external secret key the initial conditions for both the logistic maps are derived.

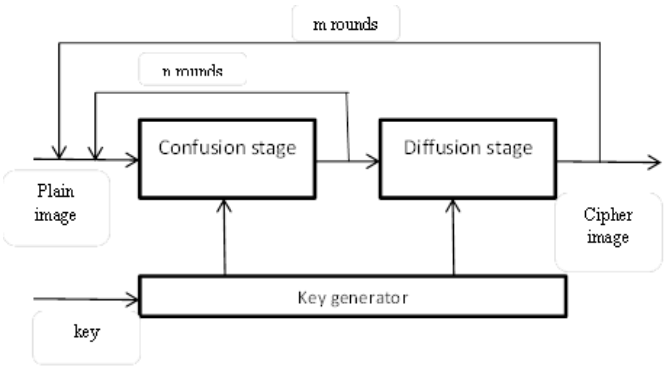

Figure 1. Chaos - based image cryptosystem.

In this algorithm the first logistic map is used for generating the numbers ranging from 1 to 24, where the numbers can be repeated. The numbers generated by the first logistic map are used to modify the initial conditions of the second logistic map. By altering the initial condition of the second logistic map in this manner, its elements get additionally randomized. In the proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a specific pixel is chosen by the result of the logistic map. The secret key is modified each time, after encrypting the each block of 16 pixels of the image, to make the cipher more powerful (robust) against any attacks. In this method key sensitivity is high, despite the fact that it can resist brute force attack, and also it has a small key space and has the key space of 10^60. [1]

Because of the disadvantage of poor security in one-dimensional chaotic cryptosystems, Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li introduced a new scheme called Nonlinear Chaotic Algorithm (NCA). The one-dimensional chaotic map has linear function. But in the case of Nonlinear Chaotic Algorithm (NCA) uses power function and tangent function instead of linear function. In the encryption method, at first the encryption key is set. After that, the NCA is iterated 100 times to acquire the encrypted image called cipher image. Once the encryption process completed, that encrypted image is send through the public communication channel and key corresponds to that encrypted image is sent through the secured communication channel. Finally at the receiver side, the decryption process is similar to the encryption algorithm, to obtain the original image from the received cipher image. In this paper I have noticed the advantages of top level security and also sensitive to key. [2]

K. Sakthidasan Sankaran and B.V. Santhosh Krishna proposed a scheme for encrypting the images; this cryptosystem consists of two stages known as confusion stage and diffusion stage. Each of these two stages makes use of different chaotic systems. In this paper they have chosen complex chaotic maps rather than simple ones to further increase the complexity level of the algorithm, this can be help in improving the security. Plain image is taken as the input for the cryptosystem, which is to be encrypted to obtain ciphered image.in the confusion stage, the 3D chaotic systems are used for permutation of the pixel position of plain image. In the diffusion stage, diffusion of pixel value is carried out using any one of the chaotic systems. Initial conditions and control parameters used for generating the chaotic sequence in both the stages are considered as the secret key. There must be separate secret keys for both permutation and diffusion stage of the encryption process. Usage of separate secret key increases the security level of that algorithm. Resulting image is called as the ciphered image. Same as encryption, the decryption process also consisting of two stages i.e. Diffusion followed by confusion stage. In the diffused image decryption stage, the original pixel values are retained back by using any one of the chaotic systems. They diffusion key used in the second stage of encryption, that same key is used here for diffused image decryption stage. The same confusion as used in the first stage of encryption is used to get back the original form of the image i.e. plain image/original image. [3]

Daesung Moon, Y. Chung, Sung Bum Pan, K. Moon and Kyo ll Chung are introduced an efficient selective encryption of fingerprint images for embedded processors. In this paper they explained about an image based selective bitplane encryption algorithm for fingerprint images.in this proposed selective biplane algorithm consisting of two steps known as image distortion and LSB encryption.in the image distortion step the full fingerprint image is misrepresented by making use of any simple operations. After that the LSB of each pixel is selected as the random noise and construct the LSB bitplane. After this we need to perform the sinple exclusive-OR operation of the LSB bitplane and all the pixels of the original fingerprint image. Advantage here is that, without knowledge of the LSB bitplane no one can recover the ridge structure of the original fingerprint image from the result obtained from image distortion step.

Next in the LSB encryption, only need is to further encrypting the LSB bitplane by using the shared session key. both sender and client share the same key so the client can easily recover the original fingerprint image by applying the decryption algorithm to the encrypted bitplane and then by applying the same exclusive- OR operation. It will guarantee confidentiality of the fingerprint image between a sensor and a client in real-time. It has a disadvantage of limited perceptual quality. This guarantees that the confidentiality between the sender and the client in real-time. But it has the disadvantage of limited perceptual quality. [4]

A new scheme for image encryption is introduced by F. Sun, S. Liu, Z. Li, and Z. Lu, based on the spatial chaos map. The basic idea of this encryption scheme is to encrypt the image, pixel by pixel in space with the use of spatial chaos map. The basic idea is to encrypt the image in space with spatial chaos map, and then the pixels are confused in various directions of space. Initially in the encryption process the original image is converted to the matrix form. After that, this matrix is encrypted using the results obtained by the iterations of spatial chaos map. Now considering the initial conditions and the control parameters of chaotic map, the spatial chaos map is initially iterated once and it generates a new matrix. Now the parameters of spatial chaos map are modified according to the newly constructed matrix. This process is repeated until we get the ciphered image. The decryption procedure used here is similar to the encryption procedure, where the ciphered image is used as the input instead of the original image in the encryption procedure. In this approach both encryption and decryption has the comparably similar structure, they have basically the same algorithmic complexity and time utilization. The advantage here is that, it is highly secure and the key space is large enough to resist the attacks. [5]

L. Chen and D. Zhao introduced a new approach based on Fractional Wavelet Packet Transform (FWPT) to encrypt images, here the fractional order of the fractional wavelet packet transform is considered as the key. FWPT is a Wavelet Packet Transform (WPT) acknowledged in a Fractional Fourier space (domain). In this strategy first the image is divided into different sub bands. At that point a portion of the sub bands are randomly chosen and then encrypted using FWPT.

The chosen encryption with FWPT is more successful than that with WPT, because it is acknowledged in the partial Fourier domain and the data is more arbitrarily distributed at fractional Fourier plane than at Fourier plane. The advantage of this paper is that, to achieve the data confidentiality. Furthermore, it has a disadvantage of constrained key space and restricted perceptual quality. Here the key space size refers to, the total number of keys that are used in the encryption scheme. When the key space is large enough to make the brute-force attacks infeasible, then that is considered as a good encryption scheme. Restricted perceptual quality means after encryption we will get the partial view of the original image. [6]

In the paper introduced by Song Zhao, Hengjian Li and Xu Yan are explains about the secure and efficient fingerprint images encryption scheme, by combining with the shuffle operation and nonlinear dynamic chaos system. Initially the original image undergo with total shuffling operation to shuffle the image pixel positions in the spatial-domain. Now the pixels of shuffled image are rearranged in the order of left to right and top to bottom, these pixels are converted to its binary equivalent form. After this the Nonlinear Digital Filter (NDF) chaotic is iterated, this NDF is used to encrypt the image. The key streams constructed by the NDF are XOR-ed with the binary equivalent of the original image for obtaining the encrypted image. The decryption process is also similar to that of encryption algorithm used. For decrypt the image, use NDF with the same parameters and same initial values as that used in the encryption algorithm. And then perform anti-shuffle to obtain the resulting image. This resulting image is nothing but the original fingerprint image. This encryption process is good resistant for brute force attack and also the encryption algorithm is sensitive to the key. But this encryption process is not time efficient. [7]

In the paper presented by Guanrong Chen, Yaobin Mao, Charles K. Chui and Guanrong Chen, Yaobin Mao, Charles K. Chu , the two-dimensional chaotic cat map is generalized in to 3D for designing a real-time secure single key encryption scheme. Initially select the key of 128 bit long, after that divide that key into 8 groups. Next these 8 groups are further mapped onto the different parameters of the 3D cat map and the logistic map. After mapping, the 2D image is converted to the 3D image. Now we can generate the shuffled images using the 3D cat map. Now need to perform XOR and mod operations on that image using the logistic map and then convert 3D image back to a 2D image. By this process encrypted image can be obtained.

Decryption process is exactly same as that of encryption process. The advantages here are the fast encryption speed. And compared to other encryption techniques it has small key space. [8] [9]

The image encryption algorithm which based on the Fractional Fourier transform (FFT) and the chaotic system is introduced by Jinhui Lai, Song Liang, and Delong Cui. In this the encryption algorithm consists of 2 steps. In the first step the image is encrypted twice in random phase using Fractional Fourier domain. In the second step that image once again encrypted using a matrix that generated by the chaotic system because of this the encrypted fingerprint image is generated. The decryption process is the reverse procedure of that encryption process used. Although it has small key space, it will resist the brute force attack. [10][11]

Tiegang Gao and Zengqiang Chen introduced an image encryption technique based on a new total shuffling algorithm. Here they explained about a new scheme, where a new image total shuffling matrix is generated to change the positions of the image pixels. Now make use of the state combination of the two chaotic systems to make confusion between the relationship of original image and the ciphered image. By doing some iteration on the logistic map the image total shuffling matrix is constructed and then changes the positions of row and columns values of that matrix. Now the cipher image can be obtained by applying Lorenz chaotic system and Chen's chaotic system. The advantage of this technique is that it has large key space and it is sensitive to the key and also it will resist all the kinds of brute force attack. Because of the row and column transformation require the more time, this encryption algorithm is not time efficient. [12]

In the paper presented by kamlesh Gupta and Sanjay Silakari, the original image of the size mxn is converted into 3 separate images like Red, Green and Blue images (by extracting the features). In which the Red and Green images are considered as the vertical and the horizontal planes respectively, and the blue image is considered as it is. From the Transformed/converted image, one row is read from each of three planes to create a new plane from these three image planes. In the first level of confusion is done by make use of the 2D cat map (Arnold's cat map). Then the final confusion stage can be performed by cascading the two maps (i.e. first by cat map and then by standard map). After the confusion stage the next will be the diffusion stage (confusion stage is followed by the diffusion stage).

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 4, April 2017)

The cipher image is obtained by XORing the each pixels of confusion matrix with the each pixels of diffusion matrix. Here also the decryption process is reverse of that encryption process. [13]

K. Gupta, R. Gupta, R. Agrawal, and S. Khan, introduced an Ethical Approach of Block Based Image Encryption Using Chaotic Map. In this paper they selected chaotic map because of its dynamic nature, randomness and the very sensitive towards initial condition. The proposed algorithm makes use of 2D chaotic map and two secret keys for encryption process. In the initial step image is divided into four blocks and each individual block was encrypted n- times. After that the secret key is inverted for each of the block, and again process was repeated up to m-times. The advantage of this technique is that it has large key space and it is sensitive to the key and also it will resist some kinds of brute force attack. By examining the proposed algorithm can be a good enough for real time secure communication. [14]

The Image Encryption Algorithm Based on Chaotic Economic Model is proposed by S. S. Askar, A. A. Karawia, and A. Alshamrani, is a new approach which uses chaotic economic map for encryption and decryption of images. This is the first attempt, where the economic chaotic map is used in the construction of chaotic cryptography. The simulations and experimental results shown in the paper clearly shows that the proposed algorithm has (1) a very large key space of 1084, (2) high sensitivity secret keys, (3) entropy value that is close to the ideal value of 8, and (4) low correlation coefficients. So we can say that, these results lead to the effectiveness and robustness of the proposed image algorithm. [15]

V. Result Analysis

The different techniques mentioned above in this paper are studied well and by comparing each of those techniques, I summarized in the form of table. Where, I am able to find out some of the advantages and disadvantages of the techniques they have proposed in their paper. By observing the Table 2, we can easily understand the techniques used in the paper, as well the advantages and disadvantages of the particular techniques.

Table 2:
The advantages and disadvantages of some chaos based encryption techniques used for encrypting the images.

Reference paper	Techniques used	Advantage	Disadvantage
[1]	*Two chaotic logistic map	*it is highly sensitive to the key	*Small key space.
[2]	*Nonlinear chaotic algorithm	*Provides High level security	*Small key space.
[3]	*Selective bitplane encryption	*Guarantees confidentiality	*Limited perceptual quality.
[4]	*Lorenz chaotic system and Chen's chaotic system + *3D chaotic cat map	*It has Fast encryption speed *key space is large *it is Sensitive to the key *Resist brute force attack.	*Plain-image must be square size. *Not time efficient
[5]	*Spatial chaotic map	*Highly secured technique.	*It has small key space.
[6]	*Fractional wavelet packet transform	*Achieve data confidentiality	*Limited key space *Limited perceptual quality.
[7]	*Logistic map + *Nonlinear digital filter chaotic map	*Resist to brute force attack *Encryption algorithm is sensitive to the key	*Not time efficient *It takes more time for encryption
[8] [9]	*3D chaotic cat map + *Logistic map	*Fast encryption speed	*Having Small key space *Plain-image

			must be square size
[10] [11]	*Fractional Fourier transforms. + *Logistic map	*Resist brute force cracking	*It has Small key space
[12]	*Logistic map + *Lorenz chaotic system and Chen's chaotic system	*Large key space *Sensitive to the key *Resist brute force attack	*Not time efficient *It takes more time for encryption
[13]	*Arnold's cat map	*Fast encryption speed	*Plain-image must be square size
[14]	*2D chaotic map	*it has large key space *it is sensitive to the key *it will resist some of brute force attack	*It takes more time for encryption
[15]	*chaotic economic map	*a very large key space of 1084 *high sensitivity *secret keys lead to the effectiveness and robustness	*It takes more time for encryption

VI. Conclusion

Providing security for the digital images is a challenging problem in the field of communication by transmitting of digital products over the open network. At present, various new encryption schemes are introducing but fast and secured conventional encryption techniques will give the high rate of security. In this paper, the literature survey on existing chaos based image encryption techniques is discussed. The mentioned encryption techniques above in the paper are studied and analysed well, to find the performance of the technique as well as its security proceedings. According to the survey I conclude that each technique discussed in this paper is unique on its own way, and also each technique is suitable for different applications.

REFERENCES

[1] Pareek, N. K., Patidar, V., & Sud, K. K. 2006. Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926-934.

[2] Gao, H., Zhang, Y., Liang, S., & Li, D. 2006. A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals, 29(2), 393-399

[3] K.Sakthidasan Sankaran and B.V.Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of information and Education Technology, Vol. 1, No. 2, June 2011.

[4] Moon, D., Chung, Y., Pan, S. B., Moon, K., & Chung, K. I. 2006. An efficient selective encryption of fingerprint images for embedded processors. ETRI journal, 28(4), 444-452.

[5] Sun, F., Liu, S., Li, Z., & Lü, Z. 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons & Fractals, 38(3), 631-640

[6] Chen, L., & Zhao, D. 2008. Image encryption with fractional wavelet packet method. Optik-International Journal for Light and Electron Optics, 119(6), 286-291.

[7] Song, Z., Hengjian, L., & Xu, Y. 2008. A secure and efficient fingerprint images encryption scheme. In Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for (pp. 2803-2808). IEEE

[8] Chen, G., Mao, Y., & Chui, C. K. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749-761

[9] Mao, Y., Chen, G., & Lian, S. 2004. A novel fast image encryption scheme based on 3D chaotic Baker maps. International Journal of Bifurcation and Chaos, 14(10), 3613-3624.

[10] Lai, J., Liang, S., Cui, D. 2010. A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Chaotic System. In Multimedia Communications (Mediacom), 2010 International Conference on (pp. 24-27). IEEE.

[11] Cui, D. 2010. A novel fingerprint encryption algorithm based on chaotic system and fractional Fourier transform. In Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference on (pp. 168-171). IEEE.

[12] Gao, T., & Chen, Z. 2008. Image encryption based on a new total shuffling algorithm. Chaos, solitons & fractals, 38(1), 213-220

[13] Kamlesh Gupta1, Sanjay Silakari," New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, 2, 139-150

[14] K. Gupta, R. Gupta, R. Agrawal, and S. Khan, "An Ethical Approach of Block Based Image Encryption Using Chaotic Map," International Journal of Security and Its Applications vol. 9, no. 9, pp.105-122, 2015.

[15] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol. 2015, Arti-cle ID 341729, 10 pages, 2015.