International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Review Paper on Chaotic Map Image Encryption Techniques

Chetana Singh[1], Binay Kumar Pandey[2], DR.H.L.Mandoria[3], Ashok Kumar[4]

[1]Information Technology, PG Student, G.B.Pant University of Agriculture and Technology, India,
[2]Information Technology, Assistant Professor, G.B.Pant University of Agriculture and Technology, India
[3]Information Technology, Professor, G.B.Pant University of Agriculture and Technology, India,

---***---

Abstract:- *This paper presents a comprehensive survey on chaotic image secret writing schemes. within the modern time,Due to the quick development of digital communication and multimedia application, security becomes a vital issue of communication, storage and transmission of digital information such as image, audio and video. Image secret writing has been a preferred research field in recent decades. Secret writing technique are used in several fields such as medical science, military, geographic satellite images. Chaotic secret writing is one of the best alternative ways to make sure security. A lot of image secret writing schemes using chaotic maps have been proposed, because of its excessive sensitivity to initial conditions, unpredictability and random like behaviors.*

Keywords- *chaotic algorithms; cryptography; image encryption chaotic maps.*

1. INTRODUCTION

In the previous few days tremendously growth of digital and multimedia technology, image protection has become an vital issue for communication of digital images through the networks and encryption is the one of approaches to provide the protection of digital images. Image encryption is the technique of transforming data using an algorithm to make it unreadable to any one without those possessing specific knowledge, generally referred to as a key. In1970s,Chaos concept was proposed, which was used in a wide range of research areas, such as mathematics, engineering, physics, biology, and so on[1]. The complicated behavior of chaotic structures in nonlinear deterministic was described. The first description of a chaotic techniques was made in 1963 via Lorenz[2], who developed a system know as the Lorenz attractor that coupled nonlinear differential equations. The implementation of chaotic maps in the improvement of cryptography structures lies in the reality that a chaotic map is characterized by:(a)the initial conditions and control parameters with excessive sensitivity, (b)unpredictability of the orbital evolution, (c)the simplicity of the hardware and software implementation leads to a excessive encryption rate. These characteristics can be related with some very essential cryptographic properties such as confusion and diffusion.[3].

1.1 WHAT IS IMAGE ENCRYPTION?

Image encryption is a smart hiding of information. An authentic essential and personal plain text is transformed into cipher text that is curiously random nonsense. The most important idea in the image encryption is to transmit the image securely over the network so that no unauthorized person can able to decrypt the image. In this paper we centre of attention on the encryption methods of digital image based totally on the chaos mapping. The encryption methods based on the chaos mapping offers the encrypted digital images to preserve the multi stage encryption approach and also decreases the computational complexity of the encryption process. Most of the algorithms particularly designed to encrypt digital images are proposed in the mid-1990s. There are two essential groups of image encryption algorithms: (a)non-chaos selective techniques and (b)Chaos-based selective or non-selective methods[4].

1.2 WHAT IS CRYPTOGRAPHY?

Cryptographic methods assist invulnerable transmission and storage of data. Cryptography includes the encoding of image at senders side which converts the image so that the contents are no longer comprehensible called Encryption and Decryption at receivers side to achieve the authentic image. Even if the eaves dropper receives get entry to the image one will now not recognize the contents. In applications like aeronautic, military, medical tightly closed communication is the most vital concern. Some specific encryption algorithms like AES, DES etc. are in efficient for image encryption. Chaotic functions are being used for image encryption rather than the standard algorithms[3].

1.3 WHAT IS CHAOTIC SYSTEMS?

The term chaotic comes from chaos. Chaos does no longer have a described meaning; it might also refer to a state that does not have deterministic behavior. Chaotic structures depend totally on initial condition. Chaotic concept was summarized via Edward Lorenzas follows "When the current determines the future, but the approximate current does not approximately determine the future Chaotic method is a area of mathematics and has a number of applications in meteorology, economics, philosophy etc.

Chaotic concept concerns deterministic structures whose behavior can be predicted. These systems can be predicted for a while and then they become random[5].

1.4 CHOS BASED IMAGE CRYPTOSYSTEM ARCHITECTURE

The architecture of chaos based image cryptosystem mainly consists of two stages: the confusion stage and the diffusion stage. The typical block diagram of the architecture is as depicted in the figure.

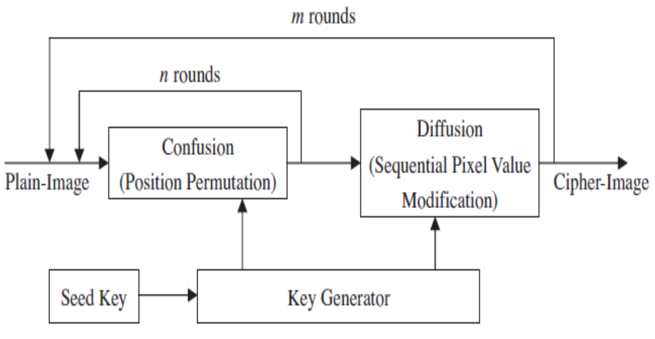

Fig. 1. A classic image encryption architecture.

The confusion stage is the pixel permutation where the positions of the pixels are scrambled over the entire image without disturbing the values of the pixels. With this the image becomes unrecognizable. It is not very secure to have only the permutation stage since it may be broken by any attack. To enhance the security, the second stage of the encryption process aims at changing the value of each pixel in the entire image. In the diffusion stage, the pixel values are modified sequentially by the sequence generated from the chaotic systems. The whole confusion-diffusion round repeats for number of times to achieve security of satisfactory level[5].

2 LITERATURE REVIEW

Asia Mahdi Naser Alzubaidi In this scheme author proposed an image encryption scheme based on 3D logistic transform, it divided the image in distinct shade channels of YCBCR and applied exclusive methods of selective encryption and chaotic encryption. On Y factor a selective encryption algorithm is performed to guard the sensitive information. Further the confusion method is adopted through the use of 2D Arnold cat transformation to make greater distortion of the relationship among adjacent pixels of Y image and to cover the statistical structure of pixels. Scrambling methods depend on row-column approach utilized in dependently on Cb andCr components.[2].

Bremnavas, B.PoornaandI. Raja Mohamed In this paper proposed the Secured clinical image transmission using chaotic map used simply Henon chaotic map for scientific image encryption therefore making it an simple task for attackers to decrypt and restricted their work to scientific images only. First step in this work is to generate the noisy signal using the Chaotic Henon map. Here the Henon equations are generated with the signal in both 'x' and 'y' axes. This offers the advantage of sending two patients clinical images at a single transmission. For example, the first patient medical is added in 'x' axis and then an other one is added in 'y'axis[3].

Lalita Gupta, Rahul Gupta and Manoj Sharma proposed an encryption scheme which targeted on disquieting the correlation among image pixels. They used pixel shuffler horizontally as well as vertically, 2D bakers map described with the following formulas $B(x,y)=(2x,y/2)$ When $1/2<x<1$,$B(x,y)=(2x-1, y/2+1/2)$ When $0<x<1/2$ and created confusion in the image with bit XOR with noise image non linear (liapunav exponential) function operation to satisfied condition of chaos. The diffusion template is created by random number generator based on Gaussian distribution and is capable of providing the key length of 64 bits although its length can be extended further[4].

Rajinder Kauretal the International Journal of Computer Science and Mobile Computing, introduced selective image cryptography based on the region, followed selective compression where parts of the image containing vital information are compressed without loss while regions containing information not important are compressed. The Henon map is used to generate the keys. The image is divided into blocks and then these blocks are mixed. The transformed image is fed to the blow-fish algorithm. This algorithm is generally used for text data encryption. The use of the blow-fish algorithm is a disadvantage of this scheme because it would make the process low and not as reliable[5].

Robert A.J. Matthews In the work considered the use of genetic algorithms (GAs) as powerful tools in breaking cryptographic systems. They demonstrated that GA scanning greatly facilitates cryptanalysis by efficiently analyzing large key spaces and demonstrating their use with GENALYST, an order-based GA for breaking a classic cryptosystem[6].

Ali Kanso In this scheme the author has exported the self-shrinking technique used in classical cryptography in chaotic systems to develop chaotic generators of key flows capable of generating key flows characterized by excellent statistical properties and a high level of security. This paper proposes an example of self-shrinking key flow generator based on the chaos implemented using a 1-D chaotic map. The randomness properties and statistical test results of the key flow bits generated by applying the self-shrinking technique on chaotic maps with appropriate parameters were encouraging [7].

Pareek, N.K., Patidar, V. and Sud, K.K. In this document a new approach for image cryptography based on chaotic logistic maps to meet the requirements of secure image transfer. In the cryptographic scheme of the proposed image, an external 80-bit secret key and two chaotic logistic maps are used. The initial conditions for both logistic maps are derived using the external secret key providing an era of different weight to all of its bits[8].

Behnia, S., Akhavan, A., Akhshani, A. and Samsudin In this approach a new algorithm of image cryptography based on the elliptical map of Jacobian was studied by. In this article, a redesign of a class of chaotic cryptographic systems is suggested to overcome the aforementioned drawbacks. This work is the first attempt to explore the elliptical maps of Jacobian as a cryptosystem. Experimental results and safety analysis indicate that the cryptographic algorithm based on the chaotic elliptical map is advantageous from the point of view of large key spaces and a high level of security[9].

Omid Mirzaei, Mahdi Yaghoobi and Hassan Irani In this algorithm, researched a new image cryptography scheme based on a total and parallel encryption algorithm. Two chaotic systems were used in the cryptographic algorithm to confuse the relationship between the simple image and the encrypted image[10].

Yicong Zhou, Long Bao and C.L.Philip Chen In the document by proposed an encryption scheme in which a new chaotic system is used for cryptography of the image. In this system, two un dimensional chaotic maps are integrated and a series of new chaotic maps are generated. A new cryptographic algorithm of the image that has the excellent properties of confusion and diffusion to withstand various attacks, in particular the chosen plaintext attacks was introduced by them to demonstrate its applications. A completely different image is obtained each time the algorithm is applied to an original image with a similar set of security keys. This ensures that the proposed algorithm is able to withstand selected plaintext attacks. This can be simulated using MATLAB[11].

G.A. Sathish Kumar, Dr.K. Bhoopathybagan and Dr.N. Sriraam In the document of Image of cryptography based on diffusion and on more chaotic maps. In this document, the cryptography of the image is based on a technique that uses multiple circular mappings based on chaos. There are three stages in this algorithm. In the first phase, the chaotic logistic maps are used to give a pair of subkeys. In the second phase, the subkeys of the logistic map are used to encrypt the image and, consequently, the diffusion is obtained. In the third step, four different chaotic maps are used to generate the subkeys. Various random numbers are produced by each map from the orbits of the maps based on the initial conditions. From those random numbers, a key is selected for encryption. Based on the key that controls the encryption algorithm, a binary sequence is generated. With the help of the two different scanning models (raster and Zigzag), the input image is converted into a 1D matrix and divided into various sub-blocks. Subsequently, the permutations are applied to each binary matrix based on the chaotic maps. Finally, the image can be decrypted using the same subkeys[12].

Shoaib Ansari, Neelesh Gupta and Sudhir Agrawal In this work proposed a new algorithm for cryptography and decryption of images. An approach based on cryptography of the image that uses the chaotic map in the frequency domain. In this algorithm, the chaotic map used for cryptography is the 2D Baker Map. First, the discrete 2D cosine transformation of the image is calculated. Then the image is mixed using the Bakers 2D map. Here two maps of bakers are used. One of them with the initial keys and the other with the Gaussian image created with mean and variance. The DCT has transformed the image and the diffusion image is XORed in an iterative way. The random number generator based on the Gaussian distribution is used to create the diffusion model. The advantage of this method is that it can provide a key length of 128 bits and above. This technique can be simulated using matlab [13].

Xiaoling Huang, Guodong Ye and Kwok Wo Wong in their article: Chaotic image encryption algorithm based on circulator functioning proposes the image coding scheme based on the time-delay Lorenz system and circulating matrix[14].

COMPAIRSON OF CHAOTIC MAPS

<table>
<tr><th>Reference</th><th>Chaotic map used</th><th>Features</th></tr>
<tr><td>[16]</td><td>Lorenz
Chen Lu</td><td>Key size-Large
Key Sensitivity-Medium
Correlation coefficient
<table>
<tr><td>Cofficent</td><td>Plain image</td><td>Cipher image</td></tr>
<tr><td>Horizontal</td><td>0.9791</td><td>0.0052</td></tr>
<tr><td>Vertical</td><td>0.9357</td><td>0.0539</td></tr>
<tr><td>Diagonal</td><td>0.9183</td><td>0.1141</td></tr>
</table></td></tr>
<tr><td>[21]</td><td>Lorenz,Baker</td><td>Key Size-2^{128}
Key Sensitivity-High
<table>
<tr><td colspan="2"></td><td colspan="3">Correlation coefficient</td></tr>
<tr><td colspan="2"></td><td>Red</td><td>Green</td><td>Blue</td></tr>
<tr><td>Horizontal</td><td>Plain image</td><td>0.9508</td><td>0.9707</td><td>0.9579</td></tr>
<tr><td></td><td>Cipher image</td><td>-0.005</td><td>0.0018</td><td>0.0002</td></tr>
<tr><td>Vertical</td><td>Plain image</td><td>0.9718</td><td>0.9754</td><td>0.9818</td></tr>
<tr><td></td><td>Ciphe</td><td>0.003</td><td>-</td><td>0.001</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td><table><tr><td></td><td>r Image</td><td>2</td><td>0.0063</td><td>8</td></tr></table>Corresponding entropies- 7.99758,7.99708,7.99749</td></tr>
<tr><td>[15]</td><td>Henon Map</td><td>Key Size-2^{128}
Key Sensitivity-High
Correlation coefficient<table><tr><td>Coefficient</td><td>Plain image</td><td>Cipher image</td></tr><tr><td>Horizontal</td><td>0.9976</td><td>0.0096</td></tr><tr><td>Vertical</td><td>0.9924</td><td>0.0038</td></tr></table>Average Entropy-7.9904
NPCR-0.0015%
UACI-0.0005%</td></tr>
<tr><td>[18]</td><td>Logistic map</td><td>Key Size-10^{45}
Key Sensitivity-High
Correlation coefficient<table><tr><td>Coefficient</td><td>Plain image</td><td>Cipher image</td></tr><tr><td>Horizontal</td><td>0.9278</td><td>0.0965</td></tr><tr><td>Vertical</td><td>0.9609</td><td>0.1086</td></tr><tr><td>Diagonal</td><td>0.9060</td><td>0.0161</td></tr></table>Average Entropy-7.9996
NPCR-99.6231
UACI-33.4070</td></tr>
<tr><td>[19]</td><td>Arnold Cat map</td><td>Key Size-2^{148}
Key Sensitivity-High
Correlation coefficient<table><tr><td>Coefficient</td><td>Plain image</td><td>Cipher image</td></tr><tr><td>Horizontal</td><td>0.9156</td><td>0.001</td></tr><tr><td>Vertical</td><td>0.8808</td><td>0.006</td></tr><tr><td>Diagonal</td><td>0.8603</td><td>0.091</td></tr></table>Average Entropy-7.9902
NPCR-99.609
UACI-33.464</td></tr>
</table>

3 CONCLUSION

This document discusses many cryptographic algorithms that use different chaotic maps. Each algorithm has its advantages and disadvantages depending on the encryption performance of these algorithms. Analyzing the research documents mentioned above, some features of the cryptographic techniques of the image are included. Each of them uses chaotic maps of different sizes for the secure encryption of images. The image can be encrypted in different ways at different speeds using chaotic maps of various sizes. The above algorithms are also resistive against various attacks that can be demonstrated by the safety analysis.

REFERENCES

[1].H.L.Mandoria,Samridhi Singh et al(2017)" A Review on Image Encryption Technique and to Extract Feature from Image" IJCA International Journal of Computer Application.

[2].Asia Mahdi, Naser Alzubaidi, “Selective Image Encryption with Diffusion and Confusion Mechanism”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) - Volume 4, Issue 7, July 2014

[3] Bremnavas1, B.Poorna2 and I.Raja Mohamed, “Secured medical image transmission using chaotic map”, Computer Science and Engineering Elixir Comp. Sci. Engg. 54 (2013) 12598-12602

[4]Lalita Gupta1, Rahul Gupta and Manoj Sharma, “Low Complexity Efficient Image Encryption Technique Based on Chaotic Map”, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 11 (2014), pp. 1029-1034

[5]Rajinder Kaur1, Er. Kanwalpreet Singh, “Comparative Analysis and Implementation of Image Encryption Algorithms”, International Journal of Computer Science and Mobile Computing (IJCSMC) - Vol. 2, Issue. 4, April 2013, pg.170 – 176

[6]R. A. Matthews, “The use of genetic algorithms in cryptanalysis,” Cryptologia, vol. 17, no. 2, pp. 187–201, 1993.

[7]A. Kanso, “Self-shrinking chaotic stream ciphers,” Communications in nonlinear science and numerical simulation, vol. 16, no. 2, pp. 822–836, 2011.

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

[9] Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2013). Image encryption based on the jacobian elliptic maps. Journal of Systems & Software, 86(86), 2429-2438.

[10] Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, 67(1), 557-566.

[11] Yicong Zhou, Long Bao and C.L.Philip Chen"A New1D Chaotic System for Image Encryption", Signal Process. 97(2014) 172-182.

[12] G.A.Sathishkumar ,Dr.K.Bhoopathybagan and Dr.N.Sriraam ―Image Encryption Based on Diffusion and Multiple Chaotic Maps||, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March2011,181-194.

[13] Shoaib Ansari, Neelesh Gupta and SudhirAgrawal, ―An Image Encryption Approach Using Chaotic Map in Frequency Domain||, International journal of Emerging Technology and Advanced Engineering-Volume 2, Issue 8, August 2012

[14] Xiaoling Huang,Guodong Ye, and Kwok-Wo Wong, ―Chaotic Image Encryption Algorithm Based on Circulant Operation‖, Abstract and Applied Analysis,Volume2013

[15] Somya Al-Maadeed,Afnam Al-Ali, and Turki Abdalla, A New Chaos-Based Image-Encryption and Compression Algorithm",Hindawi Publishing Corporation,Journal of Electrical and Computer Engineering, Volume 2012,Article ID 179693.

[16]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.

[17] Mrs.A.Anto Steffi,Mr. Dipesh sharma,"An Image Encrption Algorithm based on 3D Lorenz map" International Journal of Advanced Research in Computer Science, Vol. 4 No.2,(Jen-Feb 2013) ISSN: 0976-5697.

[18] Hazem Mohammad Al-Najjar,Asem Mohammad AL-Najjar"Image Encrption Algorithm Based on Logistic Map And Pixel Mapping Table".

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

[20] A.Anto Steffi, Dipesh Shrama "An Image Encryption Algorithm based on 3D Lorenz Map"