ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Survey on various image encryption schemed through Chaotic Maps

Pooja Kathil
Dept. of Information Technology
Rajiv Gandhi Technical University
Bhopal (M.P.), India

Sachin Goyal
Dept. of Information Technology
Rajiv Gandhi Technical University
Bhopal (M.P.), India

Ratish Agrawal
Dept. of Information Technology
Rajiv Gandhi Technical University
Bhopal (M.P.), India

Abstract: In modern days there are various image encryption techniques forecast for bringing image reliability and protection in the internet for the evolution of government, medical applications, military. In this paper, we analysed many encryptions techniques of digital image utilizing multiple chaotic map methods of demands of security side. For the protection purpose, it is more essential or encryption of image is important method for establish protection. There is multiple encryption of image techniques scheduled, every image encryption method and decryption schemes have its own strengths and defects. In the paper, focusing on approaches to encryption of an image by chaotic map and to enhance the method to solve the major issues of encryption of image techniques by chaotic map.

Keywords: Chaotic-map based pixel abstraction, image encryption, image security, Image decryption, permutation, substitution.

1. INTRODUCTION

Internet is growing rapidly now-a-days. However, due to responsiveness and sharing vast amount of data which lacks high security of data like- image, audio, video etc. The security of image has a serious intimidation in the transmission of data onto medical imaging and military message communication. One of the profitable techniques is to obtain the multimedia data security is cryptography, which restricts the unauthorized objects of getting intimate data. It is very different encryption of text and because of some underlying properties of digital image like large amount of data in bulk and huge redundancy which are usually challenging to handle some conventional methods. Among these images stenography frequently is picked and most widespread approach since it exploits the redundancy property of image.

To overcome this obstacle, there are many modernized encryptions of image strategies recommended for on-going days, amid which is depend on chaos-based techniques emerging occur trusting direction. There are great types of image encryption schemes depended on chaotic map recommended. In this document many different image encryption designs to depend on chaotic systems have been developed. Also there are many encryption techniques that recommended for this paper. And more familiar method is used conventional method of encryption techniques to secure huge multimedia files.

Today era, the data generated consists of unstructured kind if data which includes audio and video. The protection for audio and video data becomes very important from today view. Today videos conferencing, image sharing, exclusively increasing due to wide use of internet world wide. But, the protection for such unstructured data is highly crucial as it is in large quantity. In unstructured data production we also give attention to confidentiality as well as sharing among such data, this includes very high confidential data like in military, medical, secret nation's records and strategies.

For security of unstructured of data couple of steps scheme are expanded and used mostly. First step consists of stability while encrypted data, for this a key technique is important for

Decryption of data. A second step consists of security of data when it travels through digital world. There is dependency on these two. So conclusively we securely focus on encryption and decryption of unstructured data. We concern on sharing-transfer of unstructured data such that while transferring it convert into an unreadable complex so that it decryption by unauthorized parties is minimized. Image encryption concern to manufacturing of an unstructured data such that while transferring the data it becomes invisible, complex and unreadable. So it becomes hardly decrypted. While transferring in unsure medium i.e. Internet it becomes protective and on destination it again comes in its original form so that the receiver gets the secured and consistent data. In that the key used are same for both encryption and decryption technology so the key is only known by the sender and receiver. This kind of cryptography is called private cryptography.

The common techniques used for a pixel block are substitution and permutation. In substitution technique we restore a pixel with another pixel that's by this is called substitution. In permutation technique the modification is done on sequence of a pixel in a block.

In the modern era there is a flood of using internet and surely increasing day by day, internet is highly used for communication of data or we can say that in internet the communication with data is done. Moving forward in this direction the question arises the security of data over internet. The use of unauthorized way increases the fraud and out of control dissemination of data.

Chaotic map gathers a wide attention to recent time for image encryption. The use of chaotic map concern in image encryption as well as permutation-substitution technique. In this two processes repeated several rounds to get the final encrypted image. An article written by Fridrich concerned to chaotic image encryption operation composed of permutation and substitution. In this article, pixels are travelling by use of 2D chaotic map. The new pixels are taken as permutation of original pixel. In substation technique the value of pixel is altered sequence. In this article, Fridrich introduced the operation of image encryption technique by chaotic map is composed the method of permutation and substitutions process, the sequence is generated by altered the changing the position of pixel sequentially. There is various technique of chaotic map and they are followings:

- Arnold 3D cat maps of A three-dimensional
- A Baker 3D map
- A pixel positions permutation of 2D cat map

2. REMARKABLE PROPERTIES OF CHAOTIC MAPS

A. Lengthwise Assessment of key

The key measurement of the key are held lengthwise operations in the huge amount of cryptographic [1], is an essential protection specification. In the confidential and intellectual organization is mentored and approximate key size should be minimum for constraint for security purpose. Both intellectuals and confidential organizations provide guidance and mathematical approach to provide approximate the minimum key size constraint for security purpose. In the process are unable to choose the size of key is an applicable to provide the confidentiality to secure the various kinds of attacks.

B. Sensitivity of Information

A suitable algorithm of encryption is to be conscious of a secret key. A negligible change of secret key to among development of decryption consequence of an absolutely recognizable decrypted image. Sensitive information illustrates as data that is perpetuating opposite to trivial disclosure. To approach the sensitive information should be sheltered. Preservation of sensitive information may be involuntary for ethical logic or legal, for involvement pertaining to individual privacy and for recovery concentration. Sensitive Data comprises all information, in its duplicate form and authentic, which consist of Personal Data, Customer record data, Student education records and Customer record information, Protected Health Data, Card holder data.

C. Profitable Generation of the Key Approach

It concerns to the outlook of image, the protection for any lock is meaningless until the key to unauthorized hand. To retain the confidentiality of key approach is based on generation of key is encrypted attentively crucial. In inspection of image encryption approach and key generation technique should be analyzed by the security of image agreement. In this article, it is necessary to evaluate multiple techniques of image encryption are probable to lock a person outside the approach from their information forever. There can be discussion of key and it should be abolished. A key abrogation method is mandatory. A process and method to evaluate of the information of key settlement to encrypt through a recent method of key should be perceived. The encryption schemes for data are necessary personals, when there is danger that information is not applicable, is done by institutional approach, by informing the authorities. A standard occurs management of key for utility that is prescribed for individuals to make usage of the mode and an exception of a file.

D. Ergodicity

Chaos based techniques had been various properties, such as unpredictability, ergodicity, mixing and the initial conditions is sensible, is linked up dignified diffusion and confusion characteristic of conventional cryptography. To retain, the cryptography has assigned a diffusion technique for the capacity of the deviation from the single bit plaintext (i.e. messages) of influence realistically every cipher-text bits (i.e. confidential messages). Now, the confusion assures that bits of cipher-text are obnoxiously blended. The parallel between the approaches to chaos theory is those notorious chaos characteristics: physically potent topological transitivity and sensitivity to initial conditions.

Chaos in situation is interdisciplinary which widely covers engineering, mathematics, physics, and etc. So this assigns to the approach to confusion and diffusion, and may be linked in underlying characteristic of chaotic schemes like sensitivity and erotic for initial conditions. Recognize that conventional cryptographic systems fundamental await on sophisticated algebraic methods. Interestingly, chaotic schemes appearance proof of pleasant complicated dynamics but exists of a comparatively simple form. In the logic, it is applicable to handle chaos theory about cryptographic form.

Chaos and Performance - In a best algorithm of cryptographic schemes suggests a good accommodation between security and performance. And "There are logically clear that someone through wonderful understanding of today cryptanalysis may prepare layout of protection yet slow algorithms by exact few exertion". There are many characteristics of chaotic are asymptotic ones; still the algorithms of cryptographic approach again and again are framed on very swift diffusion and/or confusion characteristics.

3. CHAOTIC ENCRYPTION TECHNIQUES

Due to the rigorous relationship between chaos and cryptography, the usage of chaotic maps to produce an encryption schemes has been extensively examined [2]. There are three representative ways of using chaos in an image encryption. Using chaos-based techniques as a source

to generate pseudo-random bits with desired statistical characteristic to recognize an obscure permutation operation. Using chaos-based techniques as a source to generate pseudo-random pixels with desired statistical properties to recognize a private substitution method [3, 4, 5, and 6]. Two chaotic maps are used in both permutation and substitution [7, 3, and 8].

The basic schemes to encrypt a block of symbols are confusion and diffusion. Confusion can make confusing the relationship between the plain-text and the cipher-text. Diffusion can expansion the modification throughout the whole cipher-text. Substitution, which replaces for symbol with another one, is the easiest type of confusion, and permutation that modified the sequence of the symbols in the block is the uncomplicated method of diffusion. These techniques together are still the infrastructure of encryption [9].

1) *Chaotic Permutation Approach*: In secret key cryptography permutation works as an important building block of combination of sequence generator which help in permutation of key. Firstly the key is a binary number which is similar to give key then we apply 1D chaotic map as a result a random bit strings to get produced. So through this a permutation matrix can be calculated.
2) *Chaotic Substitution Techniques:* In substitution cipher we substitute a cipher-text in the place of plaintext here blocks may be of one or several letters. On the receiver side the opposite substitution done to get a correct message. It is little bit similar with permutation cipher. In permutation cipher the plain-text is reproduced in a distinct periodical sequential manner. While in substation cipher is replaced by substation text. Here the blocks them self is de-sequenced

A permutation technique is little bit give less security then substation technique. It is easy operation to do some operation like- shift, XOR, XNOR, Add. Or a combination of these easy operations. We can also do a combination of these by using substation method. Chaotic map is used for the production of random image which is used for substation. After this a chaotic image is generated which is equal to the size of plain image substitution system diminished. The co-relation between blocks of text so that when we make histogram it seen to uniform.

4. LITERATURE REVIEW ON VARIOUS EXISTING CHAOTIC TECHNIQUE OF IMAGE ENCRYPTION SCHEMES.

In this field Jeri Fridrich [10] work. In his article he presented an encryption algorithm that changed chaotic two-dimensional maps to design new symmetric block encryption techniques. Actually the design given by Jeri Fridrich is seen more profitable for large amount data encryption. If we keenly watch it is applicable on three dimensional data which give velocity to image encryption and also provide high security of the data. It concerns to the protection and implementation of the image.

In the reference [11] a plant image encryption uses for external key in secret cryptography which is of 18-bits and uses two chaotic logistic maps. In this article they enumerate initial constrain for the both logistic map used which is derived from external secret key which includes distinct wait age to all bit.

There are eight ways for encryption of a pixel the question arises which type of the encryption is used for the particular pixel. We can use a logistic map for deciding the kind of encryption is used for particular pixel. To make cipher is more crucial task than any other. In that the secret key is changed after encryption of the image.

In reference [12] there is a keen study of initial constraint parameter of the schemes for chaotic standard map. A number of steps together for secret key algorithm.

In reference [13], there is a suggestion for lossless symmetric image encryption. In this encryption the cipher basically based on substitution diffusion architecture which broadly uses chaotic standard and logistic map. It is designing mainly for colored image which consists of 3D image

In reference [14] there is a planning for encryption of new image. In this scheme an improbable chaotic sequence is generated then it is used of binary sequence again. Accordingly this binary sequence, Image pixel are recognized. The steps of this algorithm are –

1) Here firstly determine the chaotic system and its initial point namely x [0], iteration number, row size and column size N on image
2) Produces chaotic sequence from chaotic sequence
3) Produce a binary sequence
4) In this last step we include special function to recognize image pixel

In reference [15], algorithm of image encryption through structure of joining permutation and diffusion are composed. First step of the process, plain-image is separate into 8×8 pixels blocks. The goal for modern outlook involves:

a. In the conveniently abbreviate pseudorandom sequence is valuable in the chaotic system
b. For fast encryption methods perform together diffusion and permutation

After these process, chaos is used to blocks shuffle and this time, for modify values of pixel ahead its block.

In this article [13], the proposed techniques of image encryption are represented an initial condition of a key to a parameters interdependent to short permutation matrices and chaotic map. There are two methods of encryption and decryption, it's an ordinary scheme by combining several small permutation matrices for producing a large permutation matrix M built, through a chaotic map is composed nonlinearly. The nature of chaos is random like conveniently dissemination by using permutation matrix into encrypted images.

In the following paper, Yong Zhang proposed the approach from an image encryption is using chaotic map based on a pseudorandom permutation and in the image cryptosystem recently-proposed analysis [16]. To enhanced operation justified to occur safe opposite to most ordinary attacks like differential, brute-force attacks and statistical. In secret key is explained for the initial conditions for a chaotic map like logistic map and the parameters related to small permutation matrices M1, M2, • • , MN. The small permutation matrices produced through logistic map are integrated into a huge permutation matrix M. In the article, while the algorithm of image encryption proposed to [16] may apparently to be great concept.

In this article [16], a technique of rapid encryption of an image and authentication techniques are produced. Thus precise here, we are introduced the key hash function and brought to produce both a value of 128-bit hash and plain-image. The role of production of key plays by the hash values for encryption and decryption. While the protection for hash keys is requirement to provide authorization for the image decrypted. Legitimate protection accomplishment is carrying out of the one only complete round.

In this paper [17], Kamlesh Gupta1*, Sanjay Silakari2 is proposed a technique of which is retrieved by traditional approach for utilizing the method of diffusion or confusion which supports a same of cascading and 3D cat map. And generates template for diffusion utilizing to rotate image and 3D standard map through uses horizontally and vertically green or red plane for image input. Image executing XOR method of shuffle image and diffusion templates. Then produces new cipher image fast with and great security. Thus the recent cipher-image actually accomplished potentials image encryption method of realistic image [17].

In the article [18], here we point out that the changed technique is still unsure about the same known chosen plaintext attack. In aggregation, some other privacy bugs existing in both the original and the changed techniques are also reported.

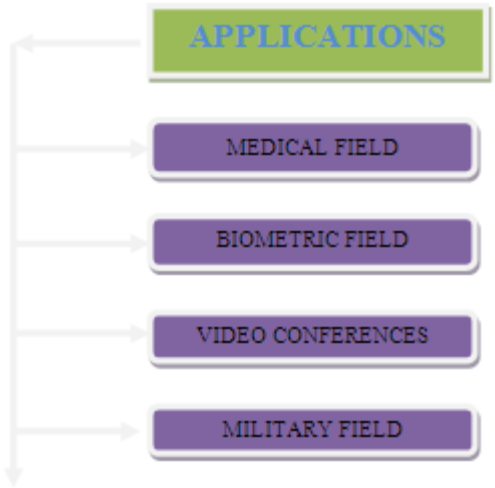
In addition, two more security faults on both the original and the changed image encryption techniques are precise in this algorithm:

·Unsatisfactory randomness of a PRNS involved.

·Unsatisfactory sensitivity with respect to modified of plain-image.

5. APPLICATION FOR TECHNIQUES OF IMAGE ENCRYPTION.

In image encryption techniques [12] perform analysis and find the need of variety of image data in various application and these are followings:



Protection For Various Images Of Medical: - In the security of image, medical images is play a vital role to create the optimal identification. The medical image analysis by physicians and add clarification and opinions. A second assessment in order to achieve by a physician of an obscure area, physician must have given the special privileges' for accessing the system with the report of internet and images of patient. In this many the outside physicians is providing arbitrary permission to use their accounts for accessing the system. In the distributing system are increasing now days and protection of patient information is not properly done. And we loss the information about patients.

In this the survey on image, diagnosis comments and record, the physician survey on the image, diagnosis comments, record's the clarification, embeds the features of the image, and for transition of image in the communication channel, that image with the Internet to another physician. When the patients checked by the physician. They are frequently needing of specialist opinions, and multiple possibly solution to provide the patient image along with the specialist report disseminate in the communication channel and so on, inspection is a potential risk and communication channel are complex. Because of this we faced through a problem of real protection when sending data. In the medical image for principled reasons are providing explanations, which cannot be dispatch when such kind of danger is existing and provide a superior protection.

Encryption is the perfect form of security in cases such as this.

The insurance companies and medical providers of the Healthcare Insurance Portability and Accountability Act (HIPPA) implemented approaches and schemes to rescue from harm patients information by medical information. Confidential data is protecting from the communication channel by ensuring regions of particularly addressed incorporate into electronic transmission and the authorized human resources is accessing the information is limited.

Biometric Security: - In the future the multimedia of internet application is absolutely mandatory encryption. To identify the unauthorized entity by password codes will just likely be exchanged by biometric images of retinal scans and fingerprints (over password and the login ID) of the forthcoming. In the other side, that data will probably deliver to the network. When images are delivered into the relation set of the communication channel. An eavesdropper may reroute or replica the data by its own changing information or data. The content has substantial degree of attached the protection by encrypting these images.

Video Conferences: - Video Conferences is the most ordinary used in the education field, and used in a huge amount of applications. In the video conferences support human being for opportunity is review cooperate by process of two–way communication.

Video conferencing is also used in Tele-nursing and Telemedicine and applications like consulting, medical images transmissions, diagnosis and so on. And also utilized through the business associations, and replaces the definite remote participants of physical presence. That by travel time and cost is reduced. The video conferences are essential in judicial system. Video conferencing system is begun to install by a number of countries in courthouse and jail. In the security risk is associated with reducing the security risks of handling defendants and transporting

Military Communication: - In the Indian authority is reasonable for confidential images capture through Sukhoi-

30 MKI camera and satellite is used for securely transmission information sent by the fighter planes. In the geographical area of military image must be secured or essential which equate to crucial systems component. Data onto defense is usually replaced by the internet. Highly protective data with providing in transmission and need to protect data are restricting from the intruders.

In the modern era is utilizing the surveillance for animals in the border. The schemes are to dilemma to camera is automatically in animals eyes and utilize that images for capturing the image immediate the objects. These images may comprise of:

· Soldiers position.

· Terrorist position.

6. SUMMARY

In the article, there are many essential current image encryption schemes represented and reviewed. Initially image encryptions methods are significant on previously existing since it is the best method to provide security of multimedia data onto example- images. When computational load is decreasing and it provides protection levels to grow fast. In this article there are various exiting techniques achieved only medium to low level of protection. Sensitivity of key size, statistical, key space is verifying the protection of image. In this paper, these schemes are emphasis on chaotic system based techniques. Because of these techniques, systems will enhance encryption algorithm and provide the protection level high with using chaotic map characteristics. In the chaotic maps computing economic and very swift. On survey of miscellaneous cryptography techniques of chaotic map are examined and calculation of the production in this criteria for example- protection of key space, key sensitivity, speed and correlation coefficient. In this article, previously existing algorithm of image encryption reviewed.

7. REFERENCES

[1]. Y. V. Mitra, S. Rao, and S. R. M. Prasanna, “A new image encryption approach using combinational permutation techniques,” International Journal of Computer Science, vol. 1, no. 2, pp. 127–131, 2006.

[2]. B. Furht and D. Kirovski, Multimedia Security Handbook, CRC Press, Boca Raton, Fla, USA, 2005.

[3]. Q. Zhou, K.-W. Wong, X. Liao, T. Xiang, and Y. Hu, “Parallel image encryption algorithm based on discredited chaotic map,” Chaos, Solitons & Fractals, vol. 38, no. 4, pp. 1081–1092, 2008.

[4]. L. P. L. de Oliveira and M. Sobottka, “Cryptography with chaotic mixing,” Chaos, Solitons & Fractals, vol. 35, no. 3, pp. 466–471, 2008.

[5]. S. Lian, J. Sun, and Z. Wang, “Security analysis of a chaos-based image encryption algorithm,” Physical A, vol. 351, no. 2–4, pp. 645–661, 2005.

[6]. W. Yuanzhi, R. Guangyong, J. Julang, Z. Jian, and S. Lijuan, “Image encryption method based on chaotic map,” in Proceedings of the 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA '07), pp. 2558– 2560, 2007.

[7]. S. Lian, J. Sun, and Z. Wang, “A block cipher based on a suitable use of the chaotic standard map,” Chaos, Solitons & Fractals, vol. 26, no. 1, pp. 117–129, 2005.

[8]. A. N. Pisarchik and M. Zanin, “Image encryption with chaotically coupled chaotic maps,” Physical D, vol. 237, no. 20, pp. 2638–2648, 2008.

[9]. G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[10]. Jeri Fridrich, “Image Encryption Based on Chaotic Maps”, Proceeding of IEEE Conference on Systems, Man, and Cybernetics, pp. 1105-1110, 1997.

[11]. N.K. Pareek., Vinod Patidar., K.K. Sud. :Image encryption using chaotic logistic map. Image and Vision Computing 24, PP. 926–934 (2006).

[12]. “Application of Image encryption” Journal of Information Systems and Communication, www.bioinfo.in ISSN: 0976-8742 & E-ISSN: 0976-8750.

[13]. Shubo Liu1., Jing Sun., and Zhengquan Xu1: An Improved Image Encryption Algorithm based on Chaotic System. Journal of Computers, Vol. 4, No. 11 (2009)

[14]. Jui-Cheng Yen, Jiun-In Guo, “A new chaotic image encryption algorithm“,Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[15]. A fast image encryption and authentication scheme based on chaotic maps. Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei, 2010

[16] Nanchang, P. R. China, "An image encryption scheme with a pseudorandom permutation based on chaotic maps" 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference

[17] Kamlesh Gupta1*, Sanjay Silakari2, "New Approach for Fast Color Image Encryption Using Chaotic Map” journal of Information Security, 2011, 2, 139-150 vol-12

[18]. Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps, Chengqing Li, Shujun Li, Kwok-Tung Lo, 2010