



www.ijarcsse.com

## Survey Report: on Various Existing Chaotic Schemes

Atul Kumar Gupta

IT Department-LNCTS Bhopal,

RGPV University, INDIA

---

**Abstract** — A number of image encryption schemes have been anticipated in modern years for image security over the network for the development of military, government and medical applications. In this paper, we review digital image encryption scheme using various chaotic map with an exacting focus on security aspects. As per security concern, security is an important issue, and encryption is one of the ways to ensure security. So many image encryption schemes have been proposed, each one of them has its strength and flaws. In this manuscript we are emphasis on image encryption using chaotic map in spatial domain only.

**Keywords** — Image encryption Scheme, Information security, Image cryptosystem.

---

### I. INTRODUCTION

In the recent years security of image and video data has become more and more important for many applications including video conferencing, protected exact copy, medical and military applications. Two most important collections of technologies have been extended for this reason. The first group is content protection through encryption, for which a key scheme is required for proper decryption of the data. The second group is digital watermarking technique, which aims to push in a message into the multimedia data. These two technologies could be used complementary to each other [1, 2]. So we focus only on key scheme method for image encryption and decryption of the data. In secured exchanges of message into the multimedia data using encryption, which is focus of the present work, the information under deliberation is converted from the comprehensible form to an unreadable structure using certain operations at the transmitter.

Data encryption is essentially scrambling the content of data, such as text, image, audio, and video to make the data scrawled, invisible or indecipherable during transmission. The unintelligible or encrypted form of the information is then transmitted through the insecure channel, i.e. (**internet**) to the destination. At the anticipated receiver side, still the information is again converted back to an comprehensible form using decryption operation and consequently the information is conveyed securely. It should be well-known that the same keys show both these encryption and decryption operations. Such encryption system is grouped under private key cryptography [1, 3].

The elementary techniques to encrypt a block of pixels are substitution and permutation. Substitution replaces a pixel with another one; permutation changes the sequence of the pixels in a block to make them indecipherable.

The recent advances in technology, particularly in computer industry and communications, allowed potentially huge market for distributing digital multimedia content through the Internet. On the other hand, the digital documents, image processing tools and the global availability of Internet way has created an ideal medium for copyright fraud and out of control distribution of multimedia such as image, text, audio, and video content.

In recent years, chaotic maps have been employed for image encryption. Most chaotic image encryptions (or encryption systems) use the permutation-substitution architecture. These two processes are repeated for several rounds, to obtain the final encrypted image. For example, in [4], Fridrich suggested a chaotic image encryption method composed of permutation and substitution. All the pixels are moved using a 2D chaotic map. The new pixels moved to the current position are taken as a permutation of the original pixels. In the substitution process, the pixel values are altered sequentially. Chen et al. employed a three-dimensional (3D) Arnold cat map [5] and a 3D Baker map [6] in the permutation stage. Guan et al. used a 2D cat map for pixel position permutation and the discretized Chen's chaotic system for pixel value masking [7]. Lian et al. [8] used a chaotic standard map in the permutation stage and a quantized logistic map in the substitution stage. The parameters of these two chaotic maps are determined by a key stream generated in each round. Mao et. al. construct a new image encryption scheme based on the extended chaotic Baker map [6]. Zhang et al. first permute the pixels of images with discrete exponential chaotic map, and then use "XOR plus mod" operation for substitution [9].

### II. SIGNIFICANT PROPERTIES OF CHAOTIC MAPS

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

#### A. Key Measurement Lengthwise

In a large amount of cryptographic functions, the key measurement lengthwise is an important security parameter. Both intellectual and private organizations provide recommendations and mathematical formulas to approximate the minimum key size constraint for security. So we require to choosing an appropriate key size to protect your system from various attacks.

### B. Sensitivity

An well-organized encryption algorithm should be sensitive to secret key i.e. a small change in secret key during decryption process results into a completely different decrypted image. Sensitive data is defined as information that is protected against unnecessary disclosure. Access to sensitive data should be shielded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive Information includes all data, in its original and duplicate form, which contains: Personal Information, Protected Health Information, Student education records, Customer record information, and Card holder data.

### C. Valuable Key Generation

It is just like physical security, the strongest lock is useless if the keys are left under the spineless person. Security of the key management process for encryption keys is especially important. Together with the review of the encryption method, key generation methods must also be reviewed in coincidence with the Information Security.

It is essential to recognize that many encryption algorithms have the potential to lock a person out of access to their data permanently. Also, keys may become compromised, and must be revoked. A process for key revocation is essential. A plan and process for movement of all data encrypted with a compromised key to encryption with a new key must be recognized.

The use of encryption methods for data at rest by individuals, where there is a risk that information would not be available, should be done according to institutional policy, normally only with informed authority. If an standard service exists for key management, it is recommended that individuals make use of that means, or file an exception.

### D. Ergodicity

Many characteristics of chaos, such as ergodicity, mixing, unpredictability and the sensitivity to initial conditions, can be connected with the distinguished confusion and diffusion properties in the traditional cryptography. More specifically, the diffusion is referred in the cryptography as the capability of the variation of a single bit in the plaintext (i.e. the message) to affect practically all bits of cipher-text (i.e. the encrypted message). At the same time, the confusion ensures that bits of cipher-text are offensively mixed. The analogues of these concepts in chaos theory are those famous chaos properties: physically powerful sensitivity to initial conditions and topological transitivity.

## III. ELEMENTARY AREA OF CHAOTIC CRYPTOGRAPHY

Chaos in environment is multidisciplinary which broadly covers physics, mathematics, communications, engineering and so on. So this refers to the concept of confusion and diffusion, which can be connected to the elementary properties of chaotic systems such as ergodic and sensitivity to initial conditions. Remember that traditional cryptographic schemes mainly rely on complicated algebraic operations. Interestingly, chaotic systems show evidence of attractive complex dynamics but exist in a relatively simple form. In this logic, it is practicable to employ chaos theory in cryptographic aspect.

Chaos and Performance - A good cryptographic algorithm offers an best trade-off between security and performance. "It is reasonably clear that someone with a good understanding of present day cryptanalysis can design secure but slow algorithms with very little effort". The properties of chaotic systems are asymptotic ones; however the cryptographic algorithms frequently are built on very rapid diffusion and/or confusion properties.

### A. Chaotic Encryption Scheme

Due to the rigid relationship between chaos and cryptography, the use of chaotic maps to construct an encryption system has been extensively investigated [12]. There are three representative ways of using chaos in an image encryption. Using chaos as a source to generate pseudo-random bits with desired statistical properties to realize a secret permutation operation [6, 7, 13]. ( ) Using chaos as a source to generate pseudorandom pixels with desired statistical properties to realize a secret substitution operation [5, 14–16]. Using two chaotic maps in both permutation and substitution [8, 10, 11].

The basic techniques 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 extend the change throughout the whole cipher-text. Substitution, which replaces a symbol with another one, is the simplest type of confusion, and permutation that changes the sequence of the symbols in the block is the simplest method of diffusion. These techniques together are still the foundations of encryption [3].

1) *Chaotic Permutation* : To designing the private key cryptographic techniques, permutation methods are considered as important building blocks in conjunction with pseudorandom sequence generators for selecting a specific permutation key. First, a Key-P is entered as a binary number equivalent to the given key. Then, a 1-D chaotic map generates a random bit-string. Consequently, a permutation matrix for the system is calculated.

A permutation matrix is an individuality matrix with the rows and columns interchanged. It has a single in each row and column; all the other elements.

2) *Chaotic Substitution*: In Cryptography a substitution cipher is a method of encryption by which blocks of plain text are replaced with cipher-text according to a usual system; the blocks may be single or several letters. At the receiver decipherers using these text by performing an inverse substitution. Substitution ciphers can be compared with permutation ciphers. In a permutation cipher, the blocks of the plain-text are rearranged in a different and frequently quite complex order, but the blocks themselves are left unchanged. By contrast, in a substitution cipher, the blocks of the plain-text are retained in the equivalent sequence as in the cipher-text, but the blocks themselves are distorted.

A permutation-only encrypted system is lacking confidence adjacent to attacks [17]. To get better the security, substitution process is added to the encryption system. The substitution could be one of simple operations such as XOR, XNOR, shift, Add, and/ or a combination of these simple operations. Chaotic map is used as generation of pseudo-random image for substitution. Actually, chaotic image with a size equal to plain-image is generated. All pixels of permuted image and new chaotic image are combined with modular addition. Substitute function decreases the correlation between blocks or samples in text and makes its histogram uniform.

#### **IV. LITERATURE SURVEY ON VARIOUS EXISTING CHAOTIC SCHEME OF IMAGE ENCRYPTION SCHEMES IN SPATIAL DOMAIN TECHNIQUES**

##### **A New Block Image Encryption Algorithm by Fridrich, 1997 .**

Jiri Fridrich [25] presented an encryption algorithm that modified assured invertible chaotic two-dimensional maps to create new symmetric block encryption schemes. Basically this design is especially useful for encryption of large amount of data, (i.e.digital images).

- It is more extended to be three-dimensional and then used to speed up image encryption while retaining its high degree of security.
- It may illustrate along with its security analysis and implementation.

##### **Image encryption using chaotic logistic map by N.K. Pareek, Vinod Patidar, K.K. Sud, 2006.**

The proposed image encryption scheme [19], an external secret key of 80-bit and two chaotic logistic maps are in use. Here they specify the initial conditions for the both logistic maps are derived using the external secret key by providing different weight age to all its bits.

- Eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map.
- To construct the cipher more robust against any type of attack, the secret key is modified after encrypting each block of sixteen pixels of the image.

##### **A new substitution–diffusion based image cipher using chaotic standard and logistic maps by Vinod Patidar, N.K. Pareek, K.K. Sud , 2008 .**

The proposed image encryption scheme [20] has describe the initial condition, system parameter of the chaotic standard map and number of iterations together constitutes the secret key of the algorithm.

##### **A new substitution–diffusion based image cipher using chaotic standard and logistic maps, 2008.**

In this paper [22], Here they have propose a new loss-less symmetric image cipher based on the extensively used substitution–diffusion architecture which utilizes chaotic standard and logistic maps. It is specifically designed for the colored images, which are 3D arrays of data streams.

##### **A New Chaotic Image Encryption Algorithm, 2008.**

Jui-Cheng Yen and Jiun-In Guo [21] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps.

**Step-1** Determines a chaotic system and its initial point  $x(0)$ , row size  $M$  and column size  $N$  of the image  $f$ , iteration number  $no$ , and constants  $k$ , and  $\mu$  used to determine the rotation number.

**Step-2** Generates the chaotic sequence from the chaotic system.

**Step-3** Generates the binary sequence.

**Step-4** It includes special functions to rearrange image pixels.

##### **A new chaos-based fast image encryption algorithm, 2009.**

In this paper [24], an image encryption algorithm with the architecture of combining permutation and diffusion is proposed. Firstly the plain-image is partitioned into blocks of  $8 \times 8$  pixels. The objectives of this new design include: (i) to efficiently take out good pseudorandom sequences from a chaotic system and (ii) to concurrently perform permutation and diffusion operations for fast encryption.

- First, the image is partitioned into blocks of pixels.
- Chaos is employed to shuffle the blocks and, at the same time, to change the pixel values along its block .

##### **An image encryption scheme with a pseudorandom permutation based on chaotic maps, 2010.**

This proposed encryption scheme [26] is defined a key as an initial conditions for a chaotic map and parameters interrelated to small permutation matrices. In both encryption and decryption, there is a common process to generate a large permutation matrix  $M$  built by combining several small permutation matrices, which are nonlinearly generated with a chaotic map.

- The random-like nature of chaos is efficiently spread into encrypted images by using the permutation matrix.

##### **A fast image encryption and authentication scheme based on chaotic maps, 2010.**

In this paper [24], a fast image encryption and authentication scheme is proposed. In exacting here, a keyed hash function is introduced to generate a 128-bit hash value from both the plain-image and the secret hash keys.

- The hash value plays the role of generation of key for encryption and decryption while the secret hash keys are used to authenticate the decrypted image.
- Reasonable security performance is achieved in only one overall round.

#### **Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps, 2010.**

In this paper [23], Here we point out that the modified scheme is still insecure against the same known/chosen-plaintext attack. In accumulation, some other security defects existing in both the original and the modified schemes are also reported.

In addition, two more security weaknesses of both the original and the modified image encryption schemes are extracted in this algorithm:

- Unsatisfactory randomness of a PRNS involved.
- Unsatisfactory sensitivity with respect to change of plain-image.

#### **V. APPLICATION OF IMAGE ENCRYPTION SCHEME.**

For studying image encryption scheme [18], the use of image and text data in a variety of application are as follows:

**Biometric Security:-** Image encryption, certainly is necessary for future multimedia internet application. Password codes to recognize entity's user will likely be replaced with biometric images of fingerprints and retinal scans (over the login ID and password) in the upcoming. On the other hand such information will apparently be sent over a network. When such images are sent over a set of connections of communication channel, an eavesdropper may replica or reroute the information by its own modifying data or information. By encrypting these images, the content has substantial degree of added security.

**Security in Medical Images:-** The medical images are playing an important role in making optimal identification. Physicians analyze the medical images and add clarification and opinions. In order to acquire a second opinion from a physician in a distant area, he should have the privilege to access the system by Internet for the patient images and reports. It may be unreasonable consent to many outside physicians have their accounts to access the system. This increases the consignment on the system and would injure patient information security.

The physician analyses the image, records the clarification and diagnosis comments, inserts the details into the image, and then transmits over the communication channel, that image through the Internet to another physician.

When a physicians receives a visit from a patient. He repeatedly requires specialist opinions before giving a diagnosis, one possible solution is to send images of the patient along with a specialist report transmit over the communication channel even so, communication channel are difficult and surveillance is a potential risk we are for that reason faced with a real security problem when sending data. For principled reasons, medical images description cannot be sent when such a risk is present and has to be superior protection.

Encryption is the best form of protection in cases such as this.

The Healthcare Insurance Portability and Accountability Act (HIPPA) requires that medical providers and insurance companies implement procedures and policies to save from harm patient's through medical information. A regions to be particularly addressed incorporate ensuring that confidential data is secured over the communication channel during electronic transmission and that access is limited only to authorized human resources.

Our goal is to design a security to shield patient information while making the information readily accessible when necessary. The design of security was motivated by the following points:-

1. Now-a-days, the patients information is frequently printed in the area of the medical images for screening, as a significance it is easily accessible to everybody.
2. The patient's information highly displayed may be intercepted by a third party during confidential data is secured over the communication channel during electronic transmission. Sometimes, this could cause big regulation ensembles.
3. For those scenarios such as medical imaging research, the patient information should not be accessible from unauthorized person.

For diagnosis purposes, the patient information needs to be enthusiastically easy to get the doctors.

**Military Communication:-** The Indian authority are concerned that state-of-the-art images caught by the camera of Sukhoi-30 MKI fighter planes needs to be sent securely through the satellite. The images include protected geographical area of military importance or drawings which correspond to critical components of system.

Defense information is routinely exchanged through internet. It is necessary to provide a highly secure transmission so as to prevent the data from intrusion.

The recent trend is to use the animals for surveillances at the border. The procedure is to fix the automatic camera in the eye to animals and use them to capture the images of the nearby objects. These images may constitute:

- Position of the soldiers.
- Position of the terrorist

These transmission, being wireless can be intruded by any third party, so it is mandatory to make it secure by some form of encryption.

Reliable image encryption technique is of utmost importance for the protection of data from counterfeiting, tampering, and unauthorized, access and fraud.

**Video Conferences :-** Video Conferences is implemented in a wide range of applications, of which most common in the field of education. Video conferences provide students with the opportunity to learn by participating in a two-way communication process.

Another common application of video conferencing is in Telemedicine and Tele-nursing application such as diagnosis, consulting, transmission of medical images etc.

It is also used by the business community as; it substitutes the actual physical presence of the remote participants thereby reducing the travel cost and time.

The video conferences are useful in judicial system. A number of countries have begun to install video-conferencing system in jails and courthouse. It reduces the security risks associated with transporting and handling defendants.

Video conferencing can also be used as a one – way monitoring technology to continuously monitor the remote site, like Railways station, airport, temple, parliament house, cinema hall, Historical places, hotels etc. The cameras are available today with features like Auto-tracking, Auto-signaling.

So, it is necessary to provide security in video conferencing transmission over network. It can be realized by encrypting the video, still images transmission from the surveillance device to the destination.

## VI SUMMARY

In this paper, many of the current important image encryption techniques have been presented and analyzed. Initially here to emphasis on already existing image encryption algorithms because the best way of protecting multimedia data like images. To reduce the computational load, and yet keep the security level high. Many of the proposed schemes could only achieve moderate to low level of security. Security verifies on its size of key space, key sensitivity, statistical. In this report, we emphasis on those techniques which are based on chaotic systems on spatial domain only, because these systems will improve the security level of encryption algorithm by using chaos properties. Chaotic maps computationally economic and fast. In this review paper various chaotic cryptography schemes are studied and their performance is evaluated on these criteria: security key space, key sensitivity, correlation coefficient and speed. In this survey report, already existing image encryption algorithms have been discussed.

## 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]. D. Van de Ville, W. Philips, R. Van de Walle, and I. Lemahieu, "Image scrambling without bandwidth expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 6, pp. 892–897, 2004.
- [3]. M. Yang, N. Bourbakis, and S. Li, "Data-image-video encryption," *IEEE Potentials*, vol. 23, no. 3, pp. 28–34, 2004.
- [4]. J. Fridrich, "Image encryption based on chaotic maps," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1105–1110, 1997.
- [5]. 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.
- [6]. Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.
- [7]. Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1–3, pp. 153–157, 2005.
- [8]. 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.
- [9]. L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.
- [10]. Q. Zhou, K.-W. Wong, X. Liao, T. Xiang, and Y. Hu, "Parallel image encryption algorithm based on discretized chaotic map," *Chaos, Solitons & Fractals*, vol. 38, no. 4, pp. 1081–1092, 2008.
- [11]. A. N. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D*, vol. 237, no. 20, pp. 2638–2648, 2008.
- [12]. B. Furht and D. Kirovski, *Multimedia Security Handbook*, CRC Press, Boca Raton, Fla, USA, 2005.
- [13]. J.-C. Yen and J.-I. Guo, "A new chaotic key-based design for image encryption and decryption," in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS '00)*, vol. 4, pp. 49–52, Geneva, Switzerland, May 2000.
- [14]. L. P. L. de Oliveira and M. Sobottka, "Cryptography with chaotic mixing," *Chaos, Solitons & Fractals*, vol. 35, no. 3, pp. 466–471, 2008.
- [15]. S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physica A*, vol. 351, no. 2–4, pp. 645–661, 2005.

- [16]. 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.
- [17]. S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, pp. 133–167, CRC Press, Boca Raton, Fla, USA, 2004.
- [18]. "Application of Image encryption" *Journal of Information Systems and Communication*, www.bioinfo.in ISSN: 0976-8742 & E-ISSN: 0976-8750.
- [19]. N.K. Pareek., Vinod Patidar., K.K. Sud.,:Image encryption using chaotic logistic map. *Image and Vision Computing* 24, PP. 926–934 (2006).
- [20]. A new substitution–diffusion based image cipher using chaotic standard and logistic maps by Vinod Patidar, N.K. Pareek , K.K. Sud ,2008
- [21]. 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.
- [22]. Shubo Liu1., Jing Sun., Zhengquan Xu1.,:An Improved Image Encryption Algorithm based on Chaotic System. *Journal of Computers*, Vol. 4, No. 11 (2009)
- [23]. Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps, Chengqing Li, Shujun Li, Kwok-Tung Lo, 2010
- [24]. A fast image encryption and authentication scheme based on chaotic maps.Huaqian Yang,Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang,Pengcheng Wei ,2010
- [25]. Jiri Fridrich, "Image Encryption Based on Chaotic Maps", *Proceeding of IEEE Conference On Systems, Man, and Cybernetics*, pp. 1105-1110, 1997.
- [26]. An image encryption scheme with a pseudorandom permutation based on chaotic maps .Ji Won Yoon a, Hyounghick Kim, *Commun Nonlinear Sci Numer Simulat* xxx (2010).