*International Journal of Innovation Sciences and Research*
*Vol.5, No, 05, pp. 729-735, May- 2016*

***Available online at***
*http://www.ijisr.com*

# RESEARCH ARTICLE

# SURVEY OF CHAOTIC IMAGE ENCRYPTION TECHNIQUES

**[1]Brinda Devi, D. and [2*]Dr. Selva Kumar, S.**

[1]M.E. CSE (With Specialization in Networks), GKM College of Engineering & Technology, Chennai, India
[2]Computer Science and Engineering, GKM College of Engineering & Technology, Chennai, India

***Accepted 27th April, 2016; Published Online 31st May, 2016***

## ABSTRACT

Cryptography is simply the science of securing sensitive and confidential information as it is stored on media or transmitted through communication network paths. Chaotic Encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information. Chaotic Encryption Method seems to be much better than traditional encryption methods. Encryption is the method of retaining the secrecy of images. Image Encryption based on chaos became very popular, since properties are related to confusion and diffusion, two basic properties of good cipher. Chaotic methods take advantage of the more and more complex behavior of chaotic signals to reach higher performance. The confidentiality, non-repudiation, validation, reliability of the information (data or image) should be checked properly. For ensuring security, the images are encrypted by the sender before transmitting them and are decrypted by the receiver after receiving them so that only the sender and the intended persons can see the content in the image. This paper is an analytical survey of popular secured chaotic encryption techniques, where researchers can get an idea for efficient techniques to be used.

***KEY WORDS:*** Cryptography, Encryption, Chaos Theory, Chaotic Encryption, Chaotic map.

## INTRODUCTION

In current scenario, providing security to secret information is a challenging issue. The high growth in the networking technology leads to a common culture for interchanging of the data very drastically. So, information has to be protected during transmission over the internet. There are three basic methods of secured communication available, namely, cryptography, steganography and watermarking (Mitra et al., 2006). Among these three, Cryptography deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange (Elbirt and Paar, 2005; Diffie and Hellman, 2003; Stallings, 2003). Steganography is a technique for hiding and extracting information which to be conveyed using a carrier signal (Besdok, 2005; Trivedi and Chandramouli, 2005). Watermarking is a technique for hiding proprietary information in the perceptual data (Wu, 2005; Wu and Shih, 2004).

### Cryptography

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. To secure our data at the time of transmission, cryptography gives an elucidation. Cryptography derived from a Greek word called "Kryptos" which means "Hidden Secrets". The main five goals of Cryptography include privacy, Non-Repudiation, Service dependability and ease of use.

***Corresponding author: Dr. Selva Kumar, S.***
*Computer Science and Engineering, GKM College of Engineering & Technology, Chennai, India.*

### Cryptosystem

Cryptosystem is the system that provides encryption and decryption. It uses algorithm for encryption and decryption. Data is provided to the encryption system with a key. In secure mode the same key is provided to the decryption system. Finally output is obtained after decryption.

### BASIC TERMS IN CRYPTOGRAPHY

**Plain Text:** The original message which we wish to communicate with the others is defined as Plain Text. In cryptography the actual data which we send to the other is referred to as Plain Text.

**Cipher Text:** The cipher text is the message which has been converted by the encryption algorithm. In cryptography the original message is transformed into non-readable message.

**Encryption:** A process of converting plain text into cipher text is known as Encryption. Encryption algorithm and a key to send confidential data through an insecure channel is used in cryptography.

**Decryption:** It is the reverse process of encryption. In this it convert the cipher into plain text. We require encryption algorithm and a key for decryption.

### GOALS OF ENCRYPTION/DECRYPTION

**Confidentiality:** Information transmitted by the computer is accessed only by the authorized party.

**Authentication:** The identity of the sender is to be checked that whether the information is arriving from an authorized person or a false identity.

**Integrity:** To maintain the integrity of information only the authorized entity is allowed to modify the transmitted information.

**Non-Repudiation:** The term in which deny the transmission is not allowed by the sender and the receiver of message.

**Access Control:** Only the authorized parties can access the given information.

**Types of Cryptography**

Cryptography is of two types:

1. Symmetric or Secret Key Cryptography
2. Asymmetric or Public Key Cryptography

In Symmetric key cryptography, both the sender and receiver know the same secret code called key. In this cryptography, the sender encrypted the message using the key and the receiver decrypts it using the same key.

E.g.: Triple DES, AES, DES and Blowfish Encryption Algorithm.

In Asymmetric key cryptography, different key is used by sender and receiver for encryption and decryption. The data is encrypted by sender using a public key and this key will be known by all the parties included in the communication. The data is decrypted by the receiver using a private key and it should be reserved as a secret. E.g.: RSA.

With the rapid developments of the communications industry, a great deal of concerns has been raised in the security of data transmitted or stored over open channels. Especially on the image data. A major challenge is to protect confidentiality for image data in digital distribution networks. The remaining paper is organized as follows. In Section II, it is about Chaos Theory. In Section III, discussed about Chaotic Image Encryption. In Section IV, discussed about Chaotic Based Encryption Schemes. In Section V, discussed about Literature Review and then conclusion follows in Section VI.

**Chaos Theory**

Chaos theory is the study of nonlinear dynamical systems that are exhibit extreme sensitivity to initial conditions and have random like behaviors (Lorenz, 1993). The small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future-behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems makes them unpredictable (Kellert, 1993). This behavior is known as deterministic chaos, or simply chaos. Random like behavior, non-predictable and sensitivity to initial value are three features that make it an acceptable choice to relate it with cryptography. The only difference is that encryption operations are defined on finite sets of integers while chaos maps are defined on real numbers. Chaotic behaviors are exhibits by chaotic maps. These maps are classified by continuous maps and discrete maps. Discrete maps usually take the form of iterated functions. Iterates are similar to rounds in cryptosystems, so discrete chaotic dynamic systems are used in cryptography. Each map has some parameters that equivalent with encryption key in cryptography. There are two general ways to apply a chaos map in a cipher system: 1) using chaotic systems to generate pseudo-random key stream; 2) using the plaintext or the secret key(s) as the initial conditions and control parameters then apply some iterations on chaotic systems to obtain cipher text. The first way corresponds to stream ciphers and the second to block ciphers (Kocarev, 2001). There are two differences in characteristics between cryptography and chaos; in cryptography, the encryption operations are defined on finite sets of integers while chaos is defined on real numbers; cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic via iterations. Two general principles that guide the design of block ciphers; diffusion and confusion, which are closely related to the mixing and ergodicity properties of chaotic maps. Hence, we can use a chaotic map in image encryption because it satisfies the requirements of a good cryptosystem.

**Chaotic Image Encryption**

Many chaos-based image encryption methods have been proposed. According to the data encrypted, they are divided into full encryption and partial encryption (also called selective encryption). Moreover, with respect to the encryption ciphers, the two encryption methods above can also be further classified into block encryption and stream encryption, where compression-combined encryption and non-compression encryption are discussed according to the relation between compression and encryption (Zhaopin Su, 2012).

**Full Encryption**

In the full encryption scheme, images as binary large objects or pixels are encrypted in their entirety. Full encryption can offer a high level of security, effectively prevent unauthorized access, and is widely used nowadays. For image encryption, full encryption is often operated without any compression process. Some algorithms have been proposed based on chaotic block ciphers, and some based on chaotic stream ciphers.

**Chaotic Block Ciphers**

A chaotic map based chaotic block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length group of plain-text bits into a group of cipher text bits of the same length. The fixed-length group of bits is called a block, and the fixed length is the block size. A block cipher encryption algorithm for image might take a 128-bit block of plain-image as input, and output a corresponding 128-bit block

of cipher-image, that is, a plain-image is encrypted block by block (Zhaopin Su et al., 2012).

**Chaotic Stream Ciphers**

A chaotic stream cipher is a pseudorandom cipher bit stream (keystream) generated by a chaotic map, which is used to encrypt a plain test bit by bit (typically by an XOR operation).

**Partial Encryption**

Partial encryption, which is also called selective encryption, only encrypts part of the data. A plain-image is partitioned into two parts: sensitive data and insensitive data. Only the sensitive data are encrypted, and others are unprotected (Zhaopin Su et al., 2012).

**Chaotic System**

Chaotic system can be considered as source of randomness and chaos is randomness of a deterministic dynamical system. Mathematically, a chaotic map can be defined as

$X_{n+1} = f(X_n)$ …….(1)

Where $0<X_n<1$ and n=0,1,2…

Chaotic sequence can be used as random number sequence and spread spectrum sequence. The chaotic systems are characterized by the non-linear and unpredictable. They appear to have irregular order but infect there is a sense of order. Chaotic systems are sensitive to initial conditions; small change in starting point can cause different outcomes. Chaos has many applications in modulation, compression, and encryption. In image encryption, 1-D chaotic system using logistic maps has simplicity and high efficiency but it has weak security and small key space. Different Chaotic maps can be used for this purpose. Generally, in chaos based algorithm, pixels of image are scrambled and correlation among pixels is decreased to get encrypted image.

**Arnold Cat Map**

It was demonstrated by using an image of a cat. Arnold cat map uses the concept of linear algebra to change the position of pixels of original image. Original image is divided into blocks and then Arnold transformation is done.

Let X is a vector, $X=\begin{bmatrix} x \\ y \end{bmatrix}$ , then Arnold cat map transformation is,

$$\Gamma: \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & p \\ q & 1+q \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

Some conditions such as p and q are positive integers and

$$\begin{vmatrix} 1 & p \\ q & 1+q \end{vmatrix} = 1$$

This makes it area-preserving. Original image can be shuffled by applying Arnold map operation iteratively. But, Shuffling image can return to original form after several iterations.

**Logistic Map**

1-D logistic map is simplest non-linear chaotic system which can be defined as

$Z_{n+1} = \lambda Z_n (1 - Z_n)$ ……. (2)

Where $Z_o$ is initial condition, n is number of iterations and λ is system parameter. For $3.57 < \lambda < 4$ map is considered as chaotic. And $Z_{n+1}$ belong to (0,1) for all n, equation 1 is used to encrypt the shuffled pixels.

**Sine Map**

Sine map is defined as

$X_{n+1} = a\, x_n^2 \sin(\square\, X_n)$ …….(3)
When $X_0$= 0.7 and a=2,3, equation 2 has the simplified form. For the interval (0,1) it generates chaotic sequence.

**Tent Map**

Tent Map resembles the logistic map. It generates chaotic sequences in (0,1) assuming the following equation

$$X_{n+1} = \begin{cases} \mu Xn, & Xn < 1/2 \\ \mu(1 \quad Xn), & Xn \geq \frac{1}{2} \end{cases}$$

Where μ is a positive number and depending on its value tent map exhibit dynamic behavior ranging from predictable to chaotic.

**Circle Map**

It is defined as

$X_{n+1} = X_n + d - (c/2\square X_n) \bmod (1)$ ……(4)

Where d=0.2, c=0.5, and $X_0$ | (0,1) generates Chaotic sequence in (0,1).

**Chaotic Based Encryption Schemes**

A new encryption algorithm based on using the chaotic logistic map produced pseudo random sequence on image and makes double time encryption with improved DES. The combination of Chaos and improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption. A new image encryption scheme based on a chaotic system. It is based on power and the tangent function instead of linear function. It uses a chaotic sequence generated by chaotic map to encrypt image data with different keys for different images. Plain-image can be encrypted by the use of the XOR operation with the integer sequence. A block based transformation algorithm is used, where the image is divided into a number of blocks. These blocks are transformed before going through an

encryption process. It uses blowfish algorithm for encryption. At the receiver side these blocks are retransformed into their original position and decryption process is performed. It has the advantage of no loss of information in reconstruction of image for the encryption and decryption process. An algorithm using two chaotic systems. One chaotic system generates a chaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, using the binary stream as a key stream, random the pixel values of the images were modified. Then, the modified image was encrypted again by a permutation matrix. Two kinds of schemes based on higher dimensional chaotic maps are presented. By using a discretized chaotic map, pixels in an image are permuted in shuffling after several rounds of operations between every two adjacent rounds of permutations, a diffusion process is performed, which can significantly change the distribution of the image histogram which makes statistical attack infeasible. Image encryption scheme utilizes the SCAN language to encrypt and compress an image simultaneously. The construction of a symmetric block encryption technique based on two-dimensional standard Baker map. There are three basic steps in the method of Fridrich

- Choose a chaotic map and generalize it by introducing some parameter.
- Discretize the chaotic map to a finite square lattice of points that represent pixels.
- Extend the discretized map to three dimensions and further composes it with a simple diffusion mechanism.

A chaotic Kolmogorov-flow based image encryption technique was designed, in which whole image is taken as a single block and which is permuted through a key-controlled chaotic system. In addition, a shift registers pseudo random generator is also adopted to introduce the confusion in the data. An encryption method called BRIE based on the chaotic logistic map. The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map. An encryption method called CKBA (Chaotic Key Based Algorithm), in which a binary sequence as a key is generated using a chaotic system. The image pixels are rearranged according to the generated binary sequence and then XORed and XNORed with the selected key. An image encryption algorithm using logistic map, uses a chaotic map with suitable initial condition for varying the pixel values randomly with respect to its initial values of the original image. Next the chaotic sequences of the logistic map are used for pixel shuffling.

The algorithm uses a secret key of 32 characters (256-bits). A chaos-based image encryption scheme, in which an image is first converted to a binary data stream by masking these data with a random keystream generated by the chaos-based PRKG, the corresponding encrypted image is formed. A new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image. An Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects, consists of four chaotic maps Cross chaotic, Logistic Ikeda and Henon map and noise effects are observed on image. Firstly, they use the image encryption algorithm to convert original image to encrypted image.

Then they apply noise on the encrypted image and then decrypt cipher image with noise back to original image. They have found out that cross chaotic map showed best results than other three chaotic maps (10). A new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorentz chaotic system and the Rossler chaotic system. The image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed.

**Literature Review**

**Image encryption using chaotic logistic map, 2006**

N.K. Pareek, Vinod Patidar (2006) introduce a image encryption method using chaotic logistic map. In this paper image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weight age to all its bits. Further, in the 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 particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting each block of sixteen pixels of the image. The results show that the image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

**Image encryption with compound chaotic sequence cipher shifting dynamically, 2007**

Xiaojun Tong, Minggen Cui (2008) design a new two-dimensional chaotic function using two one-dimensional chaotic functions, and then prove the chaotic properties to a new function by choosing one of the two one-dimensional chaotic functions randomly.

**Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, 2008**

Chengqing Li, Shujun Li, Guanrong Chen, Wolfgang A. Halang (2009) design an image encryption scheme based on a compound chaotic sequence. In this paper, the security of the scheme is studied and the following problems are found: (a) a different chosen-plaintext attack can break the scheme with only three chosen plain-images; (b) there is a number of weak keys and some equivalent keys for encryption; (c) the scheme is not sensitive to the changes of plain-images; and (d) the compound chaotic sequence does not work as a good random number source.

**The Algorithm of Fractional Fourier Transform and application in digital image encryption, 2009**

Yuhong Zhang, Fenxia Zhao (2009) introduce a image Encryption algorithm using fourier transform. In this paper the matrix algorithm of discrete fractional Fourier transform is an approximate method to calculate the FrFT. But, the limitation is that, the encrypted digital Image can be decrypted by someone who attempts parameter; he may get the correct decryption digital image. In other word, this encryption can improve with more complex method as encrypt two or more digital image as one.

**Image Encryption with Discrete Fractional Cosine Transform and Chaos, 2009**

Lin Zhang, Jianhua Wu and Nanrun Zhou (2009) proposed a method for image encryption with discrete fractional cosine transform and chaos. Chaos function has extreme sensitivity to the initial conditions, the effect of image encryption with DFrCT and chaos is better than in the case of DFrCT. Due to the reality of DFrCT and the confusion properties, the proposed cryptosystem is extremely secure and the transmission of the encrypted images is fast.

**Hybrid Image Encryption Using Multi-Chaos-System, 2009**

H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu (2009) proposed this method uses hybrid encryption technique for the color image based on the multichaotic-system which combines Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) and increases the key space of images.

**Image Encryption With Multiorders of Fractional Fourier Transforms, 2010**

Ran Tao, Xiang-Yi Meng, Yue Wang (2010) proposed the another technique for image encryption using multi order fractional Fourier transform. In this paper, the encrypted image is obtained by the summation of different orders of IDFRFT of the interpolated sub images. The whole transform orders of the utilized FRFT are used as the secret keys for the decryption of each sub image. Compared with the traditional image encryption methods based on the FRFT, the method is with a larger key space and the amount of keys can be set as large as two times the amount of the pixels in the original image. In future work, one can also combine the proposed method with other image encryption methods to enhance the security system.

**Image Encryption using Discrete Fractional Transforms, 2010**

Neeru Jindala, Kulbir Singh (2010) proposed a method for image encryption using Fractional Fourier Transforms and compare the DFrFt and DFrCT and the performance of two recently proposed image encryption algorithms involving the use of discrete fractional transform. Simulation results under conditions of ideal encryption, decryption with correct and incorrect keys verify the performance of these techniques, that DFrCT is better for the encryption. Robustness of keys for decryption has also measured.

**Chaos-Based Image Encryption Algorithm Using Wavelet Transform, 2010**

Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng (2010) proposed a method Chaos-Based Image Encryption Algorithm using Wavelet Transform, in this paper the algorithm uses the wavelet decomposition concentrating image information in the high-frequency sub-band image, and then encryption is applied for the sub-band image. After a wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process is used to complete the encryption process. Theoretical analysis and experimental results show that the algorithm has an obvious increase in efficiency, as well as satisfied security.

**Double-image encryption based on discrete fractional random transform and chaotic maps, 2011**

Huijuan Li, Yurong Wang (2011) design a novel double-image encryption algorithm based on discrete fractional random transform and chaotic maps. The random matrices used in the discrete fractional random transform are generated by using a chaotic map. One of the two original images is scrambled by using another chaotic map, and then encoded into the phase of a complex matrix with the other original image as its amplitude. Then this complex matrix is encrypted by the discrete fractional random transform. By applying the correct keys which consist of initial values, control parameters, and truncated positions of the chaotic maps, and fractional orders, the two original images can be recovered without cross-talk.

**Image encryption by using local random phase encoding in fractional Fourier transform domains, 2011**

Zhengjun Liu, Lie Xu, Jingmin Dai, Shutian Liu (2012) proposed an image encryption algorithm based on fractional Fourier transform. A local random phase encoding is introduced into this algorithm. The data at the local area of complex function is converted by fractional Fourier transform.

**SD-AEI: An Advanced Encryption Technique for Images, 2012**

Somdip Dey (2012) proposed a method, SD-AEI, for image encryption, which is an upgraded module for SD-AEI combined image encryption technique and basically has three stages:

1) In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then reversed;
2) In second stage, extended hill cipher technique is applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure;

3) In third stage, the whole image file is randomized multiple number of times using Modified MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption.

**New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform, 2012**

R. Krishnamoorthi, P. Murali (2012) proposed a new hybrid-domain image encryption technique that uses the frequency-domain encryption with Discrete Cosine Transform (DCT) incorporating multi resolution approach and spatial domain for pixel shuffling. First, original image divided into significant and insignificant blocks using prewitt's edge detector operator and significant blocks are encrypted using Arnold cat map and Logistic map. Next, insignificant blocks are shuffled in the DCT domain using Arnold cat map then inverse DCT applied and pixels in the blocks are XORed with discretized output of logistic map. Finally, diffusion process is applied to get final encrypted image and the numerical simulations have demonstrated the security and robustness of the proposed encryption scheme.

**Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map, 2013**

Riah Ukur Ginting and Rocky Yefrences Dillak (2013) proposed an algorithm which relies on the RC4 Stream Cipher and Chaotic Logistic map. The proposed technique consists of three stages. In the first stage, system converts the external key into the initial value. Afterward, in the second stage, the technique applies the initial value to the Chaotic Logistic Map for engendering a pseudo random number. Afterward, in the third stage, the system XOR the byte stream of the plain image with the stream of pseudo random number for the encryption. Experimental outcomes of this encryption algorithm validate that the decryption process is the highly key sensitive.

**An Image Encryption Scheme Based on Bit Circular Shift and Bi-Directional Diffusion, 2014**

Ruisong et al. (2014) have proposed a novel image encryption based on chaotic system. This scheme utilized one tent map to generate a pseudorandom sequence and then shift the bits of the expanding 0-1 image circularly so as to shuffle the image gray values. Moreover generalized Arnold maps and Bernoulli shift maps are applied to produce two pseudo-random gray value sequences and then diffuse the gray values bi-directionally, which resisted the scheme from differential attack efficiently. The bit circular shift process and diffusion processes greatly confused the statistical nature between plain-images and cipher images. The scheme used a large key space which is useful to frustrate brute-force attack efficiently.

**A Novel Double-Image Encryption Scheme Based on Cross-Image Pixel Scrambling in Gyrator Domains, 2015**

Jun-Xi Chen et al. (2015) have proposed a novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains. The two input images are firstly shuffled by the proposed cross-image pixel scrambling approach, which can well balance the pixel distribution across the input images. The two scrambled images will be encoded into the real and imaginary parts of a complex function, and then converted into gyrator domains. An iterative architecture is designed to enhance the security level of the cryptosystem, and the cross-image pixel scrambling operation is performed to the real and imaginary parts of the generate complex encrypted data in each round. Numerical simulation results prove that a satisfactory and balanced security performance can be achieved in both channels.

**Conclusion**

Nowadays, providing security of a secret image is very important. This survey paper shows some important chaotic encryption techniques in the span of 10 years (2006-2015) and those techniques are studied and analyzed in order to make familiar with the various encryption algorithm used in encrypting the image. To sum up, all the techniques are useful for real time encryption and each technique is unique in its own way, which might be suitable for image as secret data. Every day new encryption technique is developing therefore fast, robust and secure conventional encryption techniques will work with high rate of security.

## REFERENCES

Besdok, E. 2005. "Hiding information in multispectral spatial images", Int. J. Electron. Commun. (AEU) 59, pp. 15-24, Feb. 2005.

Chengqing Li, Shujun Li, Guanrong Chen and Wolfgang A. Halang, 2009. "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence", Elsevier, Image and Vision Computing 27, 1035-1039.

Diffie, W. and Hellman, M.E. 1976. "New Directions in Cryptography", IEEE Trans. Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

Elbirt, A.J. and Paar, C. 2005. "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography", IEEE Trans. Parallel and Distributed Systems, vol. 16, no. 5,pp. 468-480, May 2005.

Huijuan Li and Yurong Wang, 2011. "Double-image encryption based on discrete fractional random transform and chaotic maps", Elsevier, Optics and Lasers in Engineering 49, 753-757.

Jun-xi Chen, Z-liang Zhu, Zhengjun Liu, Chong Fu, Li-bo Zhang and Hi Yu, 2015. "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains", Optics Express, Optical Society of America, Vol.22(6), pp. 7349-7361.

Kellert, H.S. 1993. "In the Wake of Chaos: Unpredictable Order in Dynamical Systems", University of Chicago, pp. 56-62.

Kocarev, L. 2001. "Chaos-based cryptography: a brief overview", IEEE Circuits and Systems Magazine 1(3): pp. 6-21.

Krishnamoorthi, R. and Murali, P. 2012. "A New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform", 4th International Confeence on Electronics Computer Technology, *IEEE* 2012.

Lin Zhang, Jianhua Wu and Nanrun Zhou, 2009. "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security, *IEEEE* 2009.

Lorenz, E.N. 1993. "The Essence of Chaos", University of Washington Press, Seattle, WA.

Mitra, A., Subba Rao, Y. V. and Prasanna, S.R.M. 2006. "A new image encryption approach using combinational permutation techniques", Journal of computer Science, vol. 1, no. 1, p.127, 2006.

Mona F.M. Mursi, "Image Security with Different Techniques of Cryptography and Coding: A Survey", Recent Advances in Electrical and Computer Engineering, pp. 95-101.

Neeru Jindala and Kulbir Singh, 2010. "Image Encryption using Discrete Fractional Transforms", International Conference on Advances in Recent Technologies in Communication and Computing, *IEEE* 2010.

Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C. and Wu, S.Y. 2009. "Hybrid Image Encryption Using Multi-Chaos-System", IEEE 2009.

Pareek, N.K. and Vinod Patidar, 2006. "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24, 926-934.

Ran Tao, Xiang-Yi Meng and Yue Wang, 2010. "Image Encryption With Multiorders of Fractional Fourier Transforms", IEEE transactions on information forensics and security.

Riah Ukur Ginting and Rocky Yefrences Dillak, 2013. "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Technology and Electrical Engineering (ICITEE), International Conference on 7-8 Oct. 2013, pages: 101-105.

Ruisong Ye, Shaojun Zeng, Peiqian Lun, Junming Ma and Chuting Lai, 2014. "An Image Encryption Scheme based on Bit Circular Shift and Bi-directional Diffusion", *International Journal of Information Technology and Computer Science*, pp. 82-92.

Somdip Dey, 2012. "SD-AEI: An Advanced Encryption Technique for Images", IEEE 2012.

Stallings, W. 2003. "Cryptography and Network Security", Englewood Cliffs, NJ: Prentice Hall.

Trivedi, S. and Chandramouli, R. 2005. "Secret Key Estimation in Sequential Steganography", IEEE Trans. Signal Processing, vol. 53, no.2, pp. 746-757, Feb. 2005.

Wu, Y. 2005. "On the security of an SVD-Based Ownership Watermarking", IEEE Trans. Multimedia, vol. 7, no. 4, pp. 624-627, Aug. 2005.

Wu, Y.T. and Shih, F.Y. 2004. "An adjusted-purpose digital watermarking technique", Pattern Recognition 37, pp. 2349-2359.

Xiaojun Tong and Minggen Cui, 2008. "Image encryption with compound chaotic sequence cipher shifting dynamically", Elsevier, Image and Vision Computing 26, 843-850.

Yuhong Zhang and Fenxia Zhao, 2009. "The algorithm of Fractional Fourier Transform and application in digital image encryption", IEEE 2009.

Zhaopin Su, Guofu Zhang and Jianguo Jiang, 2012. "Multimedia Security: A Survey of Chaos-Based Encryption Technology", 2012.

Zhengjun Liu, Lie Xu, Jingmin Dai and Shutian Liu, 2012. "Image encryption by using local random phase encoding in fractional Fourier transform domains" Elsevier, Optik 123, 428-432.

Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie and Zhang Yunpeng, 2010. "A Chaos-Based Image Encryption Algorithm using Wavelet Transform", *IEEE* 2010.

*******