SURVEY REPORT ON CHAOS BASED CRYPTOGRAPHY

Bhavana Agrawal*

Himani Agrawal**

ABSTRACT

In recent years, encryption technology has been developed quickly the chaos based cryptographic algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power. This paper presents survey of some encryption methods based on chaos system

Keywords: *Chaos System, Modern Cryptosystem, Encryption, Chaotic Map.*

*Department of Electronics & Telecom, Shri Shankara Charya College of Engineering and Technology, Bhilai, India.

**Assistant Professor, Department of Electronics & Telecom, Shri Shankara Charya College of Engineering and Technology, Bhilai, India.

1. INTRODUCTION

The nature of chaos has initiated a lot of interests in different engineering disciplines, where cryptography must be one of the most potential applications. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. Unlike the conventional cryptographic algorithms which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, which is crucial for multimedia data transmission over fast communication channels, such as the broadband internet communication. [1] .During this time of foundation and development, it came to mean different things, mostly depending on the implementation. So, we can speak of additive masking, chaos shift keying two-channel communication, message embedding, etc. [2]

2. CHAOS BASED CRYPTOGRAPHY

2.1 Cryptography Based on Chaotic System, 1997

Tao Yang, Chai Wah Wu, and Leon O. Chua (1997) presented a new chaos-based secure communication scheme is proposed in an attempt to thwart the attacks proposed recently. Instead of encoding the message signal in a chaotic system directly, we use two chaotic signals in our scheme. One of the chaotic signals is used to synchronize the chaotic encrypter and the chaotic decrypter. The other is used to encrypt the plain signal by using a multishift cipher scheme. Thus the transmitted signal is not used to encrypt the message and a more complicated method of encryption is used.

2.2 Secure Communication Using A Chaos System In A Mobile Channel, 1998

Jaejin Lee, Sooyong Choiw, and Daesik Hang (1998) compared three threshold techniques and show the results **of** the bit error ratio **(BER)** performance in an AWGN channel and in a mobile channel. We also compare the **BER** performance as frequency selectivity is changed. **A** drawback of the proposed system is that the optimal solution **of** the threshold value has not been found yet. The proposed secure communication system using chaotic signals is robust to mobile and AWGN channels resulting in a **good BER** performance without synchronization between the receiver and the transmitter.

2.3 Chaotic Cryptosystem, 1999

G. Alvarez et al. (1999) presented the performance of new cryptosystems based on chaotic dynamical systems properties will be examined. We will cover the latest advances in chaotic cryptography and discuss their practical uses and security levels.

2.4 A New Image Encryption Algorithm Based on Chaos System, 2003

Zhang Han et al. (2003) presented a new image encryption algorithm based on chaos system. First, deal with image using technique of permutation transform in image. Then, two-dimensional nonlinear map is utilized to circularly iterate gray value **of** pixels .The algorithm validly solves problem of failure **of** encryption owing to the self-similarity and visional physiological characteristic **of** image

2.5 Security Performances of a Chaotic Cryptosystem, 2004

V. Guglielmi et al. (2004) presented the security performances of a chaotic cryptosystem implemented on DSP. It uses one encryption scheme using the chaotic dynamics of two-dimensional noninvertible maps. The implementation of this algorithm had been realized on DSP. This realization had demonstrated first that the cryptosystem works properly, and then had shown very important computing times for brute force attacks.

2.6 Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption, 2004

Daniel Socek et al. (2004) enhanced the CKBA algorithm three-fold: (1)–we change the 1-D chaotic Logistic map to a piecewise linear chaotic map (PWLCM) to improve the balance property, (2)–we increase the key size to 128 bits, and (3)– we add two more cryptographic primitives and extend the scheme to operate on multiple rounds so that the chosen/known-plaintext attacks are no longer possible.

2.7 A Novel Approach for Designing the $-Box of Advance Encryption STD Algorithm *(AES)* Using Chaotic Map, 2005

Aha Eldin Rohiem, Suluh Elugooz, Hisham Dahshan (2005) presented the concepts of completeness and the avalanche effect were combined to define a property which was called the strict avalanche criterion. In this paper a couple chaotic system based pseudo random bit generator (CCS-PRBG) were tested using the NIST statistical tests for randomness to ensure. Two CCS-PRBG were used to design **a** chaotic key dependent **S-box** for **the *AES*** encryption algorithm.

2.8 Chaos-based Cryptography: an Overview, 2005

Ljupco Kocarev, Jos´e M. Amig´o, and Janusz Szczepanski (2005) proposed some of the recent work on chaos-based cryptography. We argue that if a chaotic map f is used in cryptography, then it should be implemented as a bijection $FM: D \rightarrow D$, where D is a finite

set with cardinality *M*, such that, for large *M*, *FM* 'approximates well' the chaotic map *f* . Several examples, including chaotic block cipher and chaotic public-key encryption algorithm are given.

2.9 A Fast Image Encryption System Based on Chaotic Maps With Finite Precision Representation, 2005

H.S. Kwok, Wallace K.S. Tang (2005) used 32-bit precision representation with fixed point arithmetic in order to achieve a fast throughput and facilitate hardware realization. The major core of the encryption system is a pseudo-random key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing

2.10 Security of Public- key Cryptosystems Based on Chebyshev Polynomials, 2005

Pina Bergamo et al. (2005) presented Chebyshev polynomials have been recently proposed for designing public-key systems. Indeed, they enjoy some nice chaotic properties, which seem to be suitable for use in Cryptography. In this paper, study a public-key cryptosystem based on such polynomials, which provides both encryption and digital signature. The cryptosystem works on real numbers and is quite efficient. Unfortunately, from our analysis, it comes up that it is not secure. We describe an attack which permits to recover the corresponding plaintext from a given ciphertext. The same attack can be applied to produce forgeries if the cryptosystem is used for signing messages.

2.11 An Enhanced Chaos Based Image Encryption Algorithm, 2006

Guosheng Gu, Guoqiang Han (2006) proposed permutation and substitution methods, to present a strong image encryption algorithm. An optimized treatment and a cross-sampling disposal are introduced for enhancing the irregular and pseudorandom characteristics of chaotic sequences. Its design and implementation has been discussed in detail and tested. Through simulation and analysis, the favorable performances of the proposed algorithm are evaluated.

2.12 An Algorithm for JPEG Compressing with Chaotic Encrypting, 2006

Huang Yuanshi, Xu Rongcong, Lin Weiqiang (2006) presented the analysis of the algorithm, we discuss the randomness of the chaotic sequence in detail and analyze the security and anti-collision of the chaotic hash sequence. The results indicate that our algorithm completely satisfied the security requirement in cryptography

2.13 Chaotic Block Ciphers, 2006

Naoki Masuda et al. (2006) presented a chaotic Feistel cipher and a chaotic uniform cipher. His plan is to examine crypto components from both dynamical-system and crypto graphical points of view, thus to explore connection between these two fields. In the due course, we

also apply dynamical system theory to create cryptographically secure transformations and evaluate crypto graphical security measures.

2.14 Key Exchange by Synchronization of two Chaotic Systems, **2006**

IAyman Mohammad Bahaa Eldin (2006) presented the idea of synchronization of two chaotic systems is used to solve the key exchange problem in cryptography. A proposal for a protocol is given and it is claimed that this method is simple and secure against known attack with the proof that the underlying chaotic systems model is a very hard problem to be solved, unlike the discrete logarithmic problem and other problems currently being used for key exchange which are only believed to be hard.

2.15 Theory & Practice of Chaotic Cryptography, 2007

J.M. Amigó, L. Kocarev, J. Szczepanski(2007) proposed a conceptual framework and illustrate it with different examples from private and public key cryptography. We elaborate also on possible limits of chaotic cryptography

2.16 An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption, 2007

Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah (2007) presented an efficient chaos based feedback stream cipher (ECBFSC) for image cryptosystems. The proposed stream cipher is based on the use of a chaotic logistic map and an external secret key of 256-bit. The initial conditions for the chaotic logistic map are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. Further, new features of the proposed stream cipher include the heavy use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms. These proposed features are verified to provide high security level.

2.17 Cryptographic Scheme Using Chaotic System, 2008

Dalia H. Elkamshoushy A.Khairy Aboulsoud (2008) proposed the schemes that make use of the chaotic system implemented at the transmitter receiver end using two different cryptographic algorithms. The encryption could be done by adding (mixing) the message signal to the output of the chaotic map and the decryption would be the subtraction of a synchronized chaotic map's output from the encoded signal. The encrypted signal would appear to be noise as it has been "mixed" with a chaotic signal.

2.18 Classical and Chaotic Encryption Techniques for the Security of Satellite Images, 2008 Muhammad Usama, Muhammad Khurram Khan(2008)presented an overview of the mechanisms used in image protection, especially Chaos-based encryption techniques available today. We will see how previously proposed methods such as Data Encryption

Standard (DES), Triple Data Encryption Standard (Triple-DES), and International Data Encryption Algorithm (IDEA) have been applied in image protection domain and how new concepts of Chaos-based encryption techniques are superior to traditional methods Chaos Theory and its Application in Modern Cryptography by Zhang hong, Dong Ji-xue in 2008.In this paper, the chaos theory and some specific contents of modern cryptography are introduced. By analyzing the relationship between chaos and cryptography, some approaches and their framework for chaotic cryptography system are proposed.

2.19 A Session Key Generator Based on Chaotic Sequence Chen, 2008

Chen Zhuo, Zhang zhengwen, Jiang nan (2008) presented a Key management which is a very important part in cryptography. It is related to generation, exchange, storage, safeguarding, use, and replacement of key. This paper focuses on the generation of session key according to the characters of chaotic system. A key generator based on chaotic sequence is proposed in this paper. It has better efficiency compared with the ANSI X9.17 standard.

2.20 A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method, 2008

Chong Fu, Zhiliang Zhu (2008) proposed an improved chaos-based image encryption scheme, in which the grayscale substitution is done by circular bit shift method. The scheme enlarges key space to 2^212, which improves the security under precision restricted condition. The combination of position permutation and grayscale substitution operation makes the encryption system strong against known/chosenplaintext attack.

2.21 A Novel Scheme for Image Encryption Based on Piecewise Linear Chaotic Map, 2008

Jun Peng et al. proposed a new digital image encryption scheme based on the piecewise linear chaotic map (PWLCM) in order to meet the requirements of the secure encryption. The proposed scheme is described in detail, along with the security analyses including key space analysis, sensitivity analysis, information entropy analysis and differential attack analysis. The results show that the suggested image encryption scheme has some properties desirable in a good security cryptosystem.

2.22 An Image Encryption Scheme Based on Cross Chaotic Map, 2008

Ling Wanq et al. (2008) Bo Zhang proposed a cross chaotic map using Logistic map and Chebyshev map. In order to realize image encryption, every pixel of image is randomly changed according to encryption matrix in the process of grayscale substitution; simultaneously scrambling transformation technique (row rotation and column rotation technique) is used in the process of position permutation

2.23 A Secure and Efficient Fingerprint Images Encryption Scheme, 2008

Song Zhao1 Hengjian Li2, Xu Yan(2008) proposed a novel chaotic fingerprint images encryption scheme is proposed combining with shuttle operation and nonlinear dynamic chaos system. Firstly, a new image total shuffling operation is employed to shuffle the positions of image pixels in the spatial-domain. Then the discrete output signal of the nonlinear dynamic chaos system is preprocessed to confuse the relationship between the shuttled image and the cipher-image.

2.24 Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption, 2008

Sai Charan Koduru and V. Chandrasekara (2008)presented three novelties in this paper: (a) we extend 2D images to 3D by using grayscale image intensities in 8-bit binary form (b) we embed the diffusion mechanism into confusion by applying the 3D Baker map based confusion algorithm. Thus, the diffusion process is accomplished by a permutation of binary bits in the third dimension, eliminating the need for a

separate diffusion process and (c) we extend the proposed method to color images by using the 24-bit color information.

2.25 Some Hints for the Design of Digital Chaos-Based Cryptosystems: Lessons Learned from Cryptanalysis, 2008

David Arroyo, Gonzalo Alvarez and Shujun Li (2008) proposed a list of what to avoid and to pay special attention to when considering chaos as source of new strategies to conceal and protect information

2.26 A Fast Image Encryption Scheme based on Chaotic Standard Map, 2008

Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2008) introduced certain diffusion effect in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. Simulation results show that at a similar performance level, the proposed cryptosystem needs less than one-third the encryption time of an existing cryptosystem.The effective acceleration of the encryption speed is thus achieved

2.27 Embedding Compression in Chaos-Based Cryptography, 2008

Kwok-Wo Wong, Ching-Hung Yuen (2008) proposed algorithm for embedding compression in the Baptista-type chaotic cryptosystem is proposed. The lookup table used for encryption is determined adaptively by the probability of occurrence of plaintext symbols. As a result, more probable symbols will have a higher chance to be visited by the chaotic search

trajectory. The required number of iterations is small and can be represented by a short code. The compression capability is thus achieved. Simulation results show that the compression performance on standard test files is satisfactory while the security is not compromised. Our scheme also guarantees that the ciphertext is not longer than the plaintext.

2.28 An Image Encryption Scheme Based on High Dimension Chaos System, 2008

Ying-yu Cao, Chong Fu (2008)analyzed the time sequences generated by Rossler system Three initial parameters of Rossler system are combined together as one key, which greatly enlarges the key space under precision restricted condition. The encryption speed is also improved since the position permutation and grayscale substitution to one pixel can be done by one iteration operation. Besides, the encryption system is strong against adaptive parameter synchronous attack since it has more complicated structure than simple chaos system based ones

2.29 Research of Chaotic Block Cipher Algorithm Based on Logistic Map, 2009

Fengjian Wang, Yongping Zhang, Tianjie Cao (2009) produced chaotic stream based on logistic mapping; the application of chaos in block cipher is researched. An encryption algorithm is proposed in this paper. In the algorithm, logistic mapping's system parameter is produced by m-sequence, and using another m-sequence's perturbation to increase the period of logistic mapping sequence. There is also output feedback mechanism in the algorithm.

2.30 A Feasible Chaotic Encryption Scheme for Image, 2009

Dongming Chen(2009) proposed an image encryption in which shifting the positions and changing the grey values of image pixels are combined simultaneously to ensure a high level of security. Arnold cat map is used to permute the positions of the image pixels in the spatial domain. Then another chaotic logistic map is used to substitute the relationship between the ciphered image and the original image. An external 128 bit secret key is employed and is further modified after encrypting each pixel of the original image to make the encryption more robust against attacks.

2.31 A Novel Image Encryption Scheme Based on Chaotic Maps, 2009

Xu Shu-Jiang et al. (2009) proposed two chaotic maps in this paper. One creates a binary stream for XOR operation, and the other creates some random numbers which are used to determine the circular bit shift. First the pixel values of the plain-image are modified randomly by the classical chaotic masking technique, namely XOR operation from the first block to the last block, and then the modified image is encrypted by the circular bit shit operation from the last block to the first block in the inverse order

2.32 A New Color Image Cryptosystem Based on a Piecewise Linear Chaotic Map, 2009

Rhouma Rhouma1, David Arroyo2 and Safya Belghith (2009) presented piecewise linear chaotic map (PWLCM)is used to build a new digital chaotic cryptosystem. The implicit digital degradation problem of PWLCM has been eluded through the discretization of the phase space. The accuracy, efficiency and security of the proposed encryption scheme are thoroughly analyzed and its adequacy for image encryption is proved.

2.33 An Improved Colour Image Encryption Based on Chaotic Map And OCML Model, 2009

Jun He, Jun Zheng, Zhi-bin Li, Hai-feng Qian(2009) proposed an improved colour image encryption which is based on a chaotic logistic map and the one-way coupled-map lattices (OCML) model. The results of several experimental, statistical analyses and key sensitivity tests prove the security robustness of the proposed cryptosystem.

2.34 An Improved AES Algorithm Based on Chaos Multimedia Information Networking and Security, 2009

Yuan Kun, Zhang Han, Li Zhaohui(2009) presented that the key space of AES encryption algorithm is limited, and there is few nonlinear factors in the whole system. In this paper, the author use two chaos systems, so the author can get two sequences. One is used as key, the other one is used to control the times of row-shift. This encryption algorithm combines the chaos theory with AES, then, a new algorithm is formed. This new method increases the key space and the nonlinear factors of AES system. In this case, the safety of encryption algorithm has been further improved

2.35 Digital Image Encryption Algo Based on Chaos and Improved DES, 2009

ZHANG Yun-peng et al. (2009) presented new encryption scheme uses the Logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time Encryptions with improvement DES, displays they respective merit. Theoretical analysis and the simulation indicate that this plan has the high starting value sensitivity, and enjoys high security and the encryption speed.

2.36 A Two-level Pipelined Implementation of the IDEA Cryptographic Algorithm, 2009

S´ergio L. C. Salom˜ao,Vladimir C. Alves ,Eliseu M. C(2009) presented the HiPCrypto chip, which implements the IDEA cryptographic algorithm. HiPCrypto is oriented towards computer network applications demanding high throughput. Its architecture exploits both the spatial and the temporal parallelism available in the IDEA algorithm. When operating at a 53 MHz clock, HiPCrypto can encrypt/decrypt at data rates up to 3.4 Gbps.

2.37 The Key Exchange Research of Chaotic Encryption Chip based on Elliptic Curve Cryptography Algorithm, 2009

Ping Zhou Qun Ding(2009) tried to encrypt the plaintext information with FPGA encryption chip based on chaotic encryption algorithm, the Elliptic Curve Cryptography algorithm is applied to encrypt and transmit the initial key to realize secure exchange. This essay emphatically researches the improvement of the point multiplication and the subjacent multiplication operations of the elliptic curve encryption so as to speed up the system implementation. Finally, the concerned experimental simulation of the improved elliptic curve encryption system proves that the system can effectively realize the security exchange of chaotic initial key.

2.38 Network Security: Synchronization in Chaotic Communication Systems, 2009

Stamatios V. Kartalopoulos (2009) proposed a pragmatic method that resolves the transmitter-receiver synchronization issue and also enhances chaotic cryptography.

2.39 A Chaos Public-Key Cryptosystem Based on Semi-Group Features, 2009

Bi Dayuan, Wang Dahu (2009) researched a hot spot to apply some chaos map in cryptosystem. Several chaos public-key cryptosystems are proposed, but proven as insecure or impractical. By analyzing the characteristics of Chebyshev polynomials, a public-key cryptosystem has been proposed in the paper. Firstly, the feature of semi group of Chebyshev polynomials is given, modular computation is introduced and the definitive range of Chebyshev polynomials is extended from [-1,1] to real field. Secondly, a new one-way drop door function, which is based on extended Chebyshev polynomials, is established. Then, we propose the correspondent public-key cryptosystem. In the end, it is proven that our algorithms are practical and feasible.

2.40 An Encryption Method Based on Dual-chaos System, 2009

Xibo WANG, Li MA, Xiaozhou DU (2009) presented Dual-chaos encryption algorithm which take Logistic Mapping as chaos model. Fibonacci sequence is adopted for mapping chaos to integer space in order to solve limited precision expression problem, dual-chaos system expend control parameters and increase complexity

2.41 Bio-Chaotic Stream Cipher-Based Iris Image Encryption, 2009

Abdullah Sharaf Alghamdi et al.(2009) presented the idea of biochaotic stream cipher which encrypts the images over the electronic media by using a biometric key and a bio-chaotic function. It enhances the security of the images and it should not be compromised. The idea also gives birth to a new kind of stream cipher named bio-chaotic stream cipher. The paper

also describes how to generate a key from a biometric string and how to encrypt and decrypt the desired data by using the bio-chaotic function.

2.42 High Security Image Encryption by Two-stage Process, 2010

C. K. Huang et al.(2010) proposed a hybrid encryption technique for the color image based on the multi-chaotic-system which combines Pixel-Chaotic-Shuffle (PCS) and Image-Multi-Encryption (IME). This method completely eradicates the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices, effectively protects against the decryption of exhaustive attack method, and more over, increases the key space of encrypted images. The test methods involving key space and correlation coefficient are adopted for the security analysis. Also NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) are preceded for the proof of the distinguished characteristic of pixels in the encrypted image. Eventually, empirical images are conducted as illustrations, which show that the proposed method has the great encryption performance and achieves the high confidential security.

2.43 New chaos Advanced Encryption Standard (AES) Algorithm For Data Security, 2010

ElBadawy et al.(2010) proposed a new chaos AES algorithm for data security. The algorithm is based on substituting the Rijndael affine transformation S-box by another one based on chaos theory. The new S-box has a low correlation and exhibits a significant performance improvement with an acceptable complexity addition. The algorithm is tested using the commonly used tests for determining whether the binary sequence possesses some specific characteristics that a truly random sequence would be likely to exhibit. These are frequency, runs, and serial and poker tests, respectively. These statistical tests are performed with random and uniform distribution plaintext data. The results of the proposed chaos AES were compared with a normal one and gave a significant improvement for the accepted sequences probability over a wide range of chaos initial conditions. The sensitivity of the initial condition gives the algorithm the ability to be used as another key for more security and confidentiality

2.44 Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption, 2010

Kamel Faraoun (2010) proposed an n-ary key stream generator, based on hierarchical combination of three chaotic maps. We demonstrate that the produced key streams have good statistical properties such as uniform distribution, δ-like auto-correlation function, near-zero cross-correlation and very height sensitivity to initial conditions, under precision restricted

condition. An image cryptosystem is constructed using the proposed approach and proven to be enough secure to resist various attacks. Complexity is analysed and an effective acceleration of chaos-based image cryptosystems is shown to be achievable

2.45 A Multiple Chaotic Encryption Scheme for Image, 2010

Zhao Mingming, Tong Xiaojun(2010) presented an image encryption scheme based on high-dimensional multiple chaotic maps and Arnold cat map is utilized to permute the positions of the image pixels in the spatial domain. The experimental results show that it is more efficient than traditional encryption schemes. Compared with simple low-dimensional chaotic system, the proposed scheme does not readily lead to precision degradation and it has passed NIST sp800-22 standards, it provides an efficient and secure way for image encryption.

2.46 Chaos Theory and its Application in Modern Cryptography, 2010

Zhang hong Dong Ji-xu (2010) presented the chaos theory and some specific contents of modern cryptography are introduced. By analyzing the relationship between chaos and cryptography, some approaches and their framework for chaotic cryptography system are proposed. Some criteria about how to choose chaotic systems and their parameters in digital encryption are given in detail

2.47 The Bifurcation Analysis of Digital Chaos Circuit and Its Application, 2010

Lu Wang Qun Ding (2010) presented on the instability of the digital chaotic orbit and the bifurcation behavior, designs the hardware circuit which is used to realize the bifurcation of digital chaotic based on FPGA, analyzes the .similarity between dynamics of chaotic systems and digital chaotic system with test comparative method, confirms the fact that digital chaotic indeed have the behavior of bifurcation, and provides the corresponding value of U.

2.48 A New Chaos-Based Cryptosystem for Secure Transmitted Images, 2010

In 2010 Abir AWAD 2010 presented a novel and robust chaos-based cryptosystem for secure transmitted images and four other versions. In the proposed block encryption/decryption algorithm, a 2D chaotic map is used to shuffle the image pixel positions. Then, substitution (confusion) and permutation (diffusion) operations on every block, with multiple rounds, are combined using two perturbed chaotic PWLCM maps. The perturbing orbit technique improves the statistical properties of encrypted images. The obtained error propagation in various standard cipher block modes demonstrates that the proposed cryptosystem is suitable to transmit cipher data over a corrupted digital channel. Finally, to quantify the security level of the proposed cryptosystem, many tests are performed and experimental results show that the suggested cryptosystem has a high security level

2.49 A New Chaos Advanced Encryption Std (AES) Algo for Data Security, 2010

El-Sayed Abdoul-Moaty ElBadawy et al.[2010] presented an algorithm based on substituting the Rijndael affine transformation S-box by another one based on chaos theory. The new S-box has a low correlation and exhibits a significant performance improvement with an acceptable complexity addition.

2.50 A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps, 2010

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab (2010) used the external secret key to derive the initial conditions for the chaotic maps, and is employed with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the pixels are en-

crypted using an iterative cipher module based feedback and data-dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information. To make the cipher more robust against any attack, the secret key is modified after encryption of each pixel of the plain image.

2.51 Efficient modified RC5 based on chaos adapted to image encryption, 2010

Mohammad Amin and Ahmed A Abd El-latif(2010) modified the RC5 to give high level security, and adopt it for image encryption by adjusting the structure of both the encryption routine and the key schedule. They generate round keys based on chaos. Then, strengthen the diffusion operation by making heavy use of rotations. The security analysis of the modified cipher against several attacks is explored from a strict cryptographic viewpoint. Experimental results demonstrate that the modified RC5 provides an efficient and secure way for image encryption.

2.52 Iris Recognition System Based on Chaos Encryption, 2010

Liu Yangl Yue Xue Dong Liu Ying Fee He Yan (2010) proposed an iris recognition, using multi-scale 2D Gabor filter to acquire the identify code of iris texture only in single-direction. To protect the identify code be transported securely, one-way coupled map lattice (OCML) chaos system be applied to generate pseudo-random number key stream, and the iris identify code will be encrypted and decrypted based on the method of ciphertext feedback. Finally, using Hamming distance to finish iris classification.

2.53 Embedding Adaptive Arithmetic Coder In Chaos-Based Cryptography, 2010

Li Heng-Jian and Zhang Jia-Shu (2010) In this study an adaptive arithmetic coder is embedded in the Baptista-type chaotic cryptosystem for implementing secure data compression. To build the multiple lookup tables of secure data compression, the phase space

of chaos map with a uniform distribution in the search mode is divided non-uniformly according to the dynamic probability estimation of plaintext symbols. As a result, more probable symbols are selected according to the local statistical characters of plaintext and the required number of iterations is small since the more probable symbols have a higher chance to be visited by the chaotic search trajectory. By exploiting non-uniformity in the probabilities under which a number of iteration to be coded takes on its possible values, the compression capability is achieved by adaptive arithmetic code

3. SUMMARY

In this paper, many of the important Chaos based encryption techniques have been presented and analyzed. These techniques are based on:

1. Two chaotic signals are used for encryption. First one is used to synchronize encripter and decrypter and second one is used for multishift rotation
2. A couple chaotic system based pseudo random bit generator (CCS-PRBG) were used for randomness. Two CCS-PRBG were used to design a chaotic key dependent S-box for the *AES* encryption algorithm.
3. Chaotic Feistel cipher and a chaotic uniform cipher.
4. Permutation and substitution methods, to present a strong image encryption algorithm.
5. the idea of synchronization of two chaotic systems is used to solve the key exchange problem in cryptography
6. A cross chaotic map using Logistic map and Chebyshev map. In order to realize image encryption, every pixel of image is randomly changed according to encryption matrix in the process of grayscale substitution; simultaneously scrambling transformation technique (row rotation and column rotation technique) is used in the process of position permutation
7. Algorithm for embedding compression in the Baptista-type chaotic cryptosystem is proposed. The lookup table used for encryption is determined adaptively by the probability of occurrence of plaintext symbol
8. Three initial parameters of Rossler system are combined together as one key,
9. The Elliptic Curve Cryptography algorithm is applied to encrypt and transmit the initial key to realize secure exchange.
10. Idea of biochaotic stream cipher which encrypts the images over the electronic media by using a biometric key and a bio-chaotic function

11. A 2D chaotic map is used to shuffle the image pixel positions. Then, substitution (confusion) and permutation (diffusion) operations on every block, with multiple rounds, are combined using two perturbed chaotic PWLCM maps. The perturbing orbit technique improves the statistical properties of encrypted
12. An iris recognition, using multi-scale 2D Gabor filter to acquire the identify code of iris texture only in single-direction. To protect the identify code be transported securely, one-way coupled map lattice (OCML) chaos system be applied to generate pseudo-random number key stream, and the iris identify code will be encrypted and decrypted based on the method of ciphertext feedback

On the basis of study of all the above mentioned research papers thoroughly, the following suggestions can be drawn:

1. To protect multimedia contents, Chaos based algorithm should be implemented
2. More complex & compressed algorithm should be used to provide high speed and security to the System
3. Utilize Chaotic Map to design new Cryptographis Algorithms
4. Finding and designing new hash functions that work better than the current existences hash functions
5. The existing technique can be implemented on hardware
6. Some other diffusion function should be used so that there should be better trade-off between the security and computational complexity

4. REFERENCES

1. Kwok, H. S.,Wallace, K.S. , Tang (2007) A Fast Image Encryption System Based on Chaotic Maps, *Ch.Solitons and Fractals* 1518–1529
2. Amigó, J.M, Kocarev,L.,Szczepanski,J. (2007). Theory and practice of chaotic cryptography. *Physics Letter* 211-216
3. Yang,T., Chai Wah Wu, and Leon O. Chua (1997).Cryptography Based on Chaotic System *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I*
4. Lee, J., Chow, S., and Hang, D. (1998). Secure Communication Using A Chaos System In A Mobile Channel *IEEE proceeding*,0-7803-4984-9
5. Alvarez,G., Montoya,F, Pastor,G., Romera ,M.(1999). Chaotic Cryptosystem *IEEE Proceeding 0*-7803-5247-5

6. Han, Z., Xiu Feng, W., Zhao Hui, L., Da Hai, L., You Chou, L. (2003). A New Image Encryption Algorithm Based on Chaos System, *Proceedings of the 2003 IEEE*
7. Guglielmi,V., Poonithl, H., Fournie.-Prunaret, D. and Taha, A. K. (2004). Security Performances of a Chaotic Cryptosystem, *IEEE-7803-8304-4/04*
8. Socek, D., Li, S., Spyros S. Magliveras and Furh, B. (2004). Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption
9. Rohiem, A. E., Elugooz, S., Dahshan, H. (2005). A Novel Approach for Designing the $-Box of Advance Encryption STD Algorithm *(AES)* Using Chaotic Map, 2005
10. Kocarev, L. Jos´e M. Amig´o, and Szczepanski, J. (2005). Chaos-based Cryptography: an overview, *2005 International Symposium on Nonlinear theory and application*
11. Kwok,H.S., Wallace K.S. ,Tang (2005). A Fast Image Encryption System Based On chaotic maps With Finite Precision Representation, 2005
12. Bergamo, P., D'Arco, P., Santis, A.D. and Kocarev L. (2005). Security of Public- key Cryptosystems Based on Chebyshev Polynomials *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS*
13. Gu, G., Han, G. (2006). An Enhanced Chaos Based Image Encryption Algorithm *IEEE proceedings*,0-7695-2616
14. Yuanshi, H., Rongcong, X., Weiqiang, L. (2006). An Algorithm for JPEG Compressing with Chaotic Encrypting. *Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation*
15. Masuda, N., Jakimoski, G., Aihara, K. and Kocarev, L. Chaotic Block Ciphers *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS*
16. Mohammad, I., Eldin, B. (2006). Key Exchange by Synchronization of Two Chaotic Systems, *IEEE proceeding*1-4244-0272-7/06
17. migó J.M, Kocarev L., Szczepanski J.,(2007). Theory and practice of chaotic cryptography *0375-9601 Elsevier B.V*.
18. El-din, H., Ahmed, H., Kalash, H.M. and Osama S. Farag Allah. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption
19. Dalia H. Elkamshoushy, A.Khairy Aboulsoud. (2008) CRYPTOGRAPHIC SCHEMES USING CHAOTIC SYSTEM, *25th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2008*)
20. Usama, M., Khan, M. K.(2008). Classical and Chaotic Encryption Techniques for the Security of Satellite Images *IEEE proceeding* 1-4244-2427-6/08

21. Zhuo, C., Zhengwen, Z., Nan, J. (2008). A Session Key Generator Based on Chaotic Sequence Chen *International Conference on Computer Science and Software Engineering* 978-0-7695-3336-0/08
22. Fu, C., Zhu, Z. (2008). A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method *IEEE Proceeding o*n978-0-7695-3398-8/08
23. Peng, J., Jin, S., Liu, Y., Yang, Z., You, M. and Pei, Y. A Novel Scheme for Image Encryption Based on Piecewise Linear Chaotic Map
24. Wang, L., Ye, Q., Xiao, Y., Zou, Y. (2008) An Image Encryption Scheme Based on Cross Chaotic Map, 2008 *Congress on Image and Signal Processing*
25. Zhao, S., Li, H., Yan, X.(2008) A Secure And Efficient Fingerprint Images Encryption Scheme *The 9th International Conference for Young Computer Scientists*
26. Koduru, S. C., and Chandrasekara, V. (2008) Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption, *IEEE 8th International Conference on Computer and Information Technology Workshops*
27. David Arroyo , Gonzalo Alvarez and Shujun Li (2008). Some Hints for the Design of Digital Chaos-Based Cryptosystems: Lessons Learned from Cryptanalysis.
28. Wong, K. W., Kwok, B. S., and Law, W. (2008) A Fast Image Encryption Scheme based on Chaotic Standard Map
29. Wong, K., Yuen, C. (2008) Embedding Compression In Chaos-Based Cryptography
30. Cao, Y., Fu, C. (2008) An Image Encryption Scheme Based on High Dimension Chaos System
31. Wang, F., Zhang, Y., Cao, T. (2009) Research of Chaotic Block Cipher Algorithm Based on Logistic Map 2009 *Second International Conference on Intelligent Computation Technology and Automation*
32. Chen, D.(2009) A Feasible Chaotic Encryption Scheme for Image
33. Shu-Jiang, Ying-Long, W., Ji-Zhi, W., Min, T.(2009) A Novel Image Encryption Scheme Based on Chaotic Maps
34. Rhouma, R., Arroyo, D. and Belghith, S. (2009) A New Color Image Cryptosystem Based ON A Piecewise Linear Chaotic Map.
35. He, J., Zheng, J., Li, Z.B., Qian, H.(2009) An improved color image encryption based on chaotic map and OCML model IEEE International Conference on Networks Security, Wireless Communications and Trusted Compution 978-0-7695-3610-1/09
36. Kun, Y., Han, Z., Zhaohui, L. (2009) An Improved AES Algorithm Based on Chaos Multimedia Information Networking and Security

37. Yun-peng, Z., ZHAI, Zheng-jun, Xuan, N., Shui-ping, C., Wei-di, D. (2009) Digital Image Encryption Algo Based on Chaos and Improved DES Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
38. S´ergio L. C. Salomao,Vladimir C. Alves ,Eliseu M. C(2009) A Two-level Pipelined Implementation of the IDEA Cryptographic Algorithm
39. Zhou, P., Ding, Q. (2009) The Key Exchange Research of Chaotic Encryption Chip based on Elliptic Curve Cryptography Algorithm 2009 Second International Conference on Intelligent Computation Technology and Automation
40. Kartalopoulos, S.V. (2009) Network Security: Synchronization in Chaotic Communication Systems 978-1-4244-4148-8-IEEE
41. Dayuan, B. Dahu, W. (2009) A CHAOS PUBLIC-KEY CRYPTOSYSTEM BASED ON SEMI-GROUP FEATURES 978-1-4244-4134-1/09/IEEE
42. WANG, X., MA, L., DU, X. (2009) An Encryption Method Based on Dual-chaos System 2009 Second International Conference on Intelligent Networks and Intelligent Systems
43. Alghamdi, A.S., Ullah, H., Mahmud, M., Khan, M. K.(2009) Bio-Chaotic Stream Cipher-Based Iris Image Encryption 978-0-7695-3823-5/09 IEEE International Conference on Computational Science and Engineering
44. Huang, C. K., Hsu, Y. H., Chen, W. Y., Changchien, S. K., Hung, C. M., Liu, C. H., Tian, Y. R. (2010) High Security Image Encryption by Two-stage Process
45. ElBadawy, E.-S.A.-M.; Mokhtar, A.; El-Masry, W.A. Hafez(2010) New chaos Advanced Encryption Standard (AES) algorithm for data security
46. Faraoun, K. (2010) Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption
47. Mingming, Z., Xiaojun, T. (2010) A Multiple Chaotic Encryption Scheme for Image 978-1-4244-3709-2/10/IEEE
48. Hong, Z., Ji-xu, D. (2010) Chaos Theory and its Application in Modern Cryptography 978-1-4244-7237-6-IEEE International Conference on Computer Application and System Modeling
49. Wang, L., Ding, Q. The bifurcation analysis of digital chaos circuit and its application 2010 978-0-7695-4247-8/10 International Workshop on Chaos-Fractal Theory and its Applications
50. AWAD, A. (2010) A New Chaos-Based Cryptosystem for Secure Transmitted Images IEEE TRANSACTIONS ON Computers

51. ElBadawy, E. A., El-Masry, W. A., Mokhtar, A., Hafez, A. S. (2010) A New Chaos Advanced Encryption Std (AES) Algo for Data Security
52. Ismail, I. A., Amin, M., and Diab, H.(2010) A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps
53. Amin, M. and Ahmed A, El-latif, A.(2010) Efficient modified RC5 based on chaos adapted to image encryption
54. Yang, L., Dong, Y. X., Ying, L., Yan, F. H. (2010) Iris Recognition System Based on Chaos Encryption 2010 International Conference On Computer Design And Applications (ICCDA 2010)
55. Heng-Jian, L. and Jia-Shu, Z. (2010) Embedding adaptive arithmetic coder in chaos Based cryptography.