CHAOS BASED CRYPTOGRPHY AND IMAGE ENCRYPTION

by

Amber Shaukat Nasim

M.Sc., University of Applied Sciences, Luebeck, Germany, 2012

A project

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Engineering

in the Program of

Electrical and Computer Engineering

Toronto, Ontario, Canada, June 2015

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this MEng Project. This is a true copy of the MEng Project, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that MEng Project may be made electronically available to the public.

Chaos based cryptography and image encryption, M.Eng. 2015, Amber Shaukat Nasim,
Program of Electrical and Computer Engineering, Ryerson University

ABSTRACT

Chaotic cryptography pronounces the use of chaos theory in specific physical dynamical systems working in chaotic system as measure of communication techniques and computation algorithms to accomplish dissimilar cryptographic tasks in a cryptographic system. We have reviewed some of the recent work on chaos-based cryptography in this piece of work.

Cryptography methodologies are critically important for storage of secured media content and transmission over exposed systems, for example, the web.For high security, encryption is one the approach to guard the information from leakage. Image encryption is transformation of image to an inaccurate form so that it can be secured from unauthorized users.

To explore application of encryption in time samples pattern, we have recommended a secured approach to code input signals by introducing a new encryption algorithm. The algorithm mechanism is such that the transmitter, an input signal was received and coded into a lengthier series of numbers. At the receiver, the coded signal by the transmitter was received and changed back into its original values. This was done based on the idea that the hidden input signal samples using a specific pattern, could only recoverable by a trusted receiver.

ACKNOWLEDGEMENTS

I am expending this chance to express my appreciation to every person who supported me throughout the thesis project of this Masters of Engineering. I am genuinely grateful to them for sharing their honest and enlightening opinions on a number of concerns related to the project. It gives me great pleasure in acknowledging my Professor Dr. Kaamran Raahemifar for the continuous support and supervision for the success of this project.

I would like to thank my parents and my family for being a great model and encouraging me throughout my studies, making this project possible.

Dedicated to my beloved Parents, husband and my lovely daughters.

Table of Contents

Table of Figures:

CHAPTER 1

1 INTRODUCTION

Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The technique of concealing plaintext in order to hide its particular material is called encryption. The impression of encryption is to make a message incomprehensible, except to the receiver.

Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text. Encryption is used to guarantee the hidden information from anyone of concern not intended to, even those who can comprehend the encrypted data. The procedure of backsliding cipher text to its original plaintext is considered as decryption.

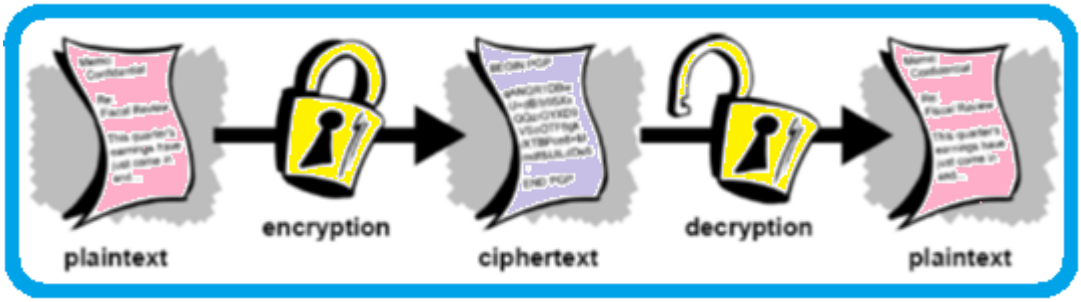


Figure 1: Encryption and Decryption

1.1 Cryptography

The science of consuming the calculation and math behind the procedure to encrypt and decrypt data is called cryptography. Cryptography facilitates to accumulate the sensitive information or pass on it through the insecure networks in order to keep it unreadable from public except the intend receiver.

Although cryptography is the skill or art of securing data, the skill of analyzing and breaking secure communication is considered as cryptanalysis. Classical cryptanalysis implicates a fascinating arrangement of application of mathematical tools, analytical reasoning, tolerance, pattern finding, willpower, and good fortune. Cryptanalysts are also considered as attackers. Cryptology comprises of both cryptography and cryptanalysis.

1.1.1 Cryptography Algorithm

A mathematical function utilized for the process of encrypting and decrypting data is called a cryptographic algorithm, or cipher. A cryptographic algorithm mechanism leads with the combination of a key a word, number, or expression to encrypt the plaintext. The identical plaintext encrypts to dissimilar cipher text with unlike keys. The security of encrypted data is completely reliant on two important aspects i.e. the strength of the cryptographic algorithm and the confidentiality of the key. A cryptosystem is entitled due to the presence of cryptographic algorithm, along with all potential keys and all the working protocols.

1.1.2 Conventional Cryptography

Conventional cryptography progress with single key for both encryption and decryption. It is also named as secret-key or symmetric-key encryption. The Data Encryption Standard (DES) is an

example of a conventional cryptosystem that is extensively engaged by the Federal Government. Figure 2 is an illustration of the conventional encryption process.

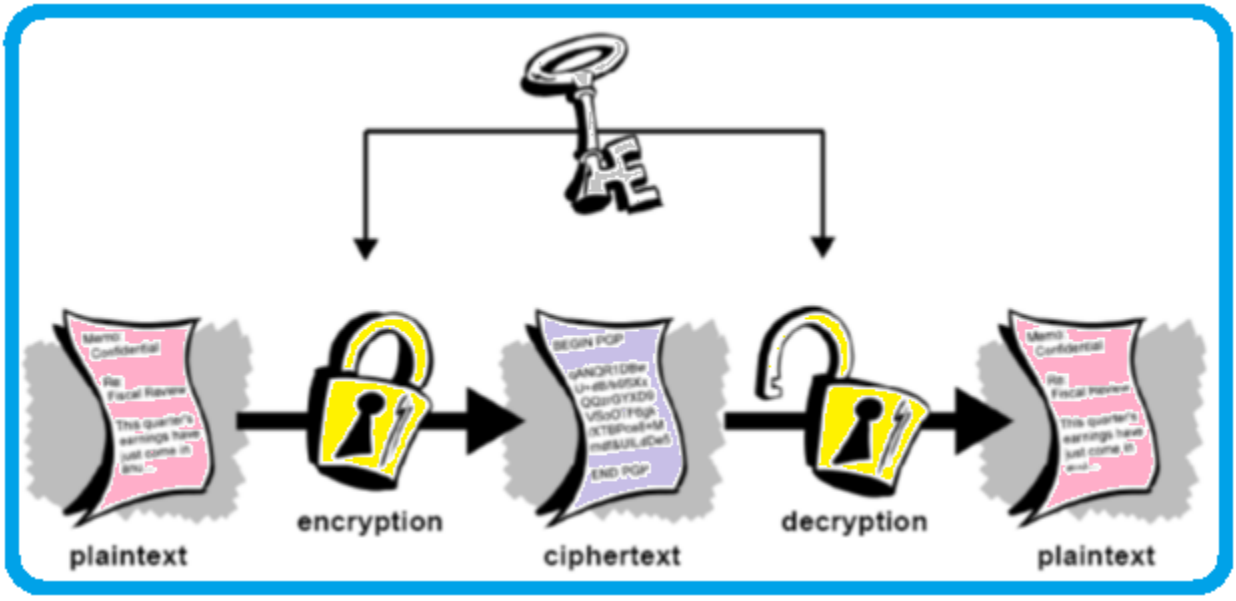


Figure 2: Conventional encryption

Conventional encryption is beneficial in a way that it is very fast. It is specifically advantageous for encrypting data that stays at the same place. On the other hand, the difficulty of secure key distribution is the main cause of making conventional encryption relatively expensive as a means for transmitting secure data.

1.1.3 Case In Point

It will be a good example to recall a character from any favorite spy movie:

There is somebody with a sealed briefcase fastened to his or her wrist. So what is secured in the briefcase, anyhow? It's undoubtedly not the missile launch code or bio-toxin formula or invasion plan itself.

In fact it's the key that resolve decrypting the secret data. Secret key is the only approach for a sender and recipient to interconnect securely consuming conventional encryption, so they must come to an understanding upon a single key and keep it secret among themselves. In case both are present in different physical locations, they must have reliance on a courier, or any other protected communication medium to inhibit the revelation of the secret key throughout the transmission. Anyone who listen to or interrupts the key in transfer can later deliver, amend, and falsify all information encrypted or authenticated with that key. From DES to Captain Midnight's Secret Decoder Ring, the determined problem with conventional encryption is key circulation where the important question arises that how the key can be given to recipient without having anyone's interception in transmission.

1.1.4 Encryption Methods

The basic encryption methods are as follows:

1. **DES** (Data Encryption Standard)

   The Data Encryption Standard (DES) is a block cipher that practises mutual secret encryption. It was a selection by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has consequently appreciated extensive use internationally. It is constructed on a symmetric-key algorithm that utilizes a 56-bit key. The algorithm was in the beginning controversial with classified design elements, a comparatively short key length, and uncertainties about a National Security Agency (NSA) way out. DES subsequently came under passionate academic inspection which encouraged the modern

appreciative of block ciphers and their cryptanalysis. This key size is susceptible to an instinctive force attack using current technology.

2. **Triple DES**

   It is a variation of DES, Triple DES, which is responsible for considerably improved security by accomplishing the core DES algorithm three times in a row. The consequence of creating the DES encryption much more challenging to instinctive force. Triple-DES is assessed to be 2 to the 56th times more tough to break than DES. Triple DES can still be well thought-out as a secure encryption algorithm. Triple DES is also written as 3-DES or 3DES.

3. **AES** (Advanced Encryption Standard)

   It is a symmetric cipher well-defined in Federal Information Processing (FIPS) Standard Number 197 in 2001 as the federal government sanctioned encryption algorithm. The NSA has permitted 128-bit AES for practise up to secret level and 192-bit AES for practise up to top secret level. AES is based upon the Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen. AES identifies three permitted key lengths: 128-bits, 192-bits and 256-bits.

1.1.5 Public Key Cryptography

The difficulties of key dissemination are deciphered by public key cryptography. Public key cryptography is an asymmetric scheme that customs a pair of keys for encryption: a public key for encrypting data, and a consistent private, or secret key for decryption. Public key is public to the world while protecting private key secret. Any person with a duplicate of public key can then encrypt information that only he or she can read. Even to people who have not ever met.

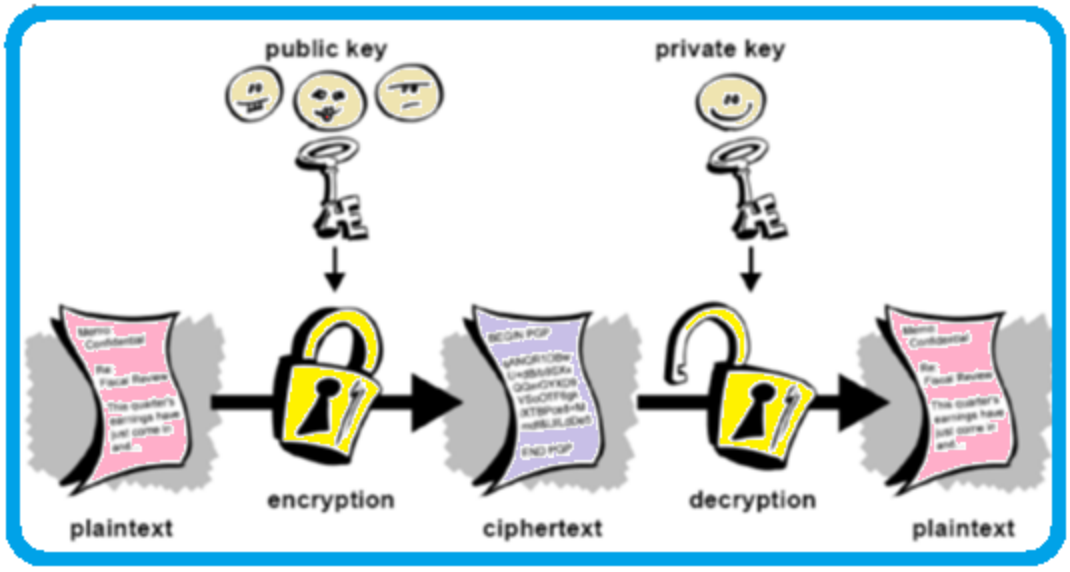


Figure 3: Public Key Encryption

The principal advantage of public key cryptography is that it permits general public who have no pre-existent security procedure to interchange messages securely. The requirement for sender and receiver to share secret keys through some secure channel is rejected; all communications consist of only public keys, and no private key is ever transferred or shared. Some examples of public-key cryptosystems are

- Elgamal (named for its inventor, Taher Elgamal),
- RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman),
- Diffie-Hellman (named, you guessed it, for its inventors), and
- DSA, the Digital Signature Algorithm (invented by David Kravitz)

For the reason that conventional cryptography was once the only accessible resources for transmitting secret information, the outflow of secure channels and key distribution downgraded its use only to those who could meet the expense of it, such as governments and large banks. Public key encryption is the technological uprising that be responsible for sturdy cryptography to the mature multitudes. Recall the courier with the protected briefcase handcuffed to his or her wrist? Public-key encryption situates him out of business, perhaps to its liberation.

Some of the public key encryption algorithm are

1. **RSA**

   It is an Internet encryption and verification system that practises an algorithm established in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the utmost frequently used encryption and verification algorithm and is contained within the portion of the Web browsers from Microsoft and Netscape. It's also portion of Lotus Notes, Intuit's Quicken, and several other products. RSA security is the owner of the encryption system. The algorithm technologies are licensed by the company and the company also trades development kits. The technologies are part of current or anticipated Web, Internet, and computing standards.

2. **Elliptic curve cryptography (ECC)**

   It is a methodology to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. In 1985, Neal Koblitz and Victor S. Miller recommended the use of elliptic curves in cryptography independently. Elliptic curves are correspondingly used in numerous integer factorization algorithms that consume applications in cryptography, for example Lenstra elliptic curve factorization.

3. **ElGamal encryption system**

   It is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. In 1985 Taher Elgamal was the one to define it. ElGamal encryption is used in the unrestricted GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a modified version of the ElGamal signature scheme, which should not be confused with ElGamal encryption.

1.2 IMAGE ENCRYPTION

The primary thought in the image encryption is to transmit the image safely over the system so no unapproved client can ready to decode the image. The image information have uncommon properties, for example, mass limit, high severance and high association among the pixels that forces exceptional prerequisites on any encryption procedure [1]. The most well-known system of secure the advanced pictures is to scramble the computerized information such that unique message of the archives ought not to be identified. There are a few methodologies to accomplish this for instance steganography, packing, advanced watermarking and cryptography. Here the emphasis is on the encryption methods of advanced digital images focused around the chaos mapping. Fundamentally image encryption is the methodology of changing data utilizing a algorithm to make it ambiguous to anybody with the exception of those having exceptional learning, normally alluded to as a key and the changing data utilizing "encryption algorithm" into a structure that can't be deciphered without a key of decryption.

From the other point of view, decryption of image recovers the genuine data from the encrypted structure image. There are more than a few computerized image encryption frameworks to encode and decode the image information, and there is no single encryption calculation accessible that fulfills the distinctive image sorts. The encryption strategies focused around the chaos mapping gives the encoded advanced images to hold the multilevel encryption strategy furthermore diminishes the computational difficulty of the encryption process. A large portion of the algorithms particularly intended to scramble or encrypt computerized images are proposed in the mid-1990s. There are two significant assemblies of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. The vast majority of these algorithms are intended for a particular image setup compacted or uncompressed, and some of them are even setup acquiescent.

There are systems that offer light encryption (degradation), although others compromise solid manifestation of encryption. A percentage of the algorithms are versatile and have different modes ranging from degradation to solid encryption [2]. The encryption methods focused around the

chaos have distinctive sorts of uses in different zones, for illustrations ; the web correspondence, military, medicinal services, mapping and situating, picture informing applications on phones, interactive media frameworks, therapeutic imaging, Tele-pharmaceutical, protection and government archives and so forth. The advancement of image encryption procedure is moving towards a prospect of unlimited conceivable outcomes. On daily basis, new strategies for encryption methods are revealed [3].

1.3 IMAGE ENCRYPTION TECHNIQUES

1.3.1 Classic Image Encryption

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for content encryption by Rijmen and Daemen in 1999 [1] furthermore known as Rijndael algorithm, however a few scientists made functional use of this algorithm for image encryption likewise with a few changes in key generation and other requirements. Zeghid et al. [2] proposed an improved AES based algorithm by including a key stream generator (A5/1, W7) to AES to guarantee enhancing the encryption execution for image encryption process. An alternate algorithm proposed by Subramanyan et al. [3] focused around AES Key Expansion in which the encryption methodology is a bit astute XOR operation of a set of image pixels besides a 128 bit key that varies for each set of pixels. The keys to be utilized are produced freely at the sender and recipient side focused around AES Key extension transform thus the preliminary key is distant from everyone else imparted instead of offering the entire set of keys.

DES, a prevalent block cipher algorithm utilizes 64 bit key, which is an alternate printed cryptosystem that utilized for image encryption by Qian Gong-canister et al. In [4] another image encryption plan focused around DES consolidated with a chaotic map introduced to enhance the security and develop the key space. The results demonstrate that blend of word-based cryptosystems with different strategies or rolling out a few improvements, enhance the security and against anti attack capacity of those algorithms adequately.

1.3.2 Public Key Image Encryption

Most of application does not provide a facility of a secure channel to transfer the private key or desire to keep the decryption key in secret, so we need to utilize public key cryptography. In the first place public key was circulated by Diffie and Hellman in 1976 [5]. It was a key trade down

to earth strategy for making an imparted secret key over a verified correspondence channel without utilizing a former imparted secret. The greater part of conventional public key cryptosystems intended to encode printed information. A few works have been distributed on public key image encryption, one is proposed by Shuihua et al. [6].

In this plan, the plain image isolated into blocks utilizing a certain network change and all pixels in each one block exchanged to DCT field. Public key, private key, encryption methodology and unscrambling procedure are characterized focused around change network of DCT coefficients. The results show that this system is vigorous in contradiction of JPEG lossy clamping and other general assaults. An alternate public key system focused around Chebyshev chaos map portrayed by K. Ganesan et al. [1] for colour images encryption and features progressively applications. In the first place they attempted to cryptanalysis the encryption focused around Chebyshev polynomial map and results demonstrate that it is not powerful on a few attacks, so they attempted to improve the security by utilizing a non-Xoring hash function to secure it against attack of picked plaintext. They do proficiency check and some testing for cryptanalysis, for example, key affectability, connection, mono bit, long run test and time examination for both image and video and determined from the result that their recommended cryptosystem is more secure and strong to any invader attack and the time investigation exhibits the effectiveness of encryption for 64x64 and 128x128 video encryption.

An image encryption strategy utilizing ECC is proposed by K. Gupta et al. [8] by transforming every pixel into the elliptic arc point to transform the plain image to encrypted image. They only suggested a framework and experiments done with a simple elliptic arc function with few points, so it is not an appropriate system, but as a innovative idea, results demonstrate the adequate encryption time in contrast with other public key techniques like RSA because of key size, and furthermore gives the key affectability yet needs to be upgraded as future works. Visual cryptography (VC) is a simple and safe technique proposed by Naor and Shamir [9] in 1994. In [10] A. Jaafar and A. Samsudin proposed another public key plan with straightforward and low processing by consolidation of VC and Boolean AND operation comes about a quick running time for encryption and decoding.

1.3.3 Compression and Encryption

Compression procedures help us to lessen the transmission data transfer capacity or storage space. These procedures can be actualized in both spatial and frequency domain. Also frequency domain procedures are further effectual and consuming collective and widespread transforms such as DCT, DFT and DWT. Data compression lessons can be classified into two types:

- **LOSSY**: Lossy methods compromise a definite loss for information in return with the high compression proportion. Usually lossy methods decline the superiority of the object so they are sought out for images, videos and audios for the reason of human observation. There Lossy coding method also moreover categorised into the following types:

a. Predictive coding
b. Transform coding

- **LOSSLESS**: On the other hand, some kinds of data could not accept any loss (e.g. Database records, executable files and word processing files and medical images), otherwise the data will be degraded, and here the lossless techniques play role. The Lossless coding technique also further classified into following categories:

a. Run length encoding
b. Huffman encoding
c. Arithmetic encoding
d. Entropy coding
e. Area coding

Ordinary cryptosystems identifies with the compressed multimedia. Encryption and compressed multimedia are typically extremely contradictory and an exchange off depends between them. Encrypting the interactive media content before pressure uproots a ton of repetition and this result in an exceptionally poor compression proportion. Then again, encrypting the information after compression demolishes the codec design, which are the bases for the decoders to crash.

As a final point, encryption is taken lightly for many applications to reserve approximate perceptual data [11]. B. Mohammed et al. [12] in their projected encryption-compression method initially enforced a FMT technique to compress the particular image and at that time AES-Based algorithm functionalized to encrypt the image. L. Vorwerk et al. [13] strained to syndicate encryption and wavelet compression. The methodology of encryption utilizes a symmetric key for encrypting image and wavelet filter, a public key cryptosystem is recommended to encrypt the symmetric key for secure key interchange.

A recent mixing arrangement of encryption and compression for images suggested by I. Masanori et al. [14] centred on Independent Component Analysis (ICA) and Discrete Cosine Transform (DCT). To attain a quick and secure image transmission they utilized DCT and a low pass filter for image compression and by rotating and making a mixture of the DCT blocks with an arbitrary image, the source image is encrypted. When this journey's end, the encrypted expected image is decrypted by taking out the protected images from the mixtures by spreading over ICA and lastly by utilizing rotation keys and IDCT the novel image is recreated.

Additional methodology to assimilate compression and encryption is deliberated in the system of C. Wu and J. Kuo [15]. They debated about benefits and drawbacks of discerning encryption and anticipated an encryption schemes which can transforms the entropy of simple message as an outcome to be a cipher message by spreading on Huffman coder and QM coder. Finally, concluded that this high security scheme can be applied to compression techniques such as MPEG and JPEG with acceptable computational speed.

1.3.4 Selective Encryption

A methodology that offered to abstain from encrypting the complete image is called selective encryption also acknowledged as partial encryption, soft encryption or perceptual encryption. The primary inspiration is to lessen the computation time for real-time applications that runtime performance is frequently serious deprived of compromising the security of the broadcast moreover. The primary objective is to divide the image content into two shares, public share and protected share. One significant feature in selective encryption is to decrease the protected part to least as it can be. Selective encryption generally accompanies compression. In frequency domain, low frequency coefficients convey most of the data of the image and high frequency coefficients convey the fine points [16].

In lossy compression techniques for example JPEG standard, an image changes to a frequency domain by DCT and at that point roughly high frequency coefficients are reproduced by zeros and new compressed image is recreated. Therefore only few low frequency coefficients can be encrypt relatively than all in frequency domain that also has many benefits [17]:

- It is less demanding to recognize the critical parts to be encrypted

- It is less demanding to recognize parts of the information are not compressible.

In 1995, Maples et al. did the very first studies on selective multimedia encryption [18] by recommending Aegis mechanism focused around MPEG video transmission and DES cryptosystem to secure MPEG video sequences from unauthorized access.

This instrument cut off points the measure about information to be encrypted or decrypted toward utilizing feature layering to decrease the measure from claiming transmitted video images by encrypting intra I frames about an MPEG stream anyhow Agi and Gong [19] discovered that this and some other systems would not sufficient to touchy provisions furthermore might not make sufficiently secure for exactly sorts of video Also person can perceive example from movement patterns with the goal they attempted to move forward those security toward progress of I-frame

frequency yet it reasons to increase in transfer speed utilization and also higher computational multifaceted nature. An elective approach will be to encrypting I-blocks on the whole frames rather that I-frames that enhances security. Droogen broeck likewise suggested two strategies to particular encryption from claiming both compacted also uncompressed images [20].

A selective encryption approach for uncompressed image is to encrypt 4 to 5 least significant bits because it is random like and plaintext attack on random like data is harder. Another selective encryption method that mentioned in this paper is based on compressed JPEG images and encrypts a selected number of AC coefficients. Results on execution time on three different encryption algorithms (DES, 3-DES and IDEA) show that real-time processing is easily achievable. Another technique for real-time applications by Droogen broeck [21] that encrypts appended bits corresponding to a selected number of AC coefficients for each DCT block and he concluded that this scheme provides flexibility, multiplicity, spatial selectivity and format compliance.

A multilevel partial image encryption (MPIE) proposed in [22] that performs the encryption before compression. Encryption is performed on parts of low frequency coefficients that determined by Haar Wavelet, and DFT applied on the approximation coefficients and a permutation matrix as encryption key is used to permute the result of transformation and then compression is doing by Huffman coding. Regardless of limitations such as complexity, low rate of compression and time consuming of this algorithm, some advantages are security, flexibility to image transformations and compression techniques.

Another different approach in partial image encryption is to extract some special and secret features in an image and encrypt these features rather than encrypting the whole image. An idea in this scope is to detect faces of input image and encrypt them, for some applications such as transmission of images with guilty, accused persons or members of security organizations or military applications. K. Hong and K. Jung [23] proposed a partial encryption method using the face region as a feature because a face has the semantic information and is the most important part in an image or video. They used Multi-Layer Perceptron's to detect face region and for more exact, Gaussian skin-color applied to discriminate between skin regions and non-skin regions.

Both DES and AES encryption algorithms are compared and results shows that encryption time is less for DES. Due to experiments, for video content encryption, fully encryption methods provide 2 or 3 frames in a second but their proposed method encrypts 25 to 30 frames per seconds. A different scheme by J. M. Rodrigues et al. [24] for selective encryption Bin video offered also for face protection based on AES stream cipher for JPEG image sequences by performing three steps on DCT blocks. These steps are respectively construction of plain text, ciphering the plain text and substitution of the original Huffmans vector with the ciphered information. This scheme provides advantages such as portability, constant bit rate and selective encryption of the region of interest and does not effects on all the JPEG compression rate, which makes it useful for a large range of applications with good information confidentiality results. JPEG2000 is a widely used compression standard based on wavelet transform. S. Lian et al. [25] proposed a selective image encryption scheme based on JPEG2000.

They lessened the encryption information ratio to short of what 20% by selecting huge bit-planes of wavelet coefficients in high and low frequency, so the encryption time proportion decrease by to short of what 12%. Their examinations demonstrate the security of their plan against savage power assault, select- plaintext assault or substitution assault and does not consequences for pressure proportion. An alternate late specific encryption focused around wavelet change in fractional wavelet area distributed by N. Taneja et al. [26]. In this work, 3.125% of noteworthy image information chose by normalized information energy (NIE) and encoded these chose sub groups by Arnold cat map, a 2D chaotic function.

1.3.5 Chaos Theory And Cryptography

Chaos hypothesis is the investigation of nonlinear dynamical frameworks that are display compelling affectability to starting conditions and have arbitrary like practices, founded by Edward Lorenz in 1963 [27], an impact which is prominently alluded to as the butterfly impact that has a definition: Does the fold of a butterfly's wings in Brazil set off a tornado in Texas? The fluttering wings speak to a little change in the starting state of the framework, which causes a bind of

occasions prompting extensive scale phenomena. Had the butterfly not fluttered its wings, the trajectory of the framework may have been immensely distinctive [28].

For the most part it implies that little contrasts in beginning conditions, (for example, those because of adjusting errors in numerical calculation) yield generally separating results for chaotic systems, interpreting long-term prediction usually intolerable. This happens despite the fact that these frameworks or systems are deterministic, implying that their future conduct is completely dictated by their starting conditions, with no arbitrary components included. At the end of the day, the deterministic nature of these frameworks or systems makes them volatile [28].

According to [29], there are two general ways to apply a chaos map in a cipher system:

- Using chaotic systems to generate pseudo-random key stream which corresponds to stream ciphers.
- Using the plaintext or the secret key(s) as the preliminary conditions and control parameters then apply some iterations on chaotic systems to obtain cipher-text corresponding to the block ciphers.

This conduct is known as deterministic chaos, or basically chaos. Irregular like conduct, non-anticipating and affectability to preliminary value are three features that make it an adequate choice to relate it with cryptography. The main distinction is that encryption operations are characterized on limited sets of numbers while chaos maps are characterized on true numbers. Chaotic behaviors are displays by chaotic maps. These maps are grouped by non-stop maps and discrete maps. Discrete maps typically take the manifestation of iterated functions. Iterates are like rounds in cryptosystems, so discrete chaotic dynamic systems are utilized as a part of cryptography. Every map consist of parameters which are correspondent to the encryption key in cryptography.

As per [29], there are two general approaches to apply a chaos map in a cipher system:

• Chaotic systems utilization for production of pseudo-arbitrary key stream which compares to stream ciphers.

- Utilization of the plaintext or the mystery key(s) as the preliminary conditions and control parameters then apply a few cycles on chaotic systems to acquire cipher content relating to the block ciphers

1.3.6 Digital Signature for Image Authentication

The demonstration of digital signature is like manually written on paper signature which assuming the principle part in validating reports and confirm the individuality. Subsequently, digital signature has numerous applications in data security. It is a system that offer verification, information reliability and on-revocation. Several years ago the first idea of digital signature was a plan focused on RSA [30] and today it is a standout amongst the most functional procedures.

The greater part of the digital signatures are focused around asymmetric cryptography. In these frameworks, the private key is utilized to make a digital signature that particularly proofs the underwriter who is holder of the private key and can be verified just with the relating public key. In 1998, C. Yung Lin and S. Chang put out an article which was one of the first studies on digital signature and its applications in images [31]. They proposed a vigorous digital signature focused around DCT coefficients in JPEG images. This produced digital signature is vigorous to trimming, strength changes, resizable and filter applicable.

Digital signature and watermarking are connected and both utilized for verification and confirmation however there is somewhat contrasts in their structure. Tao Chen et al. attempted to consolidate digital signature with watermarking [32]. The preference of this consolidation is to spare the obliged data transfer capacity for signature which is encoded to a different record. To attain this point, they install the signature record as a watermark, so their proposed plan can be able to verify the image, as well as can perform a copyright security. An alternate image verification plan [33] utilize the substance of an image wavelet change space to develop a structural

digital signature. They demonstrated that this plan is forceful to content stabilizing controls and delicate to content evolving alterations.

H. Zang et al. proposed a plan focused around an arrangement of comprehensive synchronization Henon discrete-time chaotic system which utilizes as a pseudo-arbitrary number generator to build encryption and digital signature. [34]. The enormous key space as 10158, affectability to misperception of parameters and preliminary condition on account of applying chaos in encryption make this plan certain to be utilized as a part of secure correspondence.

1.4 SECURITY ANALYSIS OF ENCRYPTED IMAGE

Security investigation is the specialty of discover the shortcoming of a cryptosystem and recovery of entire or a piece of a ciphered message (here we consider an image) or discovering the mystery key without knowing the decryption key or the algorithm. There are numerous methods to investigate, contingent upon what access the expert has to the plaintext, cipher content, or different parts of the cryptosystem. The following are probably the most widely recognized sorts of assaults on encrypted images:

1.4.1 Key Space Analysis

Attempt to discover the decryption key by checking all conceivable keys. The quantity of attempt to discover specifically denotes to key space of the cryptosystem become exponentially with aggregate key size. It implies that multiplying the key size for an algorithm does not just twice over the obliged number of operations, but instead squares them. An encryption algorithm with a 128 bit in key size characterizes a key space of 2128, which takes around 1021 years to check all the conceivable keys, with superior computers of these days. So a cryptosystem with key size of 128 bit computationally looks powerful against a beast energy assault.

1.4.2 Statistical Analysis

Original and encrypted image relationship can be determined by analysing data statistically. In this manner, image after encryption must be totally differentiate from the original. Because of Shannon hypothesis. It is conceivable to illuminate numerous sorts of images by statistical investigation. For a image there are a few approaches to figure out if the ciphered image releases any data about the first one or not.

1.4.3 Correlation Analysis

Two contiguous pixels in a plain image are intensively corresponded vertically and on a level plane. The most extreme estimation of relationship coefficient is 1 and the base is 0 considered as the property of an image, where a strong image that has been encrypted to measurable assault ought to have a connection coefficient estimation of 0.

1.4.4 Differential Analysis

The point of this examination is to focus the affectability of encryption algorithm to minor changes. On the off chance that an challenger can make a little change (e.g. one pixel) in the plain image to watch the results, this control ought to cause a noteworthy change in the image that has been encrypted and the challenger ought not to have the capacity to discover a compelling relationship between the original and the image that has been encrypted as for distribution and misperception, the distinct assault loses its productivity and get to be inadequate..

1.4.5 Key Sensitivity Analysis

Moreover of vast enough key space to oppose a cryptosystem at brute force attack, additionally a protected algorithm ought to be totally delicate to mystery key which implies that the encrypted image can't be decrypted by somewhat changes in mystery key.

CHAPTER 2

2 THEORY

2.1 Chaos System

To gain a consistent method for encryption has been always in need even all over the past. Several encryption applications are in an assortment from defense and intelligences utilize in profitable undertakings on daily basis. An expertise has enhanced to take into account simpler and improved encryption and transmission, hence it has also permitted the development in interception and cryptanalysis. Codes have been turn out to be further progressive, developing from simple character replacement ciphers to today's algorithm of large pseudo-primes, exponents, and particular consistency.

In any case the idea has stayed basic; it is anticipated to have the capacity to send data starting with one point then onto the next without any one having the capacity to comprehend it in the mid. The appearance of the web has made security of information and assurance of protection a significant reason for concern toward anybody. The profoundly eccentric and irregular look nature of chaotic signals is the most tempting feature of deterministic chaotic system that may prompt to as novel applications. With the quick advancement of the computer innovation and data processing technology, the issue of data security is constantly more imperative. Data hiding away is normally used to secure the imperative data from unveiling when it is transmitting over an uncertain channel. Computerized image encryption is a standout amongst the most vital systems for image data.

The image encryption methods chiefly incorporate compression approach, cryptography system, chaos strategies, and DNA procedures etc. Cryptography and chaos have some regular peculiarities, which is debated in consequent segment. With the progression of portable correspondence technologies, the usage of varying audiovisual data in account with textile data

gets to be more common than the past. Cryptography methodologies are in this way essential for storage of secured media content and circulation over open systems, for example, the web. A conventional approach to oppose statically and differential cryptanalysis is to utilize transformation and dispersion on the other hand.

Chaotic cryptography depicts the utilization of chaos hypothesis (specifically physical dynamical systems working in chaotic administration as a component of correspondence methods and processing algorithms) to accomplish diverse cryptographic assignments in a cryptographic system.

The ability of creating truly perplexing examples of conduct is an astonishing characteristic of chaotic systems. This is carried out from straightforward genuine systems or in recreations from low dimensional systems given by a little set of development mathematical equations. This quality has made them especially valuable for application in a wide variation of restraints, for example, science, commercial concerns, engineering and others [35][36]. Chaotic systems are utilized to create, reproduce, support or control diverse techniques enhancing their execution or giving a more suitable yield, in these sort of applications.

The utilization of chaos in cryptography appears to be very regular, as its characteristic properties unite it specifically with cryptographic qualities of perplexity and dispersion. This thought is available in Shannon's works (Shannon, 1949), much sooner than the expression "chaos" showed up in logical writing. Furthermore, chaotic dynamical systems have the focal point of giving qualitatively straightforward systems to produce deterministic pseudo arbitrariness. This could be the guarantee of creating more straightforward or better arbitrariness regarding execution for cryptography [37].

At this point, the historical backdrop of chaos based cryptography is more than twenty years long. To start with, a few works show up in the 80's [38] [39], however it is in the 90's, when chaotic cryptography truly profits off. As an outcome, chaotic cryptography has been a dynamic exploration field yet with minimal effect in traditional cryptography [40] [41].

2.2 Chaos and Cryptography

Fundamental concepts of chaos theory is explained in this segment. Focusing on those characteristics which tends to be important for its implementation in cryptography. Certainly the introduction starts with basic concept of chaotic systems, and then it will lead to practical implementation through non-linear dynamical systems. Hence this part of theory will accomplish to describe the relationship importance between chaos schemes in cryptographic applications.

2.3 Basic Properties of Chaotic Systems

Chaos has been seen to be involved in various natural and laboratory systems (Sneyers, 1997; May, 1976; Casperson, 1988; Kyrtsou & Vorlow, 2005; van der Pol & van der Mark, 1927) where a significant number of scientific and engineering areas (physics, biology, meteorology, ecology, electronics, computer science and economy, among others) has been involved. As stated earlier these singularities, demonstrate particular properties that mark them difficult and impulsive.

Chaos system manages with schemes that develop in time with a specific sort of dynamical action. As this is an enormous mathematical concept, the concerned reader is tended to [42] for a more extensive presentation. Normally, these type of systems follow some particular laws of evolution, and so, they are deterministic. It must be said, that chaos happens only in some deterministic non-linear systems. Obviously, chaos give the impression as if there is a nonstop and disorderly-looking elongated evolution that fulfills certain mathematical standards.

There is a set of features that encapsulate the characteristics perceived in chaotic systems. These are deliberated as the mathematical standards that define chaos. The most appropriate ones are:

•**Dynamic instability**: Also mentioned as butterfly effect, it is the property of sensitivity to preliminary state of affairs, where two randomly closed preliminary situations progress with considerably dissimilar and deviating trajectories [43].

•**Topological mixing**: spontaneously represented as mixing colored dyes, which explains that the system will progress in time so that any specified section of states is constantly converted or overlaps with any other specified section [44].

•**A periodicity**: the system progresses in an orbit that on no occasion replicates itself, that is, these orbits are never periodic [45].

•**Dense periodic orbits**: it explains that the system follows a dynamics that can diligently approach every potential asymptotic state in random.

•**Ergodicity**: arithmetical capacities of the variables give related outcomes no matter if they are executed over time or space. Other way around, the dynamics indicates alike statistics when measured over time or space.

•**Self-similarity**: the progression of the system, in time or space, demonstrates the similar presence at dissimilar scales of observation. This distinguishing feature creates the system to appear auto-repetitive at dissimilar scales of observation [46].

2.4 Non-Linear Dynamical Systems (NLDS)

A dynamical system is a somatic phenomenon that progresses in time. In mathematical terms, the positions of the system are pronounced by a set of variables and its progression is specified by an equation and the value of the initial state. This is summarized in Eq. (1),

$$\frac{dX_i(t)}{dt} = F_i(X_j(t), \Lambda) \quad \text{..... (1)}$$

Where

X_i (t) ЄRN = coordinate i of the state of the system at instant t,

X = N-dimensional vector with i, j=0, 1…N with N≥1,

F = parametric function that describes the evolution of the system and

Λ = vector of parameters that control the evolution of the system.

As chaotic systems simply take place in non-linear dynamical systems, F will be deliberated to be non-linear. The intentions are focused on discrete-time NLDS for digital cryptographic applications. At that point, a discrete-time NLDS is specified by the following equation:

$$X_{i+1} = F(X_i, \Lambda) \qquad \text{……………………………………………. (2)}$$

The consequence of the mathematical symbols in Eq. (2) is the same as in Eq. (1) but at this instant the time t is discrete. It is perceived that this type of system is deterministic, therefore the time progression of X can be calculated with F and Λ from a specified initial state X0. They are similarly recursive, as the following state is calculated from the prior state.

Learning of NLDS develop distinctive attention towards sequences of concepts and terms. The one to begin with is the phase space that is the subspace of RN, where all potential states of the system are restrained:

$$U \subset R^N \text{ and } F: U \rightarrow U$$

Where N is the dimension of the phase space or degree of freedom of the system. The progression in space of a preliminary state when time passes is termed as orbit. As F is considered as a discrete-time function, the orbits of these systems will be an assortment of actual pairs of numbers:

$$(t_0, X_0), (t_1, F(X_0)), \ldots, (t_i, F_i(X_0)), \ldots$$

The attractor is the dominant concept in chaos scheme. The word attractor mentions to the elongated behavior of the orbits, and it signifies the region of phase space where the orbits of the system come together after the transient. The attractor A is a dense region where all orbits come together and where the system gets confined,

$$A \subset U \quad and \; A = F(A)$$

An attractor can be a point, a curve, a manifold, or even a complex set with a fractal structure identified as a strange attractor from geometrical point of view. A transitory explanation of them is as follows:

- **Fixed point,** it relates to a stationary state of the system.

- **Limit cycle,** which is related with a periodic conduct of the system. Once the system arrives with in the attractor the states of the system starts periodic recurrence.

- **Manifold,** where there are more than one frequency in the periodic trajectories of the system. For example, in the case of two frequencies, the attractor is a 2D-torus.

- **Strange attractor,** it is informally said to have a complex geometric shape with non- integer dimension. Any state in the attractor evolves within it and never converges to a fixed point, limit cycle or manifold. The dynamics on this attractor is normally chaotic, but there exist also strange attractors that are not chaotic [44].

Coming around the inspection of the fundamental standard for NLDS, one could characterize the term chaotic system as an issue that have at any rate a confused weird chaotic attractor. NLDS are typically considered on just in a subjective and computational way, rather than the investigation of linear systems, where there is a situation of scientific instruments inclusion [47]. Distinctive models of N-dimensional discrete-time mappings have been considered on, and in specific situations complex conduct in time development has been demonstrated. The 1-dimensional cases have been deeper investigated [48], instances of N=2 have likewise a few generally investigated samples [49] and [50], however as N expands, the unpredictability develops and less writing is found with a decently archived examination of the chaotic properties of the mapping [51].

2.5 Connection between Chaos and Cryptography

Chaotic systems are executed with deterministic NLDS, having the capacity to deliver the deterministic pseudo-haphazardness needed in cryptography. Apart from that, NLDS have the capacity to produce complex configurations of advancement. This provides for chaotic systems the algorithmic intricacy needed in cryptographic systems.

The characteristic properties of chaos join it straightforwardly with cryptographic attributes of perplexity and dissemination (Shannon, 1949). Indicating the properties deliberated about the chaotic systems, it is clear that the properties of periodicity, auto resemblance, topological blending are straightforwardly joined with misperception. The elements in the chaotic attractor is given by aperiodic circles that produce comparable statistical arrangements. These arrangements can be utilized to cover clear messages by method for substitution-like procedures.

Then again, dissemination is nearly associated with the affectability that chaotic systems present to introductory conditions and control parameters. Dispersion creates the avalanche slide impact, where a base distinction in the contribution of the cryptosystem gives a totally distinctive yield. A chaotic system creates this conduct when a little change is connected to its introductory conditions or control parameters. The utilization of these variables as contribution in the cryptosystem calculation may deliver the same avalanche slide impact.

2.5.1 Comparison of Chaotic and Cryptographic Properties

In the review article of 2006, Alvarez & Li have made the comparison between the two very clearly [52]:

- Periodicity, Mixing property and Auto- similarity in chaotic compare with the confusion in cryptography where the output of the system seems similar for any input.

- Sensitivity to introductory conditions and control parameters in chaotic relate to Diffusion in cryptography where a small difference in the input produces a very different output.

- Deterministic property of chaotic relate to deterministic pseudo randomness where a deterministic procedure is one that produces pseudo randomness.

- Complexity of chaotic relates to algorithmic complexity of cryptography where a simple algorithm produces highly complex outputs.

2.6 Review of Chaos Based Encryption Techniques

Appreciated summaries with conforming references can be found in [53]. It is essential as well, to have in mind that it is a dynamic area of research and modern enlargements requisite some time to consider their security.

CATEGORY	METHOD	DESCRIPTION	
Analog cryptosystems	Additive chaos masking	A chaotic signal is added to the message	
	Chaotic shift keying	A digital message signal switches among different chaotic systems to be added to the message	
	Chaotic modulation	A message signal is used to change the parameters or the phase space of the chaotic transmitter	
	Chaotic Control	A message signal is ciphered in a classical way and used to perturbate the chaotic system	
Digital cryptosystems	Stream ciphers	Chaotic PRNG	A chaotic signal generates a pseudorandom sequence (keystream) to XORed the message
		Chaotic Inverse System approach	A message signal is added to the output of the chaotic signal, which has been feeded by the ciphered message signal in previous instants
	Block ciphers	Backwards iterative	A block of a clear message is ciphered using of inverse chaotic systems
		Forwards iterative	A block of ciphered message is obtained by pseudoramdom permutations obtained from a chaotic system
		S-Boxes	An S-Box is created from the chaotic system. There can be dynamic or static S-Boxes
	Miscellaneous	Searching based chaotic ciphers	A table of characters is generated from a chaotic system. The table is used to cipher the characters of the message text
		Cell. Automata	The chaotic system is a Cellular Automata

Table 1: Different kinds of chaos based cryptosystems presented in literature

As it is seen in Table 1, the submission of chaotic systems to cryptography has surveyed two main methodologies. These have been known as, analogue and digital techniques [52].

Chaos is a clear truth that happens in nonlinear determinable systems touchy to starting conditions and has a pseudo-irregular activity. Dynamic chaotic systems if they face an occurrence of Liapunov exponential mathematical statements, will stay steady in chaos mode. It is the pseudo-arbitrary conduct that has brought about this recognizable reality to consider for several cryptographic systems. Because of pseudo-arbitrary character, the yield of the vision system look like irregular in ‘attackers' perspective, while in beneficiary's view, the system can be characterized and decryption is conceivable. Many chaos based cryptographic algorithms are exhibited till now and some of them are by one means or another being used in the way that they are fit for image

encryption and additionally message encryption. An image encryption framework must have suitable pace for image gigantic information ciphering.

Consequently, one of the most important benefit of chaotic system's comprehension is simplified key management methodology meanwhile this method just have need of protection and secure transmission of secret key (parameters and initial values of chaotic system), which has a uncertain capacity and as a consequence not only a minor memory is preferred to uphold it but also there is further assurance throughout its transfer. The illegal access to short length keys is remarkably not as much of potential as the large length keys in the course of information transmission through the insecure channel.

2.7 Architecture of Chaotic Image Cryptosystems

A distinctive structural design of prevailing chaos-based image cryptosystems is presented in Fig. 4. It comprises of two phases, namely; confusion and diffusion phases. In the confusion phase, permutations of image pixels are prepared in a secret demand, deprived of varying their values. The purpose of the diffusion phase is to alter the pixel values in sequence so that a small alteration in one pixel is blowout out to several pixels, with looking forward to the whole image. To disassociate the affiliation among adjacent pixels, the confusion phase is performed n times, where n is usually larger than 1, monitored by the diffusion phase. The comprehensive n-round confusion and single round diffusion replicate from times, with m typically higher than 1, so as to acquire a satisfactory level of security. The constraints of the chaotic maps primary to the permutation and the diffusion should better be unrelated in diverse rounds. This is achieved by a round key generator with a seed secret key as input.

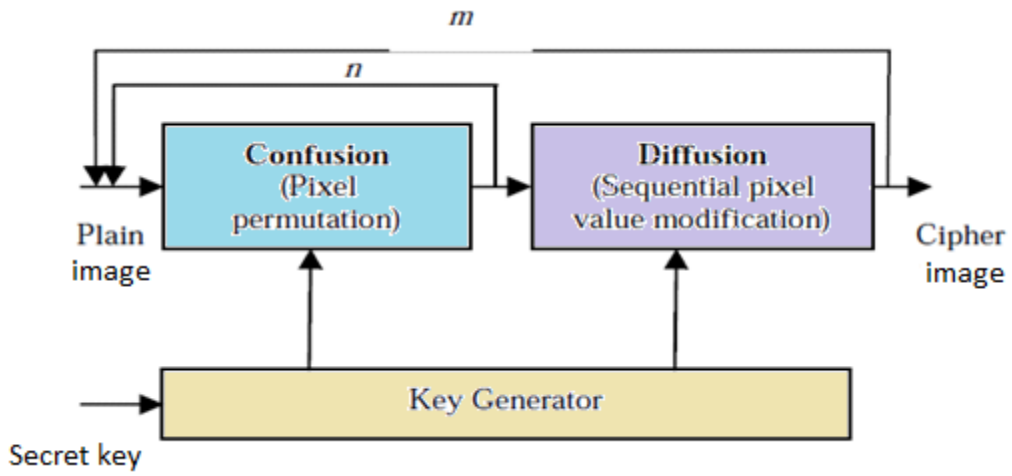


Figure 4: Typical Architecture of Chaos Based Image Cryptosystems

2.7.1 Selection of Right Chaotic Map

Chaotic system can be deliberated as source of unpredictability and chaos is unpredictability of a deterministic dynamical system. Mathematically A chaotic map can be distinct as

$X_{n+1} = f(X_n)$

Where $0<X_n<1$ and n=0, 1, 2…

Chaotic arrangement can be utilized as arbitrary number succession and spread spectrum arrangement. The chaotic systems are portrayed being the non-direct and impulsive. They seem to be irregularly arranged but in reality there exist a definite arrangement. Chaotic systems are profound to preliminary conditions, minor variation in initial point can be a source of dissimilar results. Chaos has numerous applications in modulation, compression, and encryption. In image encryption, 1-D chaotic system consuming logistic maps has easiness and great effectiveness but it has weak security and small key space. Unalike Chaotic maps can be utilized for this reason.

Pixels of image are scrambled and correspondence between pixels is reduced to acquire encrypted image usually in chaos based algorithm.

It is difficult to select right chaotic maps for encryption algorithms and one should consider just those maps which have the subsequent properties like mixing, robust chaos and huge parameter set [54].

- Mixing property: Mixing property of chaotic maps is very considerably linked with the property of diffusion in encryption algorithms. Assume that the set of potential (sensible) plaintexts as an initial region in the phase space of the map (transformation), then it is considered as the mixing property (or in other terms, sensitivity to initial conditions) which indicates scattering out of the effect of a single plaintext digit over several ciphers text digits.

- Robust chaos: An upright encryption algorithm should extent the effect of a single key digit over several digits of cipher text. The keys represent constraints of an encryption algorithm. For that reason, we should visualize almost those transformations in which parameters and variables are mutually concerned in a subtle approach.

- Parameter set: Huge parameter space of the dynamical system indicates that its distinguished description will have bigger keys.

2.7.2 Chaotic Maps Used For Image Encryption

- **Arnold cat map**: This map was proven by Vladimir Arnold in 1960s by means of consuming an image of a cat. Arnold cat map utilizes the theory of linear algebra to bring a variation in the position of pixels of original image. Original image is allocated into blocks and then Arnold transformation is completed.

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

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

About conditions such as p and q are positive integers and

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

This sort it as area-preserving. Original image can be shuffled through spread over the Arnold map operation repeatedly. But shuffled image can make a reappearance to original form after numerous repetitions.

- **Logistic map**: 1-D logistic map was recommended by RM may. This map is simply a non- linear chaotic system which can be distinctly defined as

$z_{n+1} = \lambda\, z_n\, (1-z_n)$……..(3)

Where z0 is initial state, n is number of iterations and λ is system parameter. For $3.57 < \lambda < 4$ map is deliberated as chaotic .And z_{n+1} belong to (0, 1) for all n. equation 1 is utilized to encrypt the shuffled pixels.

- **Sine map**: sine map is defined as

$X_{n+1} = a\, x_n^{\,2} \sin(\pi\, x_n)$ …….. (4)

When $x_0 = 0.7$ and a=2.3, equation 3 has the simplified form. For the interval (0, 1) it produces chaotic sequence.

- **Tent map:** tent map is similar to the logistic map. It produces chaotic sequences in (0,1) assuming the subsequent equation

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

Where μ is a positive number and reliant on its value which is found from tent map exhibiting dynamic behavior ranging from predictable to chaotic.

- **Circle map**: it is defined as

$X_{n+1} = X_n + d - (c/2\pi) \sin(2\pi X_n) \bmod (1)$…… (5)

Where d = 0.2, c = 0.5, and x0 € [0, 1] produces Chaotic sequence in [0, 1].

2.8 Chaotic Image Encryption

The properties of chaos consist of random performance, deterministic dynamics, and non-linear transform and can be utilized for chaotic image encryption. This theory give indications to techniques that can instantaneously propose security functions and an general visual check, which might be suitable in some applications. Digital images are extensively used in numerous applications, as for example military, legal and medical systems and these applications demand monitoring access to images and giving the means to authorize reliability of images. Block encryption is a type of scheme where the plain text is allocated into blocks of fixed length, and one block is encrypted at a time. However, stream ciphers are centered on producing an "infinite" cryptographic key stream, and utilize this key stream to encrypt one bit or byte at a time. The Table 2 shows the review of Block and Stream cipher image encryption schemes making an allowance for the parameters deliberated by the many researchers in their effort.

CHAOTIC BLOCK ENCRYPTION SCHEMES			
S. No.	*Authors& Year*	*Chaotic map used*	*Remarks*
1	G. Jakimoski and L.Kocarev (2001)	Exponential and logistic maps	A block encryption uses a procedure to create chaos based ciphers. The two chaotic maps, exponential and logistic, defined on the unit interval by $x \rightarrow \alpha^x \bmod 1$ and $x \rightarrow 4x(1-x)$, respectively, are used for this purpose.
2	Y.B. Mao, G. Chen, S.G. Lian (2004)	2D baker map	2D baker map is extended to be 3D and is then used to compose a fast and secure image encryption scheme.
3	H. Gao, Y. Zhang, S. Liang, and D. Li (2006)	A new non-linear chaotic algorithm (NCA)	The scheme uses power function and tangent function instead of linear function. An experimental analysis is done to obtain the structural parameters and an image encryption algorithm based on one-time-one-password system is designed.
4	S. S. Maung, and M. M. Sein (2008)	Logistic and 2D standard map	A fast encryption scheme based on chaotic maps is proposed. Firstly the dynamical 8×8 S-box is formed by using logistic map and 2D standard map. Secondly a sequence of pseudo-random bytes is generated by using 2D chaotic cat map to index the entries of the S-box. The output bytes from the S-box are XOR-ed with the plaintext to produce the cipher text.
5	M. Ahmad and M. S. Alam (2009)	2D cat map and logistic map	The plain image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map. The shuffled image is encrypted using chaotic sequence generated by one dimensional logistic map.
6	F.Wang, Y.Zhang and T.Cao (2009)	logistic map	This technique produces chaotic stream based on logistic map. The system parameter of logistic map is produced by m-sequence, and using another m-sequence's perturbation to augment the period of logistic mapping sequence. An output feedback mechanism is also provided in the system.

CHAOTIC STREAM ENCRYPTION SCHEMES			
.1	J. Yen, and J. Guo (2000)	Chaotic binary sequence	This paper presents an image encryption/decryption algorithm and its VLSI architecture. The gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. Its features are as follows: (1) low computational complexity, (2) high security, and (3) no distortion.
2	P. Pei and Y. Chen (2003)	2D map	They use a known chaotic dynamical system to generate a sequence of pseudo-random bytes, and then apply certain permutations to them, using the discredited version of another two-dimensional chaotic map.
3	Socek, D et. al. (2005)	piecewise linear chaotic map (PWLCM)	They enhanced the CKBA algorithm in three-ways: 1) change the 1-D chaotic Logistic map to a piecewise linear chaotic map (PWLCM) to improve the balance property, 2) increase the key size to 128 bits, and 3) 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. The new cipher has much stronger security and its performance characteristics remain very good.
4	D. Rao and K. Gangadhar (2007)	piecewise linear chaotic map (PWLCM)	They proposed an algorithm to enhance the security of CKBA.
5	H.E.H. Ahmed, H.M. Kalash, and O.S.F. Allah (2007)	logistic map	They proposed a method based on the use of a chaotic logistic map and an external secret key of 256-bit. Use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms are additional features of the system.
6	S. Liu, J.Sun, Z.Xu (2009)	logistic map	The system consists of a key stream generator that generates the satisfied random number which is XOR-ed with the plaintext in binary format.
7	A.Awad, A.Saadane (2010)	piecewise linear chaotic map (PWLCM)	The system is based on piecewise linear chaotic map (PWLCM) perturbed by a new technique. Both chaotic maps are then used to control three bit-permutation methods having good inherent cryptographic properties.
8	Ai-hongZhu, Lia L (2010)	logistic map	They presented a new algorithm that produced nine chaotic sequences with the help of only one secret-key, six sequences were used to scramble the position of image pixels, and the others were used to confuse and diffuse image pixels value.

Table 2: Review of Block and Stream cipher image encryption schemes

The first chaotic encryption algorithm was suggested by Matthews in 1989. Afterwards, investigations on chaos-based encryption were done and one of these primarily studies was completed by Baptista [55]. Simple one-dimensional logistic map was utilized to encrypt each character of a text message as the integer number of iterations accomplished in the logistic equation.

Ge Xin et al. attempted to examine Baptistas cryptosystem [56] and inferred that it has 2 imperfections, first is that the encryption rapidity is moderate in correlation with routine cryptosystems due to substantial number of iterations and then again the proposed strategy is not

powerful to known-plaintext attack, however it was the source of using chaos in cryptography. M. Sharma and M. Kowar in their article [57] grouped image encryption focused around chaotic plan in two assemblies: Spatial Domain and Frequency Domain. In spatial space, Fridrichs distributed research [58], [59] was one of the first on chaos based image cryptography in 1997. J.

Yen and J. Guo [60] offered an algorithm which as indicated by a chaotic binary sequence, the encrypted image created by the gray level of every pixel is XORed or XNORed bit by bit to one of the two prearranged keys. Works on chaotic image encryption has been developed by trying different chaotic maps to overcome the traditional cryptosystem disadvantages and this technique found adequate for image encryption due to speed and strong security.

A chaotic image encryption utilizing Lorenz map by Sobhy [61] was anticipated with application in image encryption, making secure databases and secure Email which executed in FPGA for actual time images. One dimensional chaotic equation is an alternative map which is utilized by F. Belkhouche and U. Qidwai [62]. It has been presented that the strategy can be utilized for two-fold image encryption with the probability of expending numerous keys for example, the preliminary state, the peripheral parameters and the number of repetitions.

Z. Han and W. Xiu Feng have worked on non-linear map used for iterating pixel values [63]. D. Shaojiang have lightened up Cat map collectively with neural network [64] and Arnold map by M. R. Zhang et al. [65] are additional discrete chaotic maps which are utilized for an image encryption. Yi Wei et al. in their innovative image encryption algorithm [66] united two chaotic maps and offered an alternative structure to accomplish greater strength somewhat than using one chaotic map.

Chaotic functions in this scheme are one-way coupled map lattice (OCML) utilized for replacement and common cat-map for transformation and dispersion. These maps are useful in every round of encryption interchangeably and this arrangement outcomes as a enormous key space and oppose to statistical attacks as research presented. Three different chaotic maps were utilized for image encryption by M. Ahmad and M. S. Alam [67].

Spreading over 2D cat map on 8*8 blocks of an image to accomplish shuffling pixels, producing control parameters of shuffling arbitrarily by 2D coupled logistic map and as a final point encrypting the shuffled image by 1D Logistic map consequences into a very low correspondence and data entropy appropriately adjacent to 8. As a result, there is no data leakage from encrypted image in this arrangement.

An alternate creation of chaotic maps [68] is focused around two logistic maps with distinctive beginning parameters to develop the key size as 104 bit and make the encoded image sheltered to diverse sorts of attacks. At long last a blend of three encryption algorithms entitled as Triple-Key chaotic is presented by G. Srividya and P. Nandakumar [69] in 2011. These three keys are an 80-bit session key, preliminary parameter key and control parameter key. To execute their own particular plan, they join two former works [70], [71] which were focused around logistic chaotic map and chaotic neural network correspondingly then utilizing these maps to perform position permutation and value transformation of image pixels to accomplish high security as their histogram investigation, association investigation and key affectability analysis where the outcomes are exhibited.

2.9 Review of Parameters for Existing Chaotic Encryption Schemes

Different researchers have suggested various parameters to estimate the performance of chaotic cryptographic system utilized for image encryption. The performance of various systems proposed by researchers are deliberated in Table given below.

Usually, cryptographic techniques are focused around number theory and algebraic notations but Chaotic procedures be determined by huge numbers (chaos) be appropriate for nonlinear dynamics field. Chaotic encryption tracks on deterministic dynamics, non-predictable behavior with non-linear functions and chaos features. The performance is most important factor somewhat for all cryptographic technique. The noticeable concern is that different authors have divergent opinions for estimating chaotic encryption techniques even the number of factors and their nature is also diverge from individual to individual.

S. No.	*Performance factors considered*	*Outcome*
.1	• Simplicity • security	• The cipher use only one byte operation that can be easily implemented on various processors and hardware's. • S-Boxes are generated by chaotic maps and discredited procedures presented in this paper are more secure. There exists no more efficient attack to these ciphers than brute force.
2	• Speed • Resistance to various kown attacks • Key space • Key sensitivity	• The use of 3D Baker map speed up the image encryption process. • It is resistant to following attacks: known plain text attack, cipher text only attack, differential and brute force attacks. • It has larger key space, about 2^{128}. • Key sensitivity is so high such that a one bit difference in key results in 99.59% difference in encrypted image.
3	• Speed • key space • key sensitivity • histogram • pixel correlation and • resistance to known attacks	• 0.5s speed • large key space • high key sensitivity • histogram of encrypted image are uniform and different from the original one. • zero correlation • It is resistant to gray code, statistical and brute force attacks.
4	• confusion and diffusion properties • correlation coefficient • histogram.	• algorithm achieved good confusion and diffusion properties • correlation coefficient between source and cipher was found to be 0.00041818. • histogram of encrypted image are uniform and different from the original one
5	• balance property • key space • correlation coefficient • information entropy	• distribution of gray scale value of image has good balance property • Key space is about 10^{112} • Correlation coefficients are close to zero • Information entropy is close to ideal entropy, so leakage of information is negligible.
6	• probability distribution • complexity • cipher sensitivity	• probability distribution of cipher text is uniform and resistant to statistical attack • cipher text has high non-linear mapping with the plain text which makes it more secure • cipher is highly sensitive to plain text due to additional output feedback
7	• Speed • Random number • Key space	• It is fast, in the sense that it can effectively exploit the intrinsic chaosof simple deterministic systems. • generate a high percentage of usable random numbers • maintaining a large enough key space
8	• Speed • precision	• the running time of the encryption / decryption algorithm increases • precision of CKBA was kept at 16 bit, while that of ECKBA is 32 bits
9	• resistance to known attacks as performance measures.	• Reduces the chosen/known-plaintext attacks and cipher text-only attacks faced by CKBA.
10	• speed	• average encryption/decryption speed is 7.46 MB/Sec for encryption and 6.63 MB/Sec for decryption. The peak speed can reach up to 7.6 MB/Sec for encryption and 6.7 MB/Sec for decryption.
11	• Key space • speed	• a key space size for initial conditions and control parameters is over than 2^{196}. • The key stream output speed is up to 571.429 Mbps, which is strongly suitable for the use of most of real-time video and audio applications.
12	• pixel correlation	• Reduction of correlation coefficients ranges from 64% to 91% with the PWLCM
13	• speed	• operating time is about 0.125s for 256x256 image and 7.5s for 1944x2596.

Table 3: Parameters for existing chaotic encryption schemes [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84].

2.10 Chaos Based Image Encryption Techniques

2.10.1 The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption, 2011

Chaotic features of trigonometric function were analyzed by Chenghang Yu, Baojun Zhang and Xiang Ruan. Based on this, they proposed another algorithm focused around the trigonometric function for quick and secure image encryption. Huge amount of analysis information and execution consideration demonstrate that the trigonometric function is of magnificent chaotic peculiarities and is exceptionally suitable for image encryption. Trigonometric function is a standout amongst the most essential and imperative function in nature. It is of numerous fascinating features in encryption field. Indeed, not the majority of the trigonometric functions can be utilized for encryption. The encryption feature of a trigonometric function is controlled by the parameters, for example, the frequency and the phase.

In future, we'll analyze the features of trigonometric function further and hope to propose more useful applications in the field of cryptography Trigonometric function is the most basic and important function in nature. Any functions can be disassembled into the sum of multi-trigonometric functions. By research, we find that the trigonometric function is of great chaos features a chaotic neural network with self-feedback of trigonometric function is presented by introducing non-linear trigonometric function as self-feedback of chaotic neural network. In this technique image encryption a complicated chaotic system using the boundary property of trigonometric function is used for image encryption [85]. 200 Nitin Kumar et al

2.10.2 Multi Chaotic Systems Based Pixel Shuffle For Image Encryption, 2009

C.K. Huang and H.H. Nien presents a new pixel shuffle technique with multi chaotic systems for the image encryption. Meanwhile the chaotic system is extremely delicate to initial values and system parameters, meanwhile, has an enormous key space, the projected method combined with

four chaotic systems and pixel shuffle can completely send away the outlines of the original image, conditions the distributive characteristics of RGB levels, and intensely declines the probability of exhaustive attacks. FIPS PUB 140-1 was conducted, correspondence coefficient, NPCR, and UACI to test on the security analysis and the circulation of eminent elements of variables for the image being encrypted. The assumed examples show the extremely confidential encrypted images and determine a good potential in the application of the image encryption with digital color [86].

2.10.3 Cryptanalysis of a Multi-Chaotic Systems Based Image Cryptosystem, 2010

Ercan Solak, Rhouma and Safya Belghith anticipated the strategy for image encryption by cryptanalysis freshly recommended image cryptosystem by two separate attacks. The shortcoming of this cryptosystem emerge from the utilization of the same rearranging methodology for each simple image. Furthermore that is an outcome of utilizing the same sequences created by the four chaotic systems. The cryptosystem suggested in mixing of plaintext image bits utilizing chaotic system. The rearranging parameters are produced by the cycles of four 3D chaotic systems. The key of the cryptosystem is the positioned of 12 starting conditions for the chaotic maps. The parameters of the chaotic systems are permanent and unrestricted.

The shuffling is performed in two stages. In the first stage, designated bits of all the pixels are shuffled. In the second stage, the bits of each pixel are shuffled among themselves. In this technique, the original plaintext is an m * n RGB image with each pixel color characterised as a byte. For the purpose of encryption, the plaintext is first vector zed using the usual row scan. The resulting vector is N * 1 vector of bytes, where N = mn. In order to manipulate the bits of pixels, the vector is further split into its bits, resulting in an N * 8 plaintext matrix, where each entry takes values 0 or 1[87].

The rearranging is achieved in dual stages. In the first stage, assigned bits of every last one of pixels are rearranged. In the second stage, the bits of every pixel are rearranged among themselves. In this method, the first plaintext is an m * n RGB image with every pixel color characterised as a byte. With the end goal of encryption, the plaintext is first vector zed utilizing the common row

scan. The ensuing vector is N * 1 vector of bytes, where N is equal to mn. So as to control the bits of pixels, the vector is additionally portioned into its bits, bringing about an N * 8 plaintext matrix, where every section takes values 0 or 1[87].

2.10.4 Image Encryption Based On Diffusion and Multiple Chaotic Maps, 2011

G. a. Sathishkumar, Dr. K. Bhoopathy bagan and Dr. N. sriraam recommended encryption algorithm fits in with the class of the grouping of value transformation and position variation. In this, two separate sorts of examining strategies are utilized and their performances are broke down. In the distinctive schematic of the projected system initially, a couple of sub keys is given by utilizing chaotic logistic maps.

On the other hand, the image is encrypted by the use of logistic map sub key and in its alteration indicates to diffusion process. From the third point of view, sub keys are created by four dissimilar chaotic maps and images are experienced as a 1D array by carrying out Raster scanning and Zigzag scanning.

The scanned arrays are isolated in different sub blocks. At that point for each one sub block, position phase and value conversion are achieved to deliver the image that has been encrypted. The sub keys are generated by applying the appropriate chaotic map banks.

Taking into account the initial conditions, the generated chaotic map banks are allowed to hop through various orbits of chaotic maps. The hopping pattern is determined from the output of the preceding map. From this time for each sub block various chaotic mapping patterns are pragmatic which additionally rises the efficiency of the key to be determined by the instinctive force attack. A sample point obtained from each orbit is utilized as key for a particular block. For that reason a specific block in a specific map has been implemented.

At that point, taking into account the chaotic system, binary sequence is created to control the bit-dissemination functions to accomplishment the progressive information change on the input information. As far as time and space is considered for a broad flat spectrum, unpredictability and extreme sensitivity to initial seeds through numerous chaotic maps and orbits hopping mechanism spread out the pseudo irregular number to it in addition to chaotic features of mixing. [88]

2.10.5 Image Encryption Based On the General Approach for Multiple Chaotic Systems, 2011

Komal D Patel, Sonal Belani (2011) suggested innovative technique for image encryption focused around a new chaotic system by accumulation of two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. After Experimental exploration they prove that the image encryption algorithm has the benefits of enormous key space and high-level security, high incomprehensible level and highly rapid [89].

2.10.6 New Image Encryption Algorithm Based On Logistic Map and Hyper-Chaos, 2013

LEI Li-hong ,BAI Feng-ming, HAN Xue-hui suggested a new image encryption algorithm focused on logistic map and hyper chaotic systems, two types of keys were formed by utilising logistic chaotic iteration and hyper chaotic systems. The two types of keys are consecutively utilized in the image encryption process, so the encryption keys have a improved arbitrary dissemination. The encryption algorithm familiarised Cipher-text cross-diffusion to intensify the cipher-text compassion .The simulation outcomes of the experiment presented the consistently spreading cipher-text pixels, the enormous key space, the minor correspondence of neighbor cipher-text pixels, extremely sensitive keys and so on. For that reason, the algorithm is more or less probable in the field of image secure storage and image secure correspondence [90].

2.10.7 Digital Image Encryption Algorithm Based On Chaos and Improved DES, 2013

Rajinder Kaur, Er.Kanwalprit Singh work was established focusing around on the chaotic encryption and enhanced and better-quality DES encryption and a arrangement of image encryption algorithm is utilized to discover the gaps. To generate pseudo random sequence on RGB image through a new encryption logistic map was discussed in this article which could create twice over times encryption with enhanced DES. Combining Chaos And enhanced DES creates the final algorithm more secure, more rapid and more appropriate for digital image encryption [91].

2.10.8 A Modified Image Encryption Scheme Based On 2D Chaotic Map, 2010

Rashidah Kadir, Rosdiana Shahril, Mohd Aizaini Maarof projected image encryption scheme as an external secret key (as used by Chen et al for image encryption and by Pareek et al for text ciphers) of 80-bit and two chaotic logistic maps are engaged together. The preliminary conditions for the both logistic maps are determined utilizing the peripheral secret key by on condition that dissimilar weight age to its bits. In the algorithm, the first logistic map is utilized to produce numbers extending from 1 to 24. These numbers might be repetitive. The preliminary condition of the second logistic map is improved from the numbers, produced by the first logistic map. By adjusting the preliminary condition of the second logistic map accordingly, its dynamics gets additionally randomized [92].

2.10.9 An Improved Image Encryption Algorithm Based On Chaotic System, 2009

Shoo Liu, Jing Sun, and Zhengquan Xu offered another new encryption algorithm by investigating the principle of the algorithm of chaos encryption focused around logistic map. Furthermore, the security and achievement of the projected algorithm is also appraised. The experimental consequences following the coupled chaotic maps support the efficiency of the offered method, and the coupled chaotic maps demonstrates benefits of enormous key space and advanced security. The system is formed in a stream-cipher structural design, where the PRKG is made by two chaotic maps, allocating the resolution of stream generation and random mixing, correspondingly. It is observed that such a design can improve the randomness, although below finite precision implementation. A comprehensive statistical analysis on the projected encryption system is specified. From the investigational consequences, it is determined that it leave behind current systems, regarding both speed and security. Consuming an extraordinary throughput, the anticipated system is all set to be in practical for fast real time encryption applications. The cipher-text produced by this technique is the similar extent as the plaintext and is appropriate for applied practise in the secure transmission of trustworthy information over the Internet [93].

2.10.10 Benchmarking AES and Chaos Based Logistic Map for Image Encryption, 2013

S.HRAOUI, F.GMIRA, A.O.JARAR, K.SATORI, LIIAN, A.SAAIDI and LIMAO prepared a relative study concerning a classical crypto-system focused around AES and additional one focused around the chaotic attractor recognised by the term the logistic map .The intention of this effort is to analyze the security eligibility of these both cryptosystems and evaluate both of their algorithms running speed. In this paper, the effectiveness of two image encryption techniques have been associated, one with the AES algorithm and the other with the chaotic attractor. The investigational consequences indicates that the AES algorithm offers improved security performance but to some extent slower regarding the encryption running speed, this permits us to suggest it for discriminating image encryption, inappropriately, it is prominent that the logistic

map displays some periodic windows that create it at risk. On the other hand, because of the computational cost, and the easiness of implementation this map is a good substitute for image encryption in real time correspondence [94].

2.10.11 A Novel Image Encryption Scheme Based On Dynamical Multiple Chaos And Baker Map, 2012

Xiao Jun Tong , Yang Liu, Miao Zhang and Zhu Wang recommended encryption algorithm consisting of two sections: primarily, the locations of the original image pixels are permuted by Baker map; secondary section includes the values of the permuted pixels which are encrypted by multiple chaotic maps. The security analysis of this anticipated image encryption was done for example, sensitivity analysis, numerical analysis, sp800-22 testing, and entropy testing and likewise to demonstrate that the suggested encryption system is secure in contradiction of the most widely recognised attacks. A fast image encryption system is anticipated which consumes dynamical multiple-chaotic map complicate the connection among the cipher image and the plain image. Baker map is utilized to permute the locations of image pixels in the spatial-domain and the combining the confusion and diffusion can generates more arbitrariness. The investigational consequences prove that image encryption technique has benefits of advanced security, for example highly strong against statistic attacks and the accuracy of cipher to be more sensitive to the secret key approach to 10-14. At similar moment, the chance of accuracy deprivation is minor than simple-chaotic map encryption system and has more elevated encryption than other prominent encryption methods [95].

2.10.12 New Image Encryption Algorithm Based On Arnold and Coupled Chaos Maps, 2010

Yun peng Zhang, Peng Sun, Jing Xie, Lifu Huang suggested another innovative algorithm focusing on multi-digital image chaotic encryption systems. The run-through demonstrates that the algorithm can rapidly encrypt and decrypt a digital image, and accomplish an improved outcome. The exploration of the algorithm's security verifies that the algorithm has a moral sensitivity of the key, an enormous sufficient key space and the encrypted pixel value is evenly disseminated, and likewise. [96].

2.11 Performance Parameters

Conferring to Suhaila O. Sharif et al suggestion, eight classifiers were utilized to recognise the cipher text, which are Support Vector Machine, Naïve Bayesian, neural network, Bagging, Instance based learning, and Decision Tree, AdaBoostM1, Rotation Forest and its precision were premeditated. The intention was to discover the finest classification algorithm established on high precision for four diverse block ciphers called DES, IDEA, AES, and RC2. Brought about, the Rotation Forest classifier has the uppermost classification precision of (53.33 %) implying that 128 out of 240 input data were classified in the approved manner. Conferring to Dr. Vikas Saxena and Jolly Shah in a review document on video encryption characterized a set of dissimilar constraints centred on which the performance can be assessed and associated with the current video encryption algorithms, these type of constraints are visual degradation, encryption ratio, speed, compression friendliness, format compliance and Cryptographic security .

By means of the quick growth of computer technology and extensive applications of internet, the security for the digital images has turn out to be extremely significant meanwhile the communication by transferring digital applications over the exposed network started to happen very often. In this paper, it has been studied that the present works on the chaos are focused on image encryption techniques. These encryption techniques are considered and analyzed properly to encourage the performance of the encryption methods additionally to guarantee the security of digital images on communicating over the networks. From the whole scenario, all the techniques are beneficial for real-time digital image encryption. Each technique is distinctive in its own

specific manner, which might get appropriate for diverse applications. In daily routine new encryption technique is developing therefore fast and secure conventional encryption techniques will permanently workout with great ratio of security.

CHAPTER 3

3 CHAOS BASED IMAGE ENCRYPTION TECHNIQUES LITERATURE SURVEY

3.1 First Paper in Consideration [97]

Two techniques for random number generation are used

3.1.1 Image Encryption Using Linear Congruential Generator

It is most commonly used method for pseudo number generation, defined by following equation:

Xn+1 = (a Xn+c) mod m..... (1)

Where a- multiplier, m- Modulus, c- Constant to be added

An arbitrary starting seed value(Xn) is needed in equation(1) with above mentioned parameters for generation of random numbers which have range up to the value of modulus (m).In this scheme, two random numbers sequences are generated based on equation(1), by choosing appropriate parameters and seed value. Then by using values of these random numbers, image permutation occurs by shuffling of rows, columns and pixels of image. One sequence is used for row shuffling and another is used for column shuffling. A masking operation [98] is used after row and column shuffling by simple XOR operations between adjacent rows and columns. By values of both sequences, pixel shuffling is done. The whole operation may be summarized by this equation:

Cimg = Epixel (Ecolumn (Erow (plainim))) ... (2)

Where Erow – Encryption by row shuffling and masking, Ecolumn – Encryption by column shuffling and masking Epixel – Encryption by pixel shuffling.

3.1.2 Image Encryption Using Chaotic Logistic Map

Logistic map is a mathematical iterative system used for generating random numbers, defined by following iterative equation:

$$Xn+1 = r*Xn*(1-Xn) \quad \text{..... (3)}$$

Where r is growth rate parameter. By choosing appropriate seed value (Xn) and growth rate (r), equation (4) can be used to generate random number sequence [98] [99] which have long period value. In this scheme, two random numbers sequences are generated based on chaotic logistic map. One sequence is used for row shuffling, another for column shuffling. Pixel shuffling is done by taking both sequences together, same as scheme (A). A masking operation is used after row and column shuffling by simple XOR operations between adjacent rows and columns. The whole operation may be summarized, same as scheme (A) by this equation:

$$Cimg = Epixel\ (Ecolumn\ (Erow\ (plainim))) \quad \text{.... (4)}$$

Where: Erow – Encryption by row shuffling and masking, Ecolumn – Encryption by column shuffling and masking, Epixel – Encryption by pixel shuffling.

3.1.3 Proposed Work

From the survey of various image compression techniques it can be concluded that chaotic image compression technique is the best and gives us good combination of speed, computation power,

and high level of security [99]. From this analysis new technique for image encryption is proposed to encrypt images by permutation and substitution operations by using chaotic map and LCG. In the proposed technique chaotic map is used twice that leads to high encryption rates and excellent security, because chaos map have pseudo-random property and non-periodicity as the chaotic signals are usually noise-like and calculate some parameters value as result.

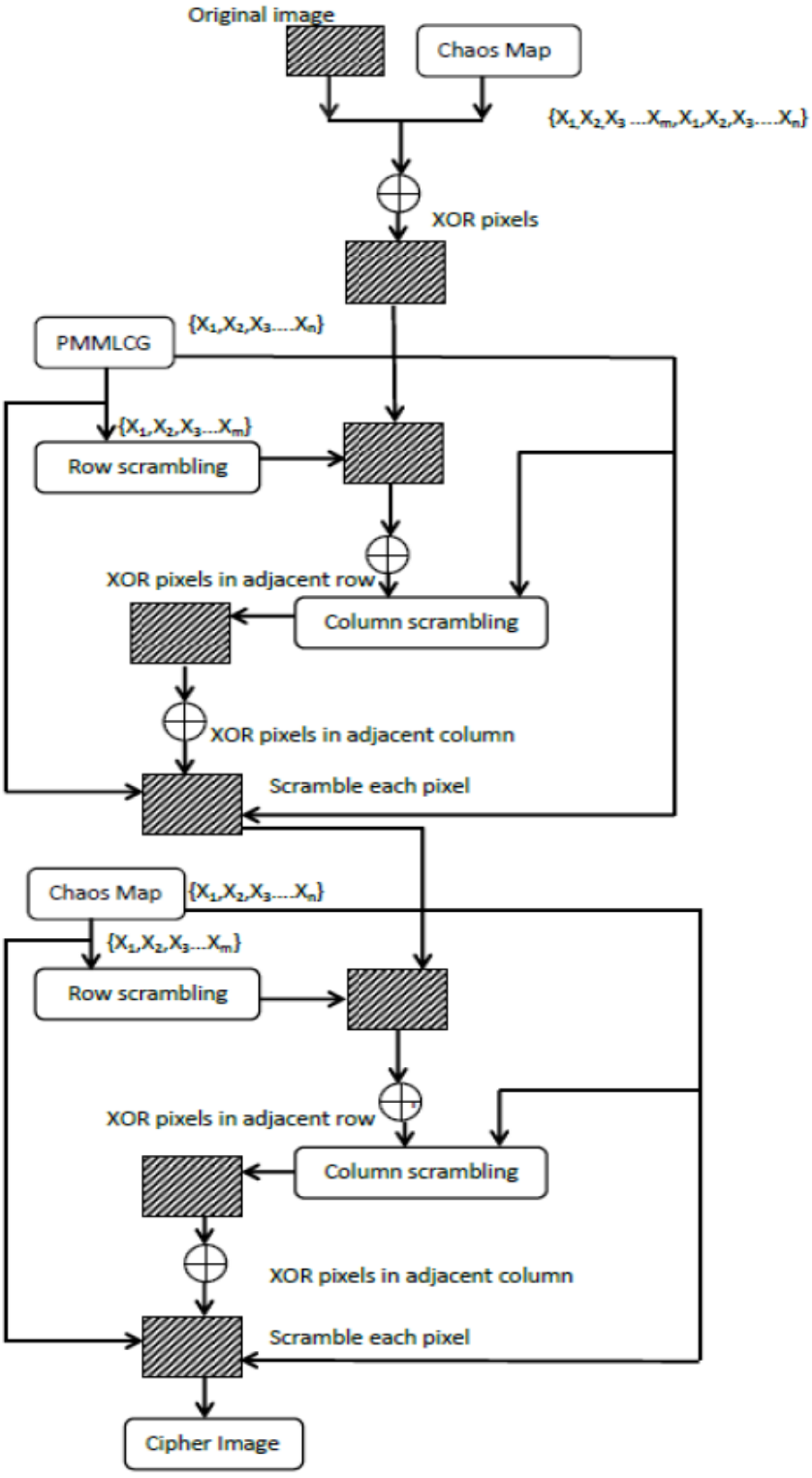


Figure 5: Proposed Chaos Map

3.2 Second Paper in Consideration (100)

Chaotic systems have various attention-grabbing characteristics such as sensitivity to initial situation and system parameter, periodicity and extending and collapsible properties, etc. These characteristics make the chaotic systems a well-intentioned selection for building and creating the cryptosystems as sensitivity to the initial situation/system parameter and extending and collapsible properties. Sandhya Rani and Sudha, the writer of this particular research have implement chaos in image encryption algorithm. Chaotic mapping techniques used are as follows:

3.2.1 Ginger Bread Man Map

The Gingerbread man system is a discrete-time dynamical system. The estimations of the map are chaotic for a definite initial situations and initial parameters. The plotted map of set of chaotic solutions of this particular kind bear a resemblance to Gingerbread.

Gingerbread man Equations:

$$x_{n+1} = 1 - y_n + |x_n|$$
$$y_{n+1} = x_n \qquad \text{..... .(5)}$$

Here x, y system parameters. For example system performances chaotic for these values x=0.5, y=3.7.

3.2.2 Cubic Map

The Cubic map is a discrete-time dynamical system. It is an illustration of a dynamical system that reveal chaotic attitude .At this point the one-dimensional map is mapped into a ternary string through symbolic dynamics for the purpose of calculating the complexity.

Cubic Equation:

$F_r(x) = rx^3 + (1 - r)\,x$ …… **(6)**

The map is governed by the value r which is known as bifurcation parameter. This will be usually 3 to produce chaotic behaviour.

3.2.3 Henon Map

The Henon map is a discrete-time dynamical system. It is the standout amongst the most intentional illustrations of dynamical systems that demonstrate the chaotic attitude. The Henon map proceeds with a point (x_n, y_n) in the plane and maps it to another point specified by the equation below.

Henon Equations:

$$x_{n+1} = 1 - ax_n^2 + y_n$$
$$y_{n+1} = bx_n \qquad \text{..... (7)}$$

The map is determined by the two constraints, a and b. The classical Henon map have values of a = 1.4 and b = 0.3. The Henon map is chaotic for classical values.

3.2.4 Logistic Map

Logistic Map is a polynomial equivalence of degree 2. Chaotic conduct can stand out from very modest non-linear dynamical equations.

Logistic Equation:

$$x_{n+1} = r x_n (1 - x_n) \quad \text{..... (8)}$$

Where x_n is a value between 0 and 1and it will be usually 0.1 and r is a positive value. Typically the system behave chaotically at r=4.

3.2.5 Proposed Work

The proposed image encryption algorithm has two most important steps. Primarily, the correspondence between the neighbouring pixels is distressed absolutely as the image data have robust correlations between adjacent pixels. For image security and privacy, one needs to interrupt this correlation. To accomplish this, a block and stream centred image shuffling system is projected by the use of three chaotic maps stated above. At that time the pixel estimations of the shuffled image are improved by utilizing Henon map. Encryption is carried out in two stages confusion and diffusion.

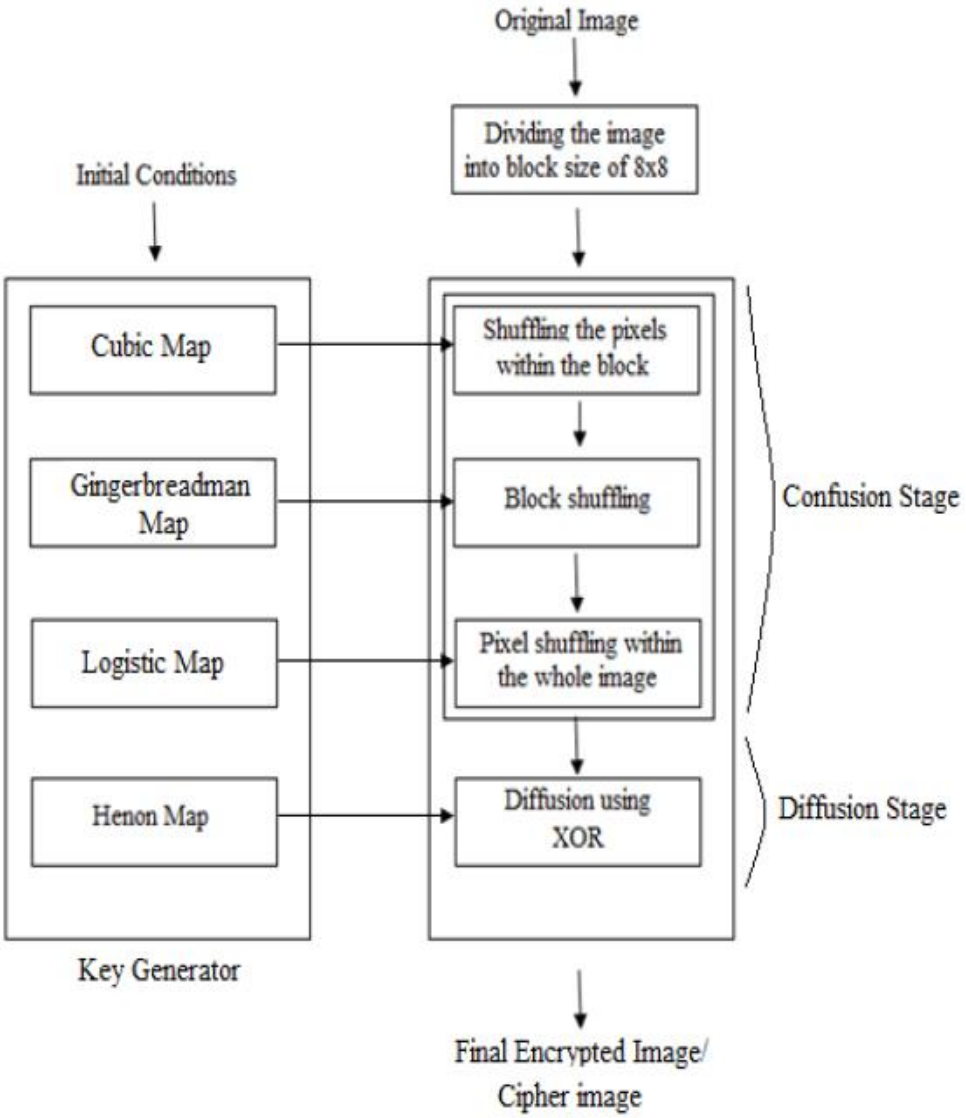


Figure 6: Block Diagram of Encryption System

3.2.6 Confusion Stage

The confusion stage is the pixel permutation wherever the position of the pixels is mixed over the complete image without distressing the estimation of the pixels and the image becomes distorted. Three levels of shuffling are active in this stage.

The trailed steps are:

Step1: An image of size NxN is distributed into 8x8 sized blocks.

Step2: The pixels contained by the block are shuffled by the use of Cubic Map.

Step3: All the 8x8 blocks inside an image are shuffled by the use of Ginger bread man map.

Step4: The pixels in the entire image are shuffled utilizing Logistic Map.

3.2.7 Diffusion Stage

In the diffusion stage, the pixel estimations are improved in sequence by the arrangement caused by the chaotic systems. Subsequently confusion stage, the histogram does not change even however the pixels are shuffled. At this time pixel estimations are improved to obtain a standardized histogram. Diffusion is accomplished using XOR operation.

Decryption

Here reverse algorithm of encryption is utilized to obtain again the original image by the use of the similar chaotic maps with similar initial situations.

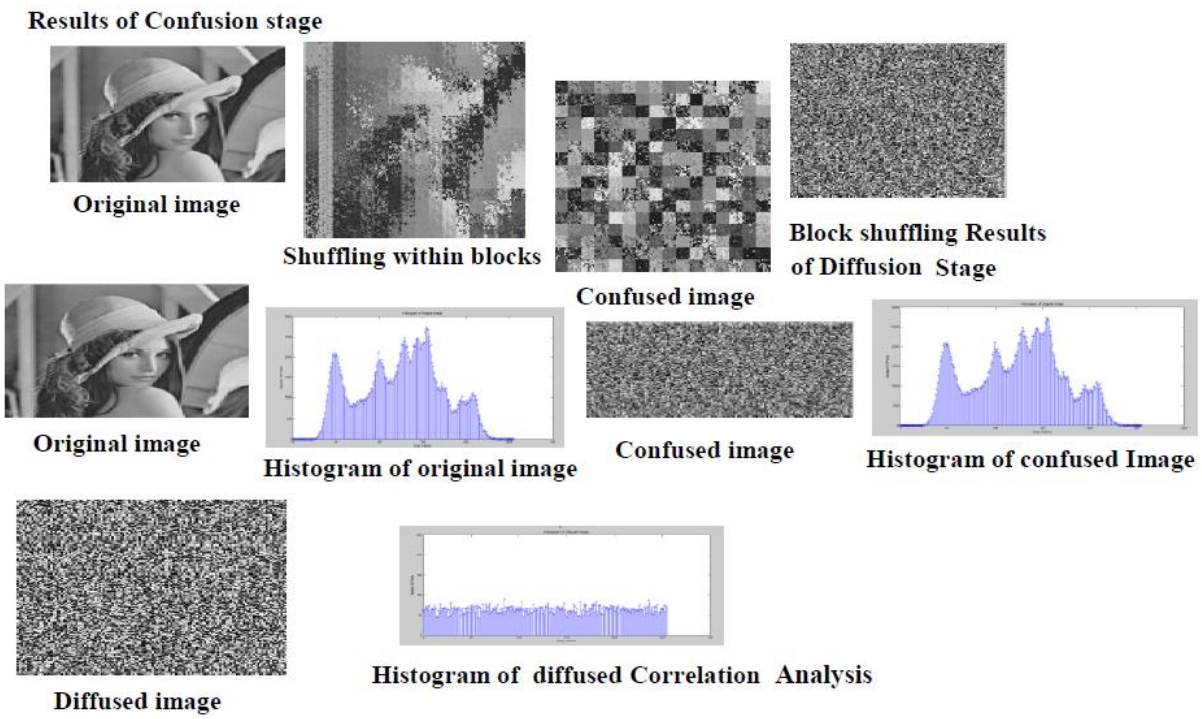


Figure 7: Results of Decrypted images

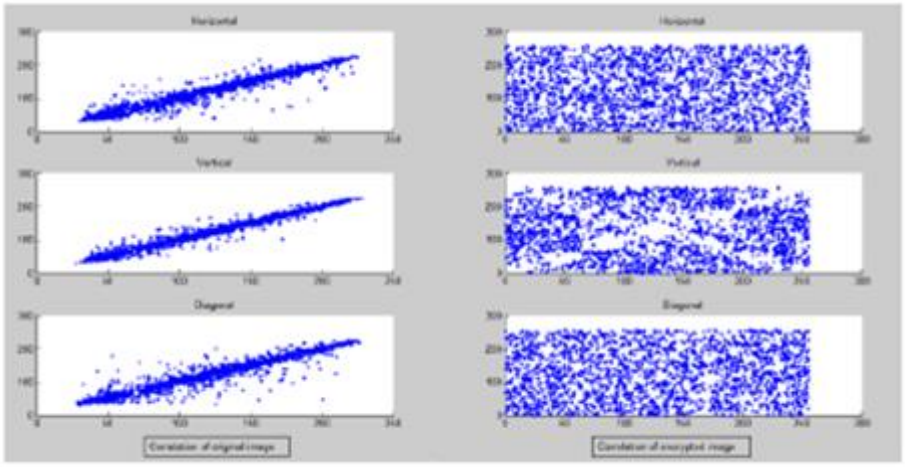


Figure 8: Correlation between two adjacent pixels horizontally, vertically and diagonally.

In this segment, the correlation amongst two vertical, two horizontal and two diagonal adjacent pixels is investigated. In the original image, every pixel is profoundly related through its adjacent pixels either in horizontal or vertical direction and there should be no connection of cipher images in the adjacent pixels. Figure shows the distribution of two horizontally, vertically and diagonally adjacent pixels in the plain image and cipher image. To make a comparison of the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, the subsequent formulae are utilized to acquire the correlation co-efficient [101]. The ideal coefficient value of original image will be 1 and for cipher image it will be 0.

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i,$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N} (X_i - E(X_i))^2,$$

$$cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N} (X_i - E(X_i))(Y_i - E(Y_i)),$$

$$r_{XY} = \frac{cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \quad \text{..... (9)}$$

In equation (5) x_i and y_i are the values of two adjacent position of pixels in the image and N is the total number of pixels existing in the image.

Correlation coefficients considered for the original and encrypted images are specified in Table. It is clear from the table that the two adjacent pixels are extremely uncorrelated.

Direction of adjacent pixel	Plain image	Ciphered image
Horizontal	0.9719	-0.0040
Vertical	0.9850	-0.0333
Diagonal	0.9593	0.0047

Table 4: Correlation Coefficient of Two Adjacent Pixels in Two Images.

3.2.8 Key Space Analysis

Key space gives the complete number of dissimilar keys that are utilized in the cryptographic system. There are overall eight initial situations of chaotic maps that are of use in the algorithm and the initial situations are x0, y0, r (for Logistic), a, b (for Henon), r (for Cubic), which can be utilized to create the secret keys of encryption and decryption. In this type of situation, the precision is 10-17, the key space size is (1017)10 i.e. **10170**, which is comprehensively big at an adequate amount to create the brute force attack and other associated attacks infeasible.

3.2.9 Key Sensitivity

A cryptosystem ought to be sensitive to a minor change in secret keys i.e. small change in secret key estimation in decryption process consequences into a entirely diverse decoded image which will be comparable to cipher image [3]. Encryption algorithm anticipated in this study is sensitive to a slight change in the secret keys. If a single bit is changed in in the least of the initial conditions then the decrypted image is completely dissimilar from the plain-image. For instance if one of the initial condition is 1.4 and substitute it by 1.41, then a complete random image is obtained. To acquire back the appropriate decrypted image the initial condition have to be **1.40000000000000001**.

3.2.10 Information Entropy Analysis

The entropy H (m) of a source m is deliberated by the following equation [10]

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} \quad bits \qquad \text{......} (10)$$

Where p (mi) signifies the probability of existence of symbol mi. Entropy is stated in expressions of bits. At this point every pixel in the image is characterised by 8 bits so number of dissimilar values that it can consume is 28. It is correspondent to a source emitting 28 symbols with equal probability. Once this is practical to eq. 5 h (m) =8 is obtained which relates to an entirely arbitrary source. Entropy is not as much of 8 for plain images however when images are encrypted, their entropy has to perfectly be 8. If it is not 8 then degree of liability is in elevation.

It is perceived that for Lena image statistics, entropy of encrypted image utilizing the anticipated algorithm is **7.9890** which are very adjacent to the theoretical value of 8. This point towards that the algorithm is secure contrary to entropy attack.

3.2.11 Peak Signal To Noise Ratio (PSNR)

The term **peak signal-to-noise ratio (PSNR)** is an expression for the ratio among the maximum possible value (power) of a signal and the power of distorting noise that distresses the eminence of its demonstration. It benefits to associate diverse image enhancement algorithms and classify the best between them. The mathematical representation of the **PSNR** is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad \text{………………………………………………… (11)}$$

Where the **MSE** is the Mean Squared Error. The PSNR value acquired for the suggested algorithm is **77. 3503.**

3.3 Third Paper in Consideration [102]

This work proposes a chaos-based symmetric image cipher with a plaintext-related key stream generation mechanism. In the diffusion stage, the state variables of Lorenz system are selected according to the plain pixel.

3.3.1 Image Permutation Using Discretized Baker Map

In the transformation stage, three zone-preserving invertible chaotic maps; Arnold cat map, baker map and standard map, are frequently working to rearrange the pixel positions of the plain image, in order to remove the tough connections between adjacent pixels. Discretized baker map is active because of its best adjustment between key space and performance. The supposed generalized baker map is a chaotic bisection of the unit square I×I onto the situation. As demonstrated by Fig. 1, a N×N image is initially divided into k vertical rectangles of height N and width n_i (i=0, 1, …, k-1), such that all n_i divide the side length N and

$n_0+n_1+ \dots +n_{k-1}= N$.

At that time, these vertical rectangles are overextended in the horizontal direction and constricted in the vertical direction to acquire a horizontal rectangle. As a final point, all these horizontal rectangles are loaded on top of each other.

Let N_i (i=1, 2, …, k) represent the inferior right corner of the vertical rectangle which comprehends the point (x, y) which have to be converted. Apparently the subsequent relation holds for N_i:

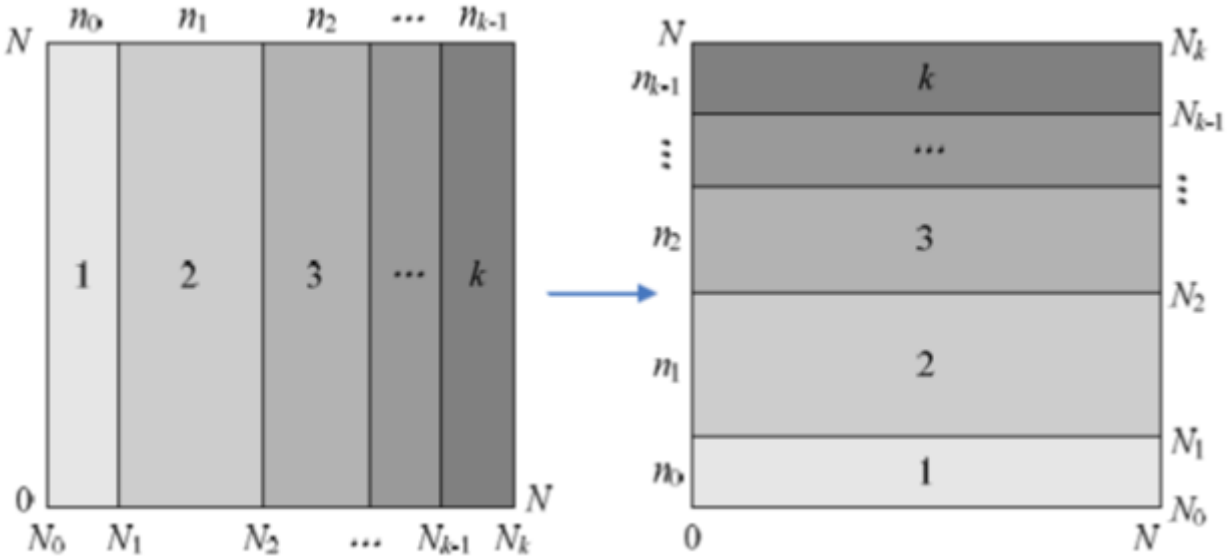


Figure 9: The discretized baker's map

$$N_i = \begin{cases} 0 & i = 0, \\ n_0 + \ldots + n_{i-1} & i = 1,2,\ldots,k. \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (12)$$

Then the discretized baker map is defined by

$$B_d(x,y) = \begin{pmatrix} \frac{N}{n_i}(x - N_i) + y \mod \frac{N}{n_i}, \\ \frac{n_i}{N}\left(y - y \mod \frac{N}{n_i} \right) + N_i \end{pmatrix}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (13)$$

where $N_i \le x < N_i + n_i$ and $0 \le y \le N$.

The inverse transform $B_d^{-1}(x,y)$ for de-shuffling is easily found to be given by

$$B_d^{-1}(x,y)=\begin{pmatrix} \frac{n_i}{N}\left(x-x \mod \frac{N}{n_i}\right)+N_i, \\ \frac{N}{n_i}(y-N_i)+x \mod \frac{N}{n_i} \end{pmatrix}. \quad \text{…….. (14)}$$

The submission of the discretized baker map to a grayscale test image with 256×256 size is established in Fig. 10. Fig. 10(a) displays the plain image, and Figs. 10(b)-(d) expresses the outcomes of spread over the map one time, two and three times, correspondingly. The ciphering keys are {32, 8, 64, 16, 8, 32, 64, 32}, which comprises of 8 divisors of 256. As Fig. 10 shows that after three rounds iterations, the correspondence among the adjacent pixels is efficiently removed and the image is absolutely incomprehensible. On the other hand, the shuffled image is weak in contrast to statistical attack and recognised or preferred plaintext attack as the permutation operation only modifies the pixels positions without transforming their values. As an issue, we utilize a diffusion procedure afterwards to progress the security.

3.3.2 Image Diffusion Using Lorenz System

In 1963, Edward Lorenz, an early pioneer of chaos theory, established a abridged mathematical model for atmospheric convection. The model is a system of three ordinary differential equations now recognised as the Lorenz equations, as pronounced by

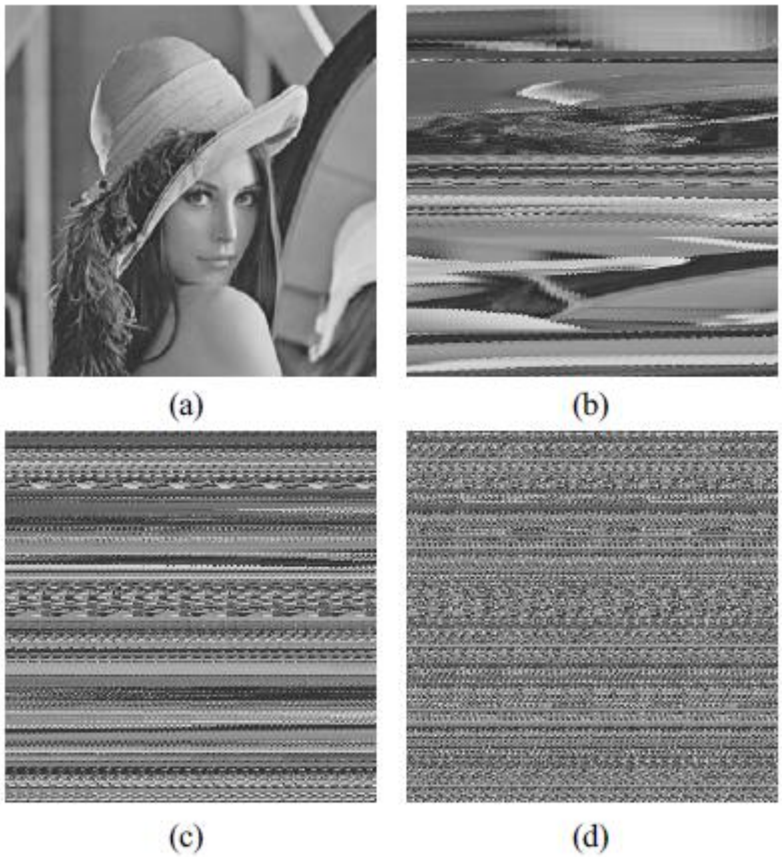


Figure 10: The application of the discretized baker map. (a) The test image 256×256 pixels with 256 gray levels. (b) The test image after applying the discretized baker map once. (c) The test image after applying the discretized baker map two times. (d) The test image after applying the discretized baker map three times.

$$\begin{cases} \dot{x} = \sigma(y-x), \\ \dot{y} = x(\rho - z) - y, \\ \dot{z} = xy - \beta z, \end{cases} \qquad \text{………………………………………. (15)}$$

Where σ, ρ, β, are the system parameters. When σ =10, ρ =8/3, β =28, the system displays chaotic behavior. The preliminary state values x_0, y_0 and z_0 assist as the diffusion keys. Associated with 1D chaotic maps such as logistic map, tent map, and Chebyshev map, the Lorenz system has further complex dynamical property and number of state variables. As a consequence, the

cryptosystem based on Lorenz system has robust changeability and bigger key space, which are important for secure ciphers.

The comprehensive diffusion process is defined as follows:

Step 1: To avoid the destructive consequence of transitional technique, the Lorenz system is N_0 times pre-iterated by means of fourth-order Runge-Kutta method, where N_0 is a constant.

Step 2: The Lorenz system is iterated uninterruptedly. For each iteration, we can acquire three state values and one is designated as quantification of key stream element conferring to

$$s_n = \begin{cases} x_n & if \ \ p_{n-1} \ \% \ 3 = 0, \\ y_n & if \ \ p_{n-1} \ \% \ 3 = 1, \\ z_n & if \ \ p_{n-1} \ \% \ 3 = 2. \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (16)$$

Where p_{n-1} is the formerly operated plain pixel. One possibly will set initial value p_0 as a constant.

Step 3: The key stream is quantified by utilizing the following formula

$$K_n = mod\ [round\ ((abs\ (s_n) - floor(abs(s_n)))*10^{14}),2^L] \ldots\ldots\ldots\ldots\ldots\ldots\ldots. (17)$$

where mod(x, y) proceeds with the remainder after division round(x) rounds x to the nearest integers, abs(x) yields the absolute value of x, floor(x) yields the value of x to the nearest integers less than or equal to x, and L is the color depth (for a 256 grayscale image, L=8).

Step 4: Calculating the cipher pixel value according to Eq. (18).

$$C_n = K_n \oplus \{[p_n + k_n]\ mod\ 2^L\} \oplus c_{n-1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (18)$$

Where c_n, k_n, p_n, c_{n-1} are the output cipher pixel, key stream element, presently operated plain pixel, and earlier cipher pixel, correspondingly, and $\oplus$ performs bit-wise exclusive OR operation. Also, the initial value c0 can be set as a constant.

Step 5: Coming back to **Step 2** until all the pixels of the shuffled image are encrypted in direction from left to right and top to bottom.

As can be realised from Eq. (18), the adjustment made to a specific pixel not only be determined by the consistent key stream element, but also the collected effect of all the preceding pixel values. As an outcome, the inspiration of a single plain pixel can be spread out over many cipher pixels, creating the cryptosystem strong in contradiction of differential attack.

The decryption technique is comparable to that of the encryption process pronounced above, and the inverse of Eq. (18) is given by

$$P_n = [k_n \oplus c_n \oplus c_{n-1} + 2^L - k_n] \bmod 2^L \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (19)$$

The above permutation-diffusion processes are generally achieved for several rounds conferring to the security obligation.

3.3.3 Security Analysis

In this segment, comprehensive security tests are supported with thorough investigation to determine the high security of the recommended scheme.

3.3.4 Key Space Analysis

The key space is the aggregate number of dissimilar keys that can be utilized in the encryption/decryption technique. For an operational cryptosystem, the key space ought to be huge sufficiently to make exhaustion attack infeasible. As specified above, the key of the projected cryptosystem is comprised of two parts: permutation key Key-P and diffusion key Key-D. For an image with N×N size, the task of approximating the total number of Key-P can be condensed to the inquiry: How many combinations of positive integers (n_0, $n_1 \ldots n_{k-1}$) summing up to N can be initiate under the constraint that every n_i (i=0, 1… k-1) has to divide N? A list of particular outcomes is given in Table 1, from which we can understand that the number of potential keys grows very promptly with the size of the image.

Key-D is made of three floating point numbers (x_0, y_0, z_0). Conferring to the IEEE floating-point standard, the computational precision of the 64-bit double-precision number is approximately 10^{-15}, so the overall number of potential values of Key-D is just about 10^{45}. The two parts key-P and key-D are independent of each other. For that reason, the total key space Key-S is

$$\text{Key-S} = \text{key-P}(N) \times \text{key- D} \approx \text{key} - P(N) \times 2^{149} \quad (20)$$

If $N \geq 256$, the total size satisfies,

$$\text{Key} - S \geq 2^{358} \quad (21)$$

Which is large enough to resist brute-force attack.

N	No. Keys	N	No. Keys	N	No. Keys
1	0	16	5271	256	$\approx 2^{209}$
2	1	32	$\approx 2^{25}$	512	$\approx 2^{418}$
4	5	64	$\approx 2^{50}$	1024	$\approx 2^{837}$
8	55	128	$\approx 2^{103}$	2048	$\approx 2^{1678}$

Table 5. Number of possible keys for some selected values of n

3.3.5 Statistical Analysis

3.3.5.1 Histogram analysis

An image histogram is a graphical demonstration which shows a visual impression of the circulation of pixels through scheming the number of pixels at each grayscale level. The histograms of the test image (Fig. 11(a)) and its ciphered image (Fig. 11(c)) formed by the proposed scheme are shown in Figs. 11(b) and (d), correspondingly. It's vibrant from Fig. 11 that the pixels in cipher image are impeccably uniformly circulated, and therefore does not be responsible for any clue to work for statistical analysis.

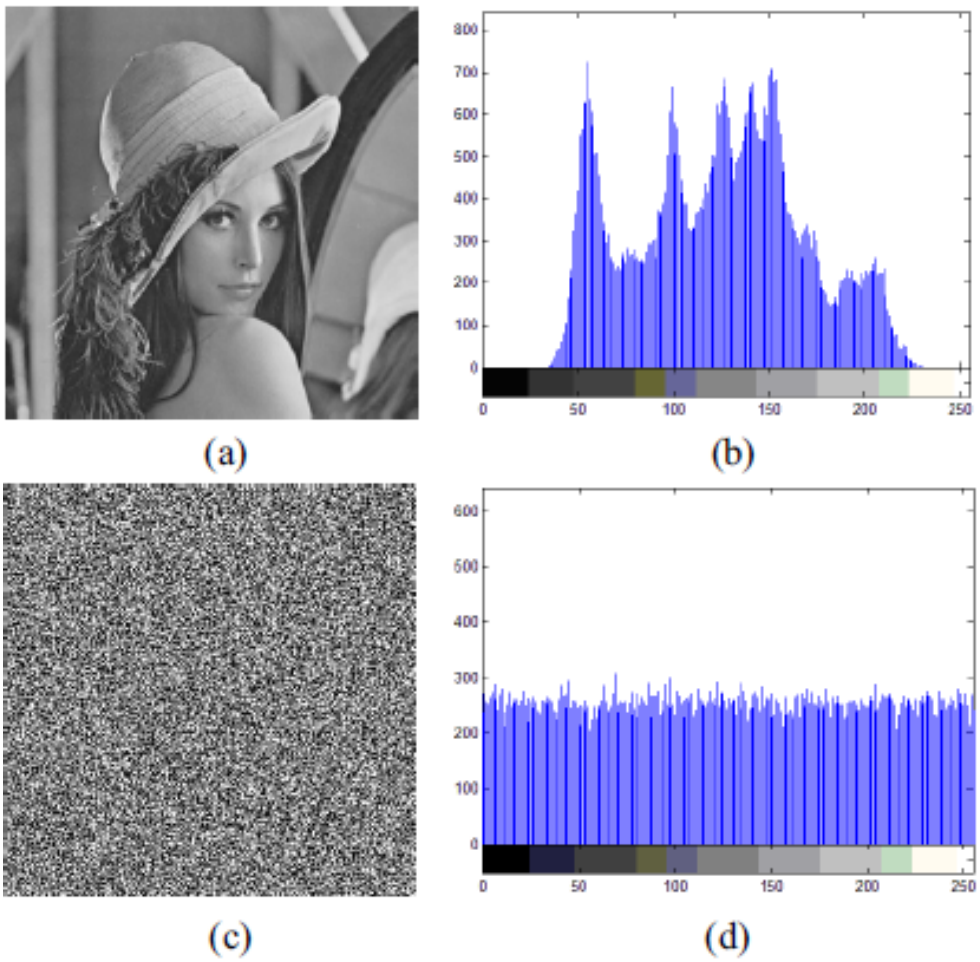


Figure 11: Histograms of plain image and cipher image. (a) Plain image. (b) Histogram of plain image. (c) Cipher image. (d) Histogram of cipher image.

3.3.5.2 Correlation of adjacent pixels

The visual analysis of the association of adjacent pixels can be prepared by the subsequent process. Primarily, random selection of N (N > 2000) pairs of adjacent pixels in horizontal, vertical and diagonal directions from the image. At that time, by utilizing each pair as the values of the x-coordinate and y-coordinate, plot the distribution of the adjacent pixels. The correspondence

circulation of two horizontally adjacent pixels of the plain image and its consistent cipher image are shown in Figs. 12(a) and (b), separately. As can be seen from Fig. 12, most points in Fig. 12(a) are situated around the diagonal, however those in Fig. 12(b) allocate consistently, which specifies that the strong correlation between adjacent pixels in plain image are efficiently excluded by utilizing the recommended cryptosystem. Comparable outcomes can be achieved for vertical and diagonal directions.

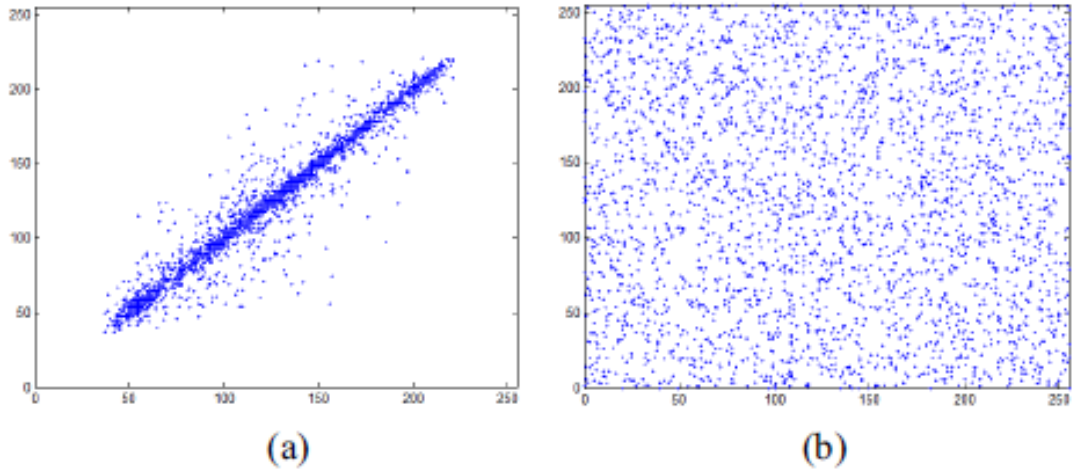


Figure 12: Correlation of horizontal adjacent two pixels in plain image. (b) Cipher image.

To promote quantification and associate the correlations of adjacent pixels in the plain and cipher image, the correlation coefficient r_{xy} is determine by means of the subsequent three formulas:

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}}, \quad \text{..... (22)}$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \text{..... (23)}$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i, \quad \text{..... (24)}$$

Where xi and yi are grayscale values of ith pair of adjacent pixels, and N signifies the total number of samples.

Table 2 lists the consequences of the correlation coefficients for the plain image and its ciphered image with N = 3000, which additionally verifies the strength of the proposed cryptosystem in the aspect of statistical analysis.

3.3.5.3 Key sensitivity analysis

Key sensitivity make certain that no data can be improved from cipher-text no matter how adjacent the encryption and decryption keys are. To estimate the key sensitivity property of the anticipated cryptosystem, the test image (Fig. 2(a)) is primarily encrypted by means of a random selection of diffusion key (x_0=5.34664387425724, y_0=6.09824818670074, z_0=3.69389916505723).

Next the ciphered image is strained to be decrypted utilizing three slightly dissimilar keys, as listed in Table. The resultant deciphered images are shown in Figs. 11(a)-(c), respectively. Similar results

are obtained with a slight change in the permutation key. Therefore it can be concluded that the proposed cryptosystem completely satisfies the key sensitivity requirement.

CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN TWO IMAGES

Direction	**Plain image**	**Cipher image**
Horizontal	0.9703	-0.0013
Vertical	0.9425	-0.0274
Diagonal	0.9188	-0.0199

DECRYPTION KEYS USED FOR KEY SENSITIVITY TEST

Figure	**Decryption key**
13(a)	x0=5.34664387425725, y0=6.09824818670074, z0=3.69389916505723
13(b)	x0=5.34664387425724, y0=6.09824818670075, z0=3.69389916505723
13(c)	x0=5.34664387425724, y0=6.09824818670074, z0=3.69389916505724

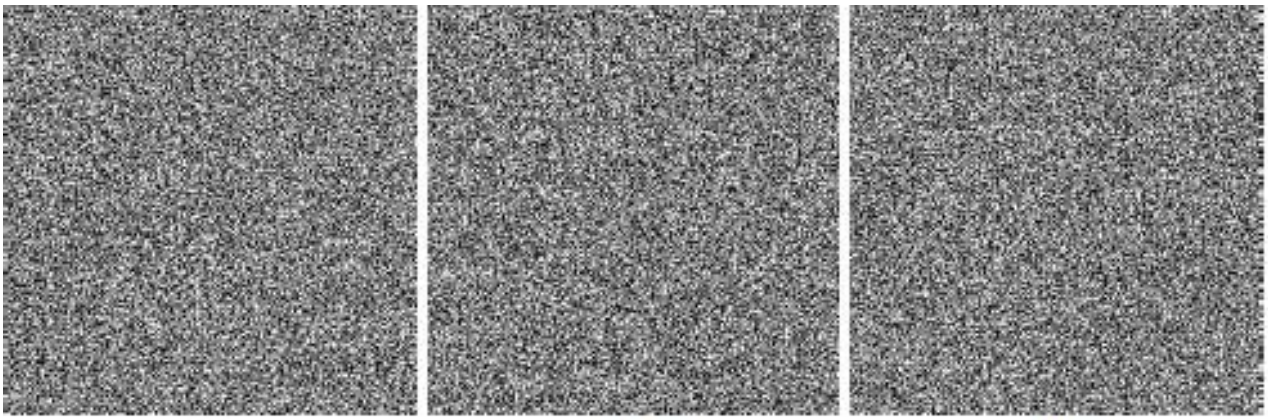


Figure 13: Deciphered images using three slightly different keys.

3.3.5.4 Differential Analysis

For the implementation of the differential attack, an opponent generally creates a slight variation in the plain image and perceives the variations of consistent cipher image to discover out some expressive association among plain image and cipher image, which supplementary simplifies in defining the secret key. If a slight variation in the plain image can be efficiently diffused to the entire cipher image, then such differential analysis may turn out to be practically inadequate. Two criteria, NPCR (number of pixel change rate) and UACI (unified average changing intensity), are usually active to measure the diffusion capacity of an image cryptosystem.

The NPCR is utilized to measure the percentage of different pixel numbers among two images. Let P1 (i, j) and P2(i, j) be the (i, j)th pixel of two images P1 and P2, correspondingly, the

NPCR is well-defined as:

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\%,$$ ..... (25)

Where W and H are the width and height of P1 or P2 and D (i,j) is defined as

The second criterion, UACI is utilized to measure the regular intensity of dissimilarities among the two images. It is defined as

$$D(i,j) = \begin{cases} 0 & \text{if } P_1(i,j) = P_2(i,j), \\ 1 & \text{if } P_1(i,j) \neq P_2(i,j). \end{cases}$$ ..... (26)

$$UACI = \frac{1}{W * H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\left[\frac{|P1(i,j) - P2(i,j)|}{L-1}\right]\right] * 100 \ldots\ldots (27)$$

The NPCR and UACI values for two correctly arbitrary images with 256 grey-levels, specifically the estimated values for a worthy cryptosystem, are 99.609% and 33.464%, correspondingly.

To evaluate the NPCR and UACI of the proposed cryptosystem, we assume a worst case that two plain images have only one pixel difference at the lower right corner, as shown in Figs. 14(a) and (b). Their corresponding cipher images are shown in Figs. 14(c) and (d), respectively.

The differential image among the two cipher images can be establish in Fig. 14(e). We achieve NPCR=99.583% and UACI=33.461%. The results indicates that a minor alteration in the original image will effect in a substantial alteration in the ciphered image, and as a result the suggested scheme is secure against differential attack.

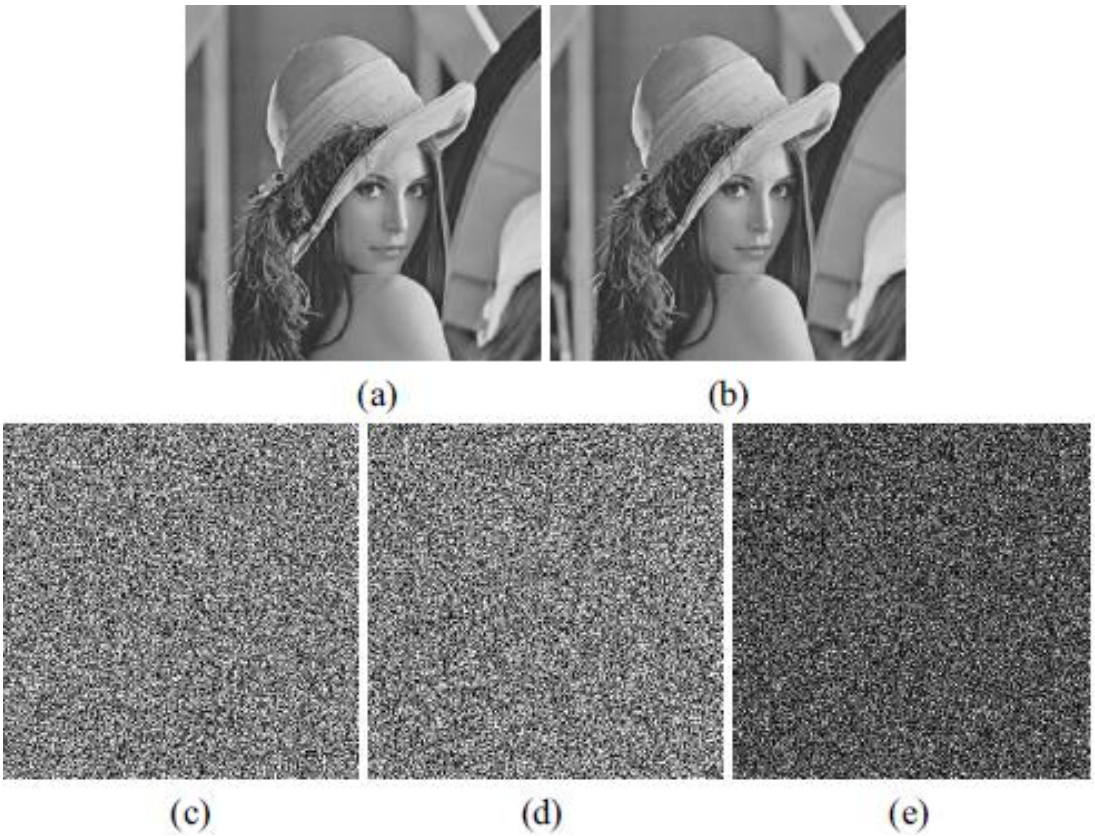


Figure 14: Diffusion capacity test. (a) and (b) are two plain images with only one pixel difference at the lower right corner, (c) cipher image of (a), (d) cipher image of (b), (e) differential image between (c) and (d).

3.3.6 Comparison Criteria for Image Encryption Algorithm

1. Number of pixel change rate (NPCR).
2. Unified average changing intensity (UACI).
3. Entropy.
4. Correlation coefficient.

3.3.7 Number of Pixel Change Rate (NPCR)

It is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images. Let Io (i, j) and IENC (i, j) be the pixels values of original and encrypted images, Io and IENC, at the ith pixel row and jth pixel column, respectively. Equation (28) gives the mathematical expression:

$$NPCR = \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \; x \; \frac{100\%}{M \; x \; N}$$

Where D(i, j) = 0 if $I_o(i, j) = I_{ENC}(i, j)$ if not then D(i, j) = 1. …… (28)

3.3.8 Unified Average Changing Intensity (UACI)

A small change in plaintext image must cause some significant change in cipher-text image. UACI is helpful to identify the average intensity of difference in pixels between the two images. For the plaintext image Io (i, j) and encrypted image IENC (i, j) the equation (29) gives the mathematical expression for UACI.

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|Io(i,j) - I_{ENC}\ (i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

…… (29)

3.3.9 Entropy

It is an important concept for analyzing an encryption scheme. Entropy gives an idea about self-information. The entropy of a message m can be indicated as H (m). If there are M symbols and p(mi) as the probability of occurrence of symbol mi , then the equation (30) for entropy is given as:

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (30)$$

3.3.10 Correlation Coefficient

Correlation computes the degree of similarity between two variables. This parameter is useful for calculating the quality of the cryptosystem. Let x and y be the gray-scale values of two pixels at the same place in the plaintext and cipher-text images respectively and C.C be the correlation coefficient and Cov be the covariance at pixels x and y. VAR(x) denotes the variance at pixel value x in the plaintext image, σx the standard deviation, E the expected value operator and N the total number of pixels for N x N matrix. Then the correlation can be calculated by the equations (31), (32), (33), (34) and (35) as below:

$$C.C = \frac{Cov(x,y)}{\sigma_x \times \sigma_y} \quad \ldots\ldots\ldots\ldots\ldots\ldots (31)$$

$$\sigma_x = \sqrt{VAR(x)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (32)$$

$$\sigma_y = \sqrt{VAR(y)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (33)$$

$$VAR(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (34)$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \quad \text{..... (35)}$$

4 IMPLEMENTATION

4.1 Time Samples Pattern **(A Secured Approach to Code Input Signals)**

4.1.1 Transmitter and Receiver

In the transmitter, an input signal, $In(n)$, is received and coded into a longer string of numbers. At the receiver, the coded signal by the transmitter is received and turned back into its original values.

4.1.2 Time Samples Pattern

The idea is to hide input signal samples within samples of a longer random signal using a specific pattern, S_n, which is only recoverable by a trusted receiver.

The pattern is generated as a combination of deterministic and random functions. The pattern is a monotonically increasing function, $S_n > S_{n-1}$.

The pattern is created by an incremental factor, f_n, which is generated as a distance between two moving points on two circles,

$$S_n = S_{n-1} + f_n$$

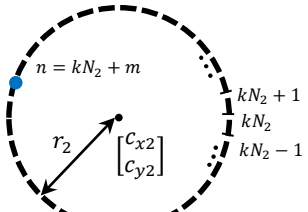
4.1.3 Coding Circles, and the Distance Function, f_n

$$X_1(n) = \begin{bmatrix} C_{x1} \\ C_{y1} \end{bmatrix} + r_1 \begin{bmatrix} \cos(\frac{2\pi}{N_1} n) \\ \sin(\frac{2\pi}{N_1} n) \end{bmatrix}$$

$$X_2(n) = \begin{bmatrix} C_{x2} \\ C_{y2} \end{bmatrix} + r_2 \begin{bmatrix} \cos\left(\left(\frac{2\pi}{N_2} + \frac{\pi}{6}\right) n\right) \\ \sin\left(\left(\frac{2\pi}{N_2} + \frac{\pi}{6}\right) n\right) \end{bmatrix}$$

$$dist(n) = f_n = \|X_1(n) - X_2(n)\|_2 + R_n$$

Where R_n is randomly selected between$\{-1,0,1\}$.



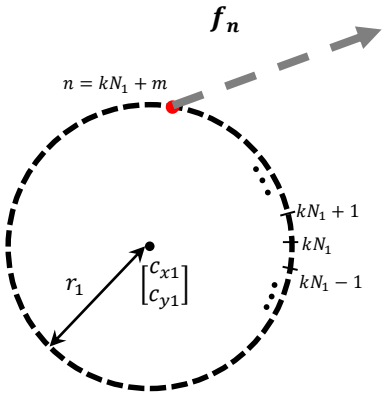


Figure 15: Coding Circles and Distance Function Diagram

4.1.4 Hiding Samples in a random Signal

We first generate a random signal as

$\{Out(k)|k \in [1, \dots, L], P_{out}: uniform\ distribution\}$.

Then the input signal is placed in the time sample pattern as follows,

$Out(f_n) = In(n)$,

To make it detectable, we repeat it 3 times as,

$$Out(f_n - 1) = Out(f_n + 1) = Out(f_n)$$

4.1.5 Coding Parameters

The coding parameters include: N_1, N_2, r_1, and r_2 of the coding circles.

Without knowing the coding parameters, the coded signal is not recoverable.

Both transmitter and receiver should have the same parameters to correctly code and decode the input signal.

4.2 Test Bench

A test bench file is written to allow users running and evaluating the operation of the transmitter-receiver system.

A sample sinusoidal signal is provided which can be replaced with any arbitrary signal (such as a speech signal).

The reconstruction error is provided in terms of room-mean-square-error.

MATLAB code (testBench.m)

```
% ================================================================

% This code is written to develop a time based coding algorithm.

%This program is a test bench.

% ================================================================

clc

close all

clear all

% Place to add your desired Input Signal

% Generating a sinosuidal input function

n=1:1000;

Input_Signal=sin(2*pi*n/10);

% Adjusting coder parameters

R1=20;
```

```
R2=30;

N1=20;

N2=10;

% Coding the input signal

Coded_Signal=Transmitter_EncodingSystem(Input_Signal,R1,R2,N1,N2);

% Decoding the coded signal to reconstruct the input signal

Output_Signal=Receiver_DecodingSystem (Coded_Signal,R1,R2,N1,N2);

% Plotting Input, coded and output signals

figure;

subplot(3,1,1);plot(Input_Signal);title('Input Signal');xlim([1 length(Input_Signal)])

subplot(3,1,2);plot(Coded_Signal);title('Coded Signal');xlim([1 length(Coded_Signal)])

subplot(3,1,3);plot(Output_Signal);title('Output Signal');xlim([1 length(Input_Signal)])

% Calculating Coding and Decoding error based on Root-mean-square-error

RMSE=sum((Input_Signal(1:length(Output_Signal))-Output_Signal).^2).^0.5

Length_Ratio=length(Coded_Signal)/length(Input_Signal)
```

4.3 Test Bench Result

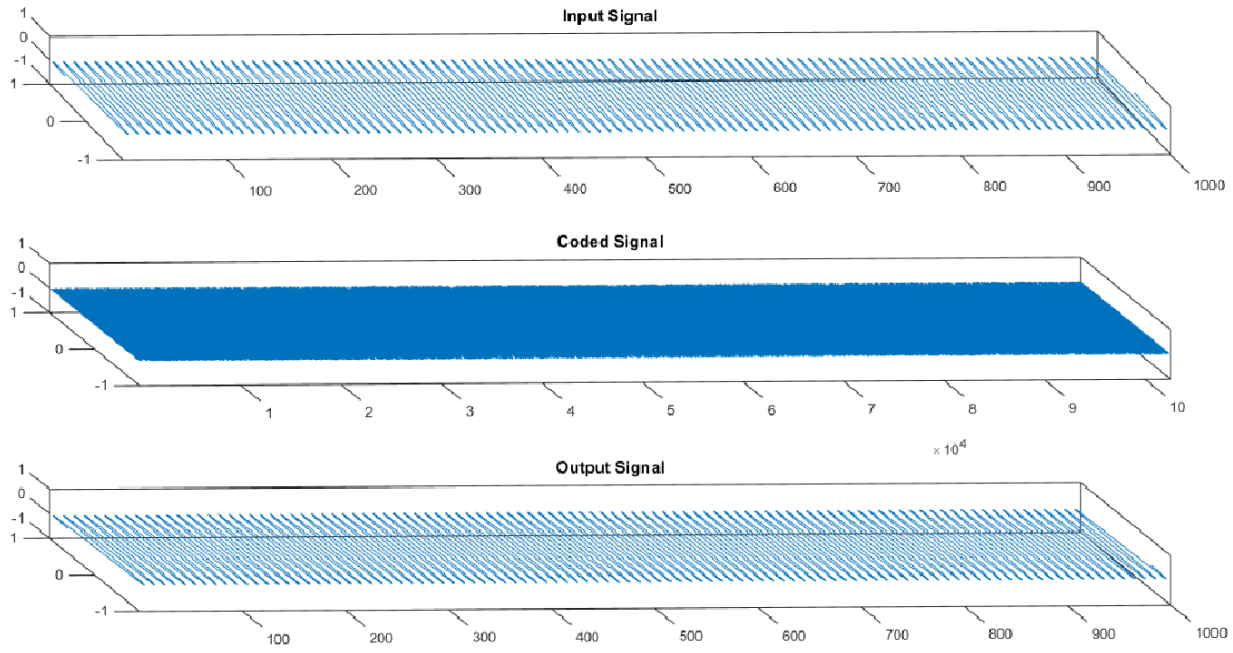


Figure 16: 3D view of input/output and coded signal

5 CONCLUSION

At existing eras where the most important communication is through wireless techniques using internet network to transfer data, so main concerns are on the subject of the security of such personal or countries defence data. Encryption is unique way to guarantee worthy security from unofficial access at many grounds. Image encryption is striking extent for research in this case because communication with the support of multimedia objects is growing promptly. Various important encryption techniques have been presented in demand to make it acquainted with a number of encryption algorithms used in encrypting the image which has been transmitted over network. The outcomes of every algorithm has advantages and disadvantages based on their techniques which are being practised on images.

Further chaos based image encryption has been reviewed in detailed. Relating current chaotic maps, the chaotic systems are capable to produce a huge number of new chaotic maps. They all have comparable properties together with exceptional chaotic behaviors, big chaotic range and uniform distributed density function.

To investigate application encryption in time samples pattern, we have proposed a secured approach to code input signals by introducing a new encryption algorithm. The algorithm works as follows; in the transmitter, an input signal was received and coded into a lengthier series of numbers. At the receiver, the coded signal by the transmitter was received and changed back into its original values. This was done based on the idea that the hidden input signal samples (within samples of a longer random signal) using a specific pattern, could only recoverable by a trusted receiver. The pattern was generated by making a combination of deterministic and random functions. Without knowing the coding parameters, the coded signal was not possible to be recoverable. Both transmitter and receiver should have the same parameters to correctly code and decode the input signal. This Technique can provide security function and a complete graphical control, which might be suitable in some applications. So no one can access data which transferring on open network. It can be modified further according to our use and convenience as modified version of various algorithms are used to increase the security level.

6 REFERENCES

1. J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.
2. M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, A Modified AES Based Algorithm for ImageEncryption, World Academy of Science, Engineering & Technology, 2007.
3. B. Subramanyan, V. M. Chhabria, T. G. S. babu, Image Encryption Based On AES Key Expansion, Second International IEEE Conference on Emerging Applications of Information Technology, 2011.
4. Q. Gong-bin, J. Qing-feng and Q. Shui-sheng, A New Image Encryption Scheme Based on DES Algorithm and Chuas Circuit, Int. Journal of Computer Science and Network Security, VOL.8, No.4, April 2008.
5. W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, Issue 6, Nov 1976.
6. H. Shuihua and Y. Shuangyuan, An Asymmetric Image Encryption Based on Matrix Transformation, Transactions on Computer and Infor- mation Technology, Vol. 1, No. 2, 2005.
7. K.Ganesan, I. Singh and M. Narain, Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps, Fifth International Conference on Computer Graphics, Imaging and Visualization, 2008.
8. K. Gupta, S. Silakari, R. Gupta and S. A. Khan, An Ethical way for Image Encryption using ECC, First I. Conference on Computational Intelligence, Communication Systems and Networks, 2009.
9. M. Naor and A. Shamir, Visual cryptography, Advances in Cryptology- EUROCRYPT94, Lecture Notes in Computer Science, Vol. 950, Springer- Verlag, Berlin, pp. 1-12, 1995.
10. A. M. Jaafar and A. Samsudin, A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation, Int. Journal of Computer Science Issues, Vol. 7, Issue 4, No. 2, July 2010.
11. R. Matthews, on the derivation of a chaotic encryption algorithm. Cryptologia, pp. 2942, 1989.

12. B. Mohammed, G. Mourad, Z. Nourddine, R. Fakhita and B. ElHoussine, Encryption-Compression Method of Images, Int. Journal on Computer Science and Information Systems Vol. 4, No. 1, pp. 30-41, 2009.
13. L. Vorwerk, T. Engel and C. Meinel, A proposal for combination of compression and encryption, Proceedings of Visual Communications and Image Processing, SPIE, Vol. 4067, 2000.
14. I. Masanori, O. Noboru, A. Ayman, M. Ali, New Image Encryption and Compression Method Based on Independent Component Analysis, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, April 2008.
15. C. P. Wu and J. Kuo, Design of Integrated Multimedia Compression and Encryption Systems, IEEE Transactions on Multimedia, Vol. 7, No. 5, 2005.
16. W. Effelsberg and R. Steinmetz, Video Compression Techniques, Heidelberg, Germany: Dpunkt-Verlag, 1998.
17. W. Zeng and S. Lei, Efficient Frequency Domain Selective Scrambling of Digital Video, IEEE Transactions on Multimedia, 5(1), March 2003.
18. T. Maples and G. Spanos, Performance study of a selective encryption scheme for the security of networked real-time video, Proceedings of the 4th International Conference on Computer Communications and Networks, Las Vegas, 1995.
19. I. Agi and L. Gong, An empirical study of secure MPEG video transmission, Symposium on Network and Distributed Systems Security, 1996.
20. M. V. Droogenbroeck and R. Benedett, Techniques for a selective encryption of uncompressed and compressed images, Proceedings of ACIVS, Ghent, Belgium, September 2002.
21. M. V. Droogenbroeck, Partial Encryption of Images for Real-Time Applications, 4th IEEE Signal Processing Symposium, Hilvarenbeek, The Netherlands, pp. 11-15, 2004.
22. O. M. Odibat, M. H. Abdallah and M. B. Al-Zoubi, New Techniques in the Implementation of the Partial Image Encryption , 4th International Multi-conference on Computer Science and Information Technology, Jordan, 2006.
23. K. Hong and K. Jung, Partial Encryption of Digital Contents Using Face Detection Algorithm, Springer-Verlag, 2006.

24. J. M. Rodrigues, W. Puech, P. Meuel, J. C. Bajard and M. Chaumont, Face Protection by Fast Selective Encryption in a Video, The Institution of Engineering and Technology Press, Seattle, WA, 1993.
25. S. Lian, J. Sun, D. Zhang and Z. Wang, A Selective Image Encryption Scheme Based on JPEG2000 Codec, LNCS 3332, pp. 6572, Springer-Verlag, Berlin Heidelberg, 2004.
26. N. Tanejaa, B. Ramanb, I. Guptaa, Selective image encryption in fractional wavelet domain, In. Journal of Electronics and Communications,(AE) 65, pp. 338344, Elsevier, 2011.
27. E. N. Lorenz, The Essence of Chaos, University of Washington Press, Seattle, WA, 1993.
28. H. S. Kellert, In the Wake of Chaos: Unpredictable Order in Dynamical Systems, University of Chicago, pp. 56-62, 1993.
29. L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine 1(3): pp. 6 21, 2001.
30. Rivest, Shamir and Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2): pp.120126, 1978.
31. C. Y. Lin and S. Fu Chang, Generating Robust Digital Signature for Image/Video Authentication, Multimedia and Security Workshop at ACM Multimedia, Bristol, UK. , 1998.
32. T. Chen, J. Wang and Y. Zhou, Combined Digital Signature and Digital Watermark Scheme for Image Authentication, Int. Conferences on Infotech and Info-net, Beijing, 2001.
33. C. S. Lu and H. Y. Mark Liao, Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, IEEE Transactions on Multimedia,Vol.5 ,No.2, 2003.
34. H. Zang, L. Min, Li Cao, An Image Encryption and Digital Signature Scheme Based on Generalized Synchronization Theorem, International Conference on Computational Intelligence and Security, 2009.
35. Cambel, A. B., (1993). Applied Chaos Theory: A Paradigm for Complexity. (Ed. 1). Academic Press, ISBN 0-12-155940-8, London.
36. Kocarev, L., Galias, Z., & Lian, S. (2009). Intelligent Computing Based on Chaos. Studies in Computational Intelligence, Vol. 184 Springer-Verlag, ISBN 978-3-540-95971-7, Berlin.
37. Tenny, R., Tsimring, L. S., Abarbanel, H. D. I., and Larson, L. E. (2006). Security of chaos based communication and encryption. In: Digital Communications Using Chaos and Nonlinear Dynamics (Institute for Nonlinear Science). Springer, 2006, pp. 191–229.

38. Wolfram, S. (1985). Cryptography with cellular automata. In: Advances in Cryptology- Crypto'85, Lectures Notes in Computer Science, Vol. 218, pp.429-432, Springer- Verlag, Berlin.
39. Guan, P. (1987). Cellular automaton publick-key cryptosystem. Complex Systems, Vol. 1, pp.51-57.
40. Dachselt, F., Schwarz, W. (2001). Chaos and Cryptography, IEEE Transactions on Circuits and Systems, Part 1, Special Issue. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 48, No. 12, pp. 1498-1509.
41. Amigó, J.M. (2009). Chaos-Based Cryptography. In: Intelligent Computing Based on Chaos, Springer, ISBN 978-3-540-95971-7, pp. 291-313, Berlin.
42. Robinson, C. (1995). Dynamical Systems, (Ed. 2), CRC Press, ISBN 13: 9780849384936, New York.
43. Boguta, K.. (2011). Sensitivity To Peturbation in Elementary Cellular Automata, from the Wolfram Demonstrations Project http://demonstrations.wolfram.com/SensitivityToPeturbationInElementaryCellularAutomata/
44. Mahieu, E. (2011). Bifurcation Diagram of the Hénon Map from the Wolfram Demonstrations Project http://demonstrations.wolfram.com/BifurcationDiagramOfTheHenonMap/
45. Zech, A., Donges, J. F., Marwan, N. & Kurths, J. (2011). Frequency Distribution of the Logistic Map, from the Wolfram Demonstrations Project, http://demonstrations.wolfram.com/FrequencyDistributionOfTheLogisticMap/
46. Fabre, C. (2011). Chaos Game 2D/3D, from the Wolfram Demonstrations Project http://demonstrations.wolfram.com/ChaosGame2D3D/
47. Devaney, R. L. (1989). Introduction to chaotic dynamical systems. Addison-Wesley Publishing Company, Inc., ISBN 13: 9780201130461, pp. 161-172.
48. Collet, P., Eckmann, J. P. (1980). Iterated Maps on the Interval as Dynamical Systems, Progress in Physics, Birkhauser, Cambridge.
49. Mira, C., Gardini, L., Barugola, A., Cathala, J. C. (1996). Chaotic Dynamics in Two-Dimensional Noninvertible Maps, World Scientific Series on Nonlinear Science, World Scientific. Series A, vol. 20, ISBN: 978-981-02-1647-4.

50. López-Ruiz, R., Fournier-Prunaret, D. (2003). Complex Patterns on the Plane: Different Types of Basin Fractalization in a Two-Dimensional Mapping, International Journal of Bifurcation and Chaos, World Scientific, Vol. 13, pp. 287-310.
51. Fournier-Prunaret, D., Lopez-Ruiz, R., Taha, A. K. (2006). Route to Chaos in Three-Dimensional Maps of Logistic Type, Grazer Mathematische Berichte, Vol. 350, pp. 82-95.
52. Alvarez, G., Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, World Scientific, Vol. 16, pp 2129-2151.
53. Kocarev, L., Lian, S. (2011). Chaos-Based Cryptography. Theory, Algorithms and Applications. Studies in Computational Intelligence, Vol. 354, ISBN 978-3-642-20542-2, Berlin.
54. M. S. Baptista, Cryptography with chaos, Phys. Lett. A 240 (1999) 50–54.
55. M. S. Baptista, Cryptography with chaos, Physics Letters A 240, pp. 50-54, Elsevier Science, 1998.
56. G. Jakimoski and L. Kocarev, Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms, International IEEE conference on Multimedia, 2007.
57. M. Sharma and M. K. Kowar, Image Encryption Techniques Using Chaotic Scheme: a Review, Int. Journal of Engineering Science and Technology, Vol.2, pp. 2359-2363, 2010.
58. J. Fridrich, Image encryption based on chaotic maps, Proceedings of International IEEE Conference on Sysytems, Man and Cybernetics, Vol. 2, pp. 11051110, 1997.
59. J. Fridrich, Secure image ciphering based on chaos, Technical Report RL-TR-97-155, the Information Directorate of the Air Force Research Laboratory, New York, 1997.
60. J. C. Yen and J. In Guo, A New Chaotic Key-Based Design for Image Encryption and Decryption, IEEE International Symposium on ISCAS, Geneva, pp. 49-52, 2000.
61. M. I. Sobhy, and A. R. Shehata, Chaotic Algorithms for Data Encryption, IEEE Proceeding of ICASSP, Vol 2, pp. 997-1000, 2001.
62. F. Belkhouche and U. Qidwai , Binary image encoding using 1D chaotic maps, IEEE Annual Technical Conference Region 5, 2003.
63. Z. Han and W. X. Feng, A new image encryption algorithm based on chaos system Proc. IEEE Int. Conf. Robotics, Intelligent Systems and Signal Processing. Changsha, China, pp. 778-782, 2003.

64. S. Deng, L. Zhang and Di Xiao, Image Encryption Scheme Based on Chaotic Neural System, Lecture Notes in Computer Science, Volume 3497, pp. 868-872, 2005.
65. M. R. Zhang, G. C. Shao and K. C. Yi, T-matrix and its applications in Image processing, IEEE Electronics Letters, Vol. 40 No. 25, 9th December 2004.
66. Z. YiWei, W. YuMin and S. XuBang, A chaos-based image encryption algorithm using alternate structure, Science in China Series F: Information Sciences, Springe-Verlag, vol. 50, no. 3, 334-341, 2007.
67. M. Ahmad and M. Shamsher Alam, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal on Computer Science and Engineering, Vol.2 (1), pp. 46-50, 2009.
68. I. A. Ismail, M. Amin and H. Diab, A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps, International Journal of Network Security, Vol.11, No.1, PP.1-10, July 2010.
69. G. Srividya and P. Nandakumar, A Triple-Key Chaotic Image Encryption Method, International Conference on Communications and Signal Processing (ICCSP), 2011.
70. N. K. Pareek, Vinod Patidar, K. K. Sud; "Image encryption using chaotic logistic map", Image and Vision Computing 24 (2006) 926-934.
71. B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption, Cambridge Security Work- shop Proceedings (December 1993), pp. 191-204, Springer-Verlag, 1994.
72. Jakimoski, G. and L. Kocarev. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps‖. IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 48(2): 163-169, 2001.
73. Y.B. Mao, G. Chen, S.G. Lian, A novel fast image Encryption scheme based on the 3D chaotic baker map Int. J. Bifurcate Chaos, vol. 14, pp. 3613–3624, 2004.
74. H. Gao, Y. Zhang, S. Liang, and D. Li, A new chaotic algorithm for image encryption, Chaos, Solutions &Fractals, vol. 29, no. 2, pp.393–399, 2006.

75. Su Su Maung, and Myitnt Myint Sein, A Fast Encryption Scheme Based on Chaotic Maps, GMSARN International Conference on Sustainable Development: Issues and Prospects for the GMS, 2008.
76. Musheer Ahmad and M. Shamsher Alam, A New Algorithm of Encryption and Decryption of Images Using Chaotic Mappin, International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.
77. Fengjian Wang, Yongping Zhang and Tianjie Cao. Research of chaotic block cipher algorithm based on Logistic map, 2009 Second International Conference on Intelligent Computation Technology and Automation, 2009: 678 – 681.
78. Po-Han Lee,Soo-Chang Pei and Yih-Yuh Chen, Generating Chaotic Stream Ciphers Using Chaotic Systems, Chinese Journal Of Physics Vol. 41 , No. 6, 2003.
79. Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:406-407.
80. Deergha Rao and K. Gangadhar, Modified Chaotic Key-Based Algorithm for Image Encryption And Its VLSI Realization, International Conference on Digital Signal Processing, 2007.
81. H.E.H. Ahmed, H.M. Kalash, and O.S.F. Allah, An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption", presented at Informatica (Slovenia), 2007, pp.121-129.
82. Shubo Liu, Jing Sun, Zhengquan Xu An Improved Image Encryption Algorithm based on Chaotic System, journal of computers, vol. 4, no. 11, 2009, pp.1091-1100.
83. Abir Awad, Abdelhakim Saadane, Efficient Chaotic Permutations for Image Encryption Algorithms, Proceedings of the World Congress on Engineering Vol I, 2010.
84. Ai-hong Zhu, Lia Li, Improving for Chaotic Image Encryption Algorithm Based on Logistic Map, 2nd Conference on Environmental Science and Information Application Technology, 2010.
85. Chenghang Yu, Baojun Zhang and Xiang Ruan(2011),The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption, Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).
86. C.K. Huang and H.H. Nien(2009), Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282 (2009) 2123–2127.

87. Ercan Solak, Rhouma Rhouma and Safya Belghith(2010),Cryptanalysis of a multi-chaotic systems based image cryptosystem, Optics Communications 283 (2010) 232–236.
88. G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam(2011), Image Encryption Based on Diffusion and Multiple Chaotic Maps, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.
89. Komal D Patel, Sonal Belani(2011),Image Encryption Using Different Techniques: A Review, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011).
90. LEI Li-hong ,BAI Feng-ming,HAN Xue-hui(2013), New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos, International Conference on Computational and Information Sciences.
91. Rajinder Kaur, Er.Kanwalprit Singh (2013).Image Encryption Techniques: A Selected Review, IOSR Journal of Computer Engineering (IOSR-JCE) e- ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83.
92. Rashidah Kadir, Rosdiana Shahril, Mohd Aizaini Maarof(2010), a modified image encryption scheme based on 2D Chaotic map, International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010, Kuala Lumpur, Malaysia.
93. Shubo Liu, Jing Sun1, Zhengquan Xu(2009), An Improved Image Encryption Algorithm based on Chaotic System, Journal of Computers, Vol. 4, No. 11.
94. S.HRAOUI, F.GMIRA, A.O.JARAR, K.SATORI and A.SAAIDI (2013), Bench marking AES and Chaos Based Logistic Map for Image Encryption, 978-1-4799-0792-2/13/$31.00 ©2013 IEEE.
95. XiaoJun Tong, Yang Liu, Miao Zhang and Zhu Wang (2012), A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map, 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science.
96. Yunpeng Zhang, Peng Sun, Jing Xie and Lifu Huang (2010), A New Image Encryption Algorithm Based on Arnold and Coupled Chaos Maps, International Conference on Computer and Communication Technologies in Agriculture Engineering.
97. Sukhjeevan Kaur Et Al , Int.J.Computer Technology & Applications, , A Review Of Image Encryption Schemes Based On The Chaotic Map, Vol 5 (1),144-149, (2014).

98. G. Chen, Y.B. Mao, C.K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps", Chaos, Solitons and Fractals 12, pp. 749-761, 2004.

99. Y.B. Mao, G. Chen, S.G. Lian, "A Novel Fast Image Encryption Scheme Based on the 3D Chaotic Baker Map", Int. J. Bifurcat. Chaos 14(10), pp. 3613-3624, 2004.

100. Sandhya Rani et al. International Journal of Advanced Computer Research (ISSN) (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue, (2014).

101. Musheer Ahmad and M. Shamsher Alam. Musheer Ahmad, "A new algorithm of encryption and decryption of images using chaotic mapping" International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50.

102. Ninth International Conference on Computational Intelligence and Security, A Symmetric Image Encryption Scheme Using Chaotic Baker map and Lorenz System, Chong Fu*, Wen-jing Li, Zhao-yu Meng, Tao Wang, Pei-xuan Li, (2013), (IEEE).