Image Encryption approach using Chaotic Map for Gray Scale Images

Thesis submitted in partial fulfilment of the requirements for the award of degree of

Master of Technology

in

Computer Science & Applications

Submitted by

Priyanka Takkar

(Roll No.-601534010)

Under the Supervision of

Dr. V.P Singh

Associate Professor

Mr. Ashish Girdhar

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA-147004

July 2017

Certificate

I hereby certify that the work is being presented in the thesis entitled, "Image Encryption approach using Chaotic Map for Gray Scale Images", in the partial fulfilment of the requirements for the award of the degree of Master of Technology in *Computer Science and Applications* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. V. P. Singh and Mr. Ashish Girdhar and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not submitted for award of any degree of this or any other university.

Priyanka Takkar

(Priyanka Takkar)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Girdhar

Mr. Ashish Girdhar

Lecturer

CSED

Dr. V. P. Singh

Associate Professor

CSED

Countersigned by

(Dr. Maninder Singh)

Head

Computer Science & Engineering Department

Thapar University

Patiala

Acknowledgement

I would like to express my sincere gratitude to my mentors and supervisors Dr. V. P. Singh and Mr. Ashish Girdhar for their immense help, guidance, stimulating suggestion and full time encouragement. They always provided me a motivational and enthusiastic atmosphere to work with. It was a great pleasure to do dissertation under their supervision.

I am also thankful to Dr. Maninder Singh, Head, Computer Science & Engineering Department for his constant support and encouragement.

I would like to thank all the faculty members and staff of the department who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of this work.

I express my thanks to my family for their love, support and enthusiastic encouragement without which I could not complete this dissertation. I would like to thank to all my friends who helped me in all possible ways towards the completion of my work.

Finally I thank the Almighty who gave me the strength to complete the work.

Priyanka Takkar

(Priyanka Takkar)

601534010

Abstract

With the immense growth of multimedia technology, technologies are required to securely transmit the information over the internet. Conventional algorithms are not good regarding to the safety of image transmitted over the internet and complex to use. So, Image encryption algorithms have been proposed to securely transmit the image over the internet. An exploratory study is performed over various scrambling techniques based on chaotic map. Firstly, image is scrambled with chaotic sequences and flipping such as pixel value is altered using logistic chaotic map while pixel position is altered using flipping. To enhance the security of an image transferred over the internet, another image encryption algorithm is proposed. The image has been divided into blocks and chaotic matrix is generated using Ikeda Map. Each block of image is scrambled by manipulation the column and row shuffling with chaotic matrix. All the scrambled blocks of an image are recombined to get scrambled image. All the pixels of scrambled image are diffused with dynamic index based diffusion. A Comparative study is performed on both the algorithms. During the simulation evaluation, it can be seen that second algorithm provides more security, can resist against attacks and is less correlated than first algorithm.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

A lot of data is communicated over the internet with the immense growth of multimedia technology. Information transmitted over the internet can be edited or replicated by unauthorized users. Because of its broad sharing, security of data is an incredible research zone. Data transmitting over the web is of various sorts, for example, data, sound, image, video and so forth. Image is better than data regarding more content, redundancy and intensity value's frequency. There is prerequisite of continuous image encryption calculations to scramble the image amid transmission.

1.1 Need of Security

Information security is required to carry out the following tasks:-

- To keep the information protected from unauthorized users.
- To keep the information protected from being altered or duplicated from unauthorized users.
- To securely transfer the information to the authenticated users.

1.2 Image Encryption

Encryption is a procedure to change over original message, for example, plain image into cipher image, for example, its scrambled shape. Encryption algorithms utilizes key to encode or unscramble the information. Encryption and Decryption of information is performed utilizing key and calculation. These days, data security is getting to be noticeably imperative in information storage and transmission. Images are generally utilized as a part of various procedures. In this manner, security of image information from unapproved clients is required. Image encryption assumes an imperative part in the field of data covering up. Image encryption changes the data into indistinguishable shape so no unapproved clients approach original data or some other sort of data conveyed over the web.

Image encryption is a strategy that changes digital image into disarranged one to make it outwardly confused. The purpose behind the image encryption is to protect the original image's content. There are two stages in image encryption- Confusion

stage and diffusion stage. Confusion phase realigns the pixel value of an image while diffusion phase alters the pixel value of an image.

1.2.1 Types of Encryption

There are two sorts of encryption: - one is Symmetric key encryption and another is asymmetric key encryption. There two are examined as takes after:-

- **Asymmetric key Encryption**

Asymmetric key encryption scrambles the information at the sending end and decodes the information at the receiving end with distinctive keys. It scrambles the information with the public key while decodes the information with private key. Private key is kept secured while public key is shared. Fig 1.1 demonstrates the asymmetric key encryption.

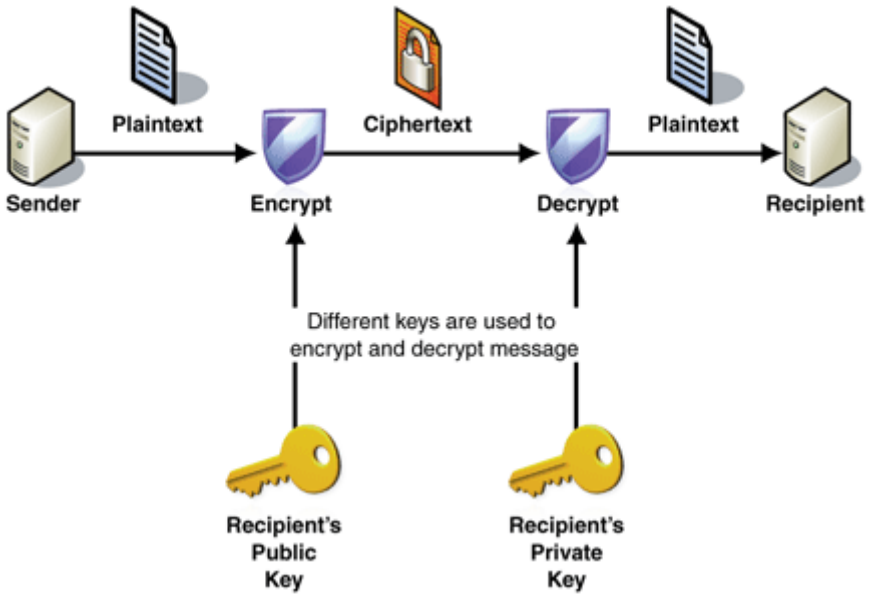


Fig 1.1 Asymmetric Encryption Technique[33]

- **Symmetric key Encryption**

Symmetric key encryption encrypts the data at the sending end and decrypts the data at receiving end with the same key. It is fast method than asymmetric key encryption. If key is random then encryption method performs better. We can also say Symmetric key encryption is known as Scrambling. Fig 1.2 shows the symmetric key encryption.

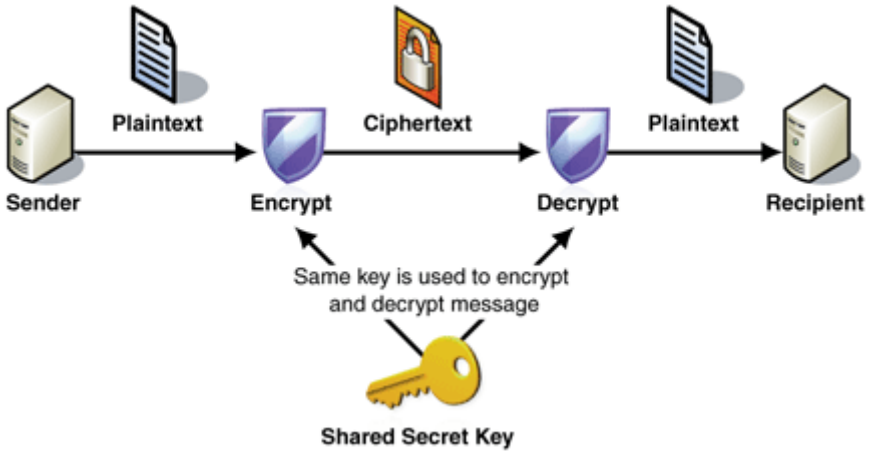


Fig 1.2 Symmetric Encryption Technique[34]

1.3 Security Attacks

These are the types of attacks occurred on image encryption scheme to get the information:-

1.3.1 Known plaintext Attack

A known plaintext attack is type of attack when hacker attacks on both plaintext and ciphertext. This type of attack helps hackers to obtain secret keys.

1.3.2 Chosen plaintext Attack

A chosen plaintext attack is type of attack when hacker gets ciphertext for a random plaintext. The goal of this attack is to get information by lowering the security of information.

1.3.3 Ciphertext-only Attack

A Ciphertext-only attack or known ciphertext attack is a type of attack when hacker attacks only have information of ciphertext. Hacker doesn't have any information regarding to plaintext. But in practical, hacker has some information like in which language plaintext is written.

1.3.4 Chosen ciphertext Attack

A chosen ciphertext attack is type of attack when hacker decrypts the cipher text and collects the information. This information is then used to crack the secret key.

1.4 Security Services

1.4.1 Data Confidentiality

Confidentiality is to keep the information secure from unauthorized users. It also leads to the procedures to prevent the disclosure of confidential data from unauthorized users. Encryption is the method of protecting information. Encryption ensures that only authenticated people can read the information such as people who know the secret key. Encryption is widely used in most of the protocols. An example of confidentiality is security protocol such as SSL/TLS which ensures security. To ensure confidentiality, permission of file and access control is used to restrict access.

1.4.2 Data Integrity

To maintain the accuracy, consistency and reliable information leads to Data integrity. The process of protecting information from unauthorized users for being altered is known as integrity. Data should not be changed in communication and integrity ensures that data received is same to the original form. Only correct information is relevant. Checksums is applied with the data for the verification of data. To restore the affected data, Backup is available.

1.4.3 Data Availability

Availability refers to ensure that authorized users are able to get the information whenever they required. A very common attack is to deny the access to the information. With the help of DDoS attack, high profile websites have been blocked. The aim of DDoS attack is deny users to access the resources of website. With the help of Backup, data is available to unauthorized users. Redundancy is appropriate for sensitive information. It is also important to maintain the updated information that should be available to users.

1.4.4 Access Control

To limit and control the access to applications for users is Access Control. To achieve this, each entity who is trying to access is first authenticated in order to provide the access rights to individual. Restriction of access provided to every individual is known as Access control. Fig 1.3 shows CIA Triad.

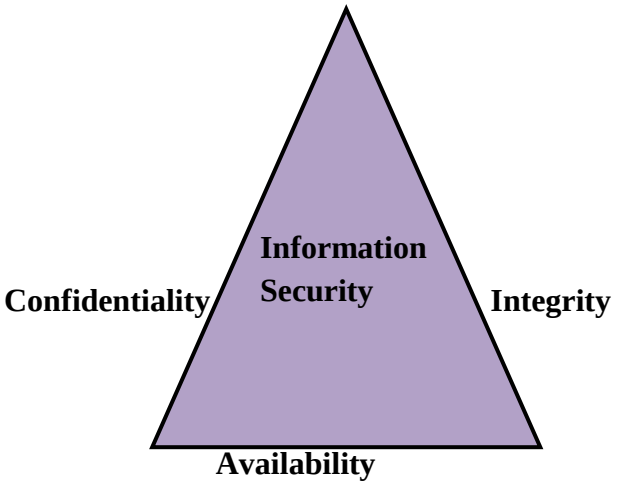


Fig 1.3 CIA Triad

1.5 Security Mechanisms

1.5.1 Encipherment

Encipherment refers to hiding or covering information. Encipherment leads to keep the information protected from unauthorized users. It helps to provide data confidentiality. Encipherment converts the plain text into cipher text.

1.5.2 Decipherment

Decipherment is the procedure to convert cipher text into plain text. Decipherment is performed at the receiver side. Encipherment and decipherment require the use of key and initialization variable, which is required for randomness of cipher text.

1.5.3 Data Integrity

Different schemes have been used to check the integrity of data. Check value is used to see whether the data integrity is preserved or not. The check value is send by the sender and receiver also creates its own check value and compares the both check values to check the integrity of the message.

1.5.4 Authentication Exchange

Digital signatures are bind to the document at the creation time. A digital signature is considered as an authentication. Key management mechanism is considered as another authentication as only users can access the data that has key.

1.5.5 Access Control

The keys or passwords can be used as access control methods to allow users to access data.

1.6 Merits of Encryption

1.6.1 Provides security

During the transmission of data, there is possibility of data being attacked. Encryption provides security as the encrypted form or ciphertext cannot be read by unauthorized users.

1.6.2 Maintains Integrity

Information is even pirated by unauthorized users. With the help of encryption algorithms, we are able to detect the information at the receiving end has been altered. This allows reacting for cyber attack.

1.6.3 Protects Privacy

Encryption is used to secure sensitive information. As there is lot of sensitive information for military, encryption is used to keep information protected from unauthorized users. This helps to ensure privacy.

1.6.4 Part of Compliance

Organizations that have people's personal information require strict compliance to secure that information. HIPAA, FIPS and other regulations used security methods such as encryption to keep the data secure.

1.6.5 Protects Data across Devices

Nowadays, smart phones are widely used and data transferring from one device to another device requires security. Encryption can protect data across devices even during transferring of data. Advanced security such as authentication also helps to detect unauthorized users.

1.7 Applications of Encryption

1.7.1 Steganography

Encryption can be applied to steganography. Steganography is technique of embedding secret message into cover media. Secret message is encrypted and then embedded to cover media and transmit over the internet.

1.7.2 Digital Watermarking

Advanced watermarking is utilized to give the legitimacy of an archive. Encoded credibility is hard to duplicate. Encryption keeps copyright from unapproved clients. With the encryption, it is hard to remove watermark.

1.7.3 Multipurpose Internet Mail Exchange (MIME)

MIME (Multipurpose Internet Mail Exchange) is utilized for encoding heterogeneous information sorts inside a single message. Messages are encoded utilizing base64, for example, encode non-content information with content information. MIME is utilized for encoding any content, pictures and applications.

1.7.4 Secure Electronic Transaction (SET)

SET (Secure Electronic Transaction) is convention created by Visa and MasterCard. It utilizes public key to guarantee secure installment.

1.8 Chaotic Map

Chaotic map is utilized to produce disordered sequences and these arrangements are then utilized as a part of image encryption. Chaotic map is much agreeable for image encryption because of its fundamental qualities. Chaotic map is subtype of non-direct dynamical frameworks. Chaotic map is broadly utilized in light of its properties, for example, deterministic, periodicity, ergodicity, non-linear, irregular behaviour. A minor change in the underlying estimations of confused framework prompts noteworthy change in the result.

Advantages of chaotic System:-

- Parameter of chaotic map and introductory condition is required to generate chaotic map.
- The chaotic succession will be enormously changed with the minor change in beginning condition.
- It generally creates same chaotic sequence with one beginning condition.
- To recover an original message, exact knowledge of initial conditions and system parameters are required.
- Due to highly sensitive nature of initial values and parameters, chaotic system is robustness and effectiveness.
- Chaotic system is deterministic.

1.9 Cellular Automata

Cell automata contain number of indistinguishable cells and cells are arranged in rectangular matrix in at least one measurement. Every one of the cells all the while refresh their cell states by applying move capacity with the end goal that as indicated by the predefined nearby control of association between the neighbours of the cell. Consider the information is the condition of the cell and neighbouring conditions of cell. A cellular automaton is widely used in image encryption due to its complex behaviour and generates useful operations. In terms of living space, cellular automata can be 1-D, 2-D, 3-D or higher dimensions.

The following categories of 1-D Cellular Automata:-

- Ordered Behaviour
- Periodic Behaviour
- Chaotic Behaviour
- Complex Behaviour

While ordered and periodic behaviour is predictable, chaotic behaviour is unpredictable and complex behaviour is somewhere in the move from periodic to chaotic and indicates complex conduct.

1.9.2 Types of cellular automata:-

(a) Uniform cellular automata

Same state move manage for every one of the cells of cell automata then those cell automata is known as uniform cell automata.

(b) Hybrid Cellular automata

Diverse state move govern for every one of the cells of cell automata then those cell automata is known as hybrid cell automata.

1.9.3 Boundary Conditions of Cellular Automata:-

Boundary condition is required in case of finite grids to determine which cell is left neighbour of furthest left cell and which cell is correct neighbour of furthest right cell.

There are three types of boundary conditions:-

- Periodic: - 1-D rows become circles such that their extraordinary cells wind up noticeably nearby each other.
- 2-D matrices progress toward becoming toroids with the end goal that their extraordinary furthest left segment will be neighbour to furthest right segment and best column will be neighbour to base line.
- Static: - Extreme cells are connected to permanent zero state cells.

1.9.4 Neighbourhood of Cellular Automata:-

- **1-D Cellular Automata**

In the event of 1-D cell automata, the cell itself, one cell to its quick left and another cell to its prompt right. For example, a b c

where ‘ a’ is the cell itself, ’b’ is immediate left neighbour of ‘a’ and ‘c’ is immediate right neighbour of ‘a’.

- **2-D Cellular Automata**

There are two neighbourhood methods are used in case of 2-D cellular automata:-

(a) Vonneumann Neighborhood

The Von Neumann neighbourhood of range t is given as:-

$$NH(p_0, q_0, t) = [(p, q): |p - p_0| + |q - q_0| \leq t]$$

And number of cells in each neighbourhood is $2t(t + 1) + 1$. A range of one is commonly used leads to five neighbours. Fig 1.4 shows that Vonneumann neighbourhood.

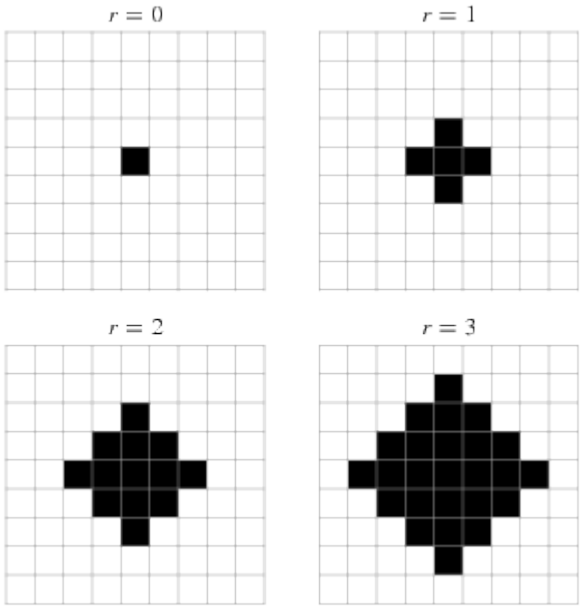


Fig 1.4 Vonneumann Neighbourhood [35]

(b) Moore Neighbourhood

The Moore neighbourhood of range t is given as:-

$$NH(p_0, q_0, t) = [(p, q): |p - p_0| \leq t, |q - q_0| \leq t]$$

And the number of cells in each neighbourhood is $(2t + 1)^2$. A range of one is commonly used leads to nine neighbours. Fig 1.5 shows the Moore neighbourhood.

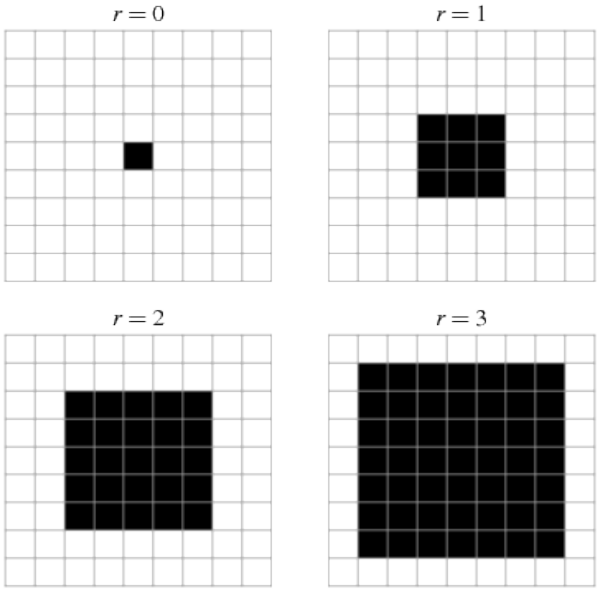


Fig 1.5 Moore Neighbourhood [36]

Chapter 2

Literature Survey

2.1 Related Work

To encrypt an image, many image encryption algorithms have been proposed by different researchers. Conventional scrambling change the pixel positions while total scrambling change the pixel positions as well as pixel values. Total scrambling is better than conventional scrambling because histogram is changed after total scrambling that leads to more secure but histogram is same in case of conventional scrambling. Different image scrambling techniques based on spatial domain, chaotic map and cellular automata have been discussed.

2.2 Image Scrambling based on spatial domain

Min Li et al. [1] proposed an algorithm which scrambles the non-square image by dividing the non-square image into different square regions. The traditional Arnold transform scrambles only square images. Each square region of image is scrambled different number of times to enhance the security of algorithm. It restores the image correctly with the keys which keep the image safe and algorithm has reliable transmission.

Due to periodicity of Arnold transformation, it is widely used. But a lot of time gets wasted to find its periodicity. Lingling Wu et al. [7] presented an improved anti-arnold based transformation which descrambles the image with the same iteration steps as with scrambling the image. With this algorithm, a lot of time get save to restore an image.

Ping Ping et al. [2] proposed an algorithm based on non-linear map known as Henon map. It is easy for attackers to discover the connection between plain image and cipher image which is scrambled with the linear map. The keys of this algorithm are the parameters of henon map and with the iteration of henon map, the image pixels are realigned. The non-linear property enhance the security of algorithm while the limitation of this algorithm it can be only applied to square images.

Yang Zou et al. [10] proposed an image scrambling algorithm in light of Sudoku Puzzle. Sudoku puzzle is a diversion where each incentive from 1-N seems just once in each line and section. Since in Sudoku puzzle, the pre-filled units and their area can be the key of the scrambling. The pre-filled units can be any number from 1-N and can find any place in the puzzle so it is elusive the right key to restore an image. With a specific end goal to upgrade the security of an algorithm, this algorithm scrambles the image both at pixel level and at bits level.

Xiuli Chai et al. [13] displayed an outwardly secure image encryption algorithm in light of compressive detecting. Change the plain image into coefficient grid utilizing DWT and afterward mixed by plain image crisscross way and after that encodes into compressed cipher image by compressive sensing. This cipher image is embedded over the carrier and after that get outwardly secure cipher image. This algorithm has high security. Size is same in both plain image and cipher image. This encryption technique has high affectability to the plain image. This algorithm can likewise overcome chosen-plaintext and known-plaintext attacks.

2.3 Image Scrambling based on chaotic map

LIU Xiangdong et al. [3] proposed an algorithm based on chaotic system and sorting transformation. With the sorting of chaotic sequences, the algorithm calculates permuting address codes. The complexity of this algorithm gets reduce as this algorithm does not require knowing probability density function of the disordered orbits ahead of time. This algorithm provides a high level security.

Guodong Ye [4] presented a novel algorithm based on chaotic system and with pixel bit. This paper uses a single chaos map which encrypts both position value and gray value. This method can be used directly to communicate the images over the internet. This method can be enhanced to high dimensional chaos map and applied to 3D images.

Wang Yangling [5] presented a method which scrambles the image with the chaotic sequences and mapping. First, chaotic sequence is generated with chaotic map. Each pixel of an image is altered by applying bit-exclusive or operation on pixel value with disordered sequences. Then, image mirror mapping is performed to get the

encrypted image. This calculation is simple and feasible, slow speed of encryption and impact of encryption is great and exceptionally secure.

M.Y. Mohamed Parvees et al. [6] presented an algorithm which has used two chaotic maps-Logistic and Ikeda Map. Logistic map is used to change the position of colour bytes while Ikeda map is used to alter the colour bytes value. The combined chaotic encryption algorithm can encrypts the image of any size. It is very difficult to crack this algorithm by unauthorized person as it uses both chaotic maps. Chaotic maps are implemented at different places which keep algorithm protected and secure.

Lu Huiying et al. [8] presented a novel arithmetic image coding algorithm based on 2D generalized logistic mapping. With the logistic chaotic map, two 2D chaotic sequences are generated according to the size of the image. Image is scrambled by sorting the chaotic sequence. Key stream is generated by optimizing the chaotic sequence, which is used to mask the image data. During the arithmetic coding process, the coding interval order is controlled by the chaotic sequence. This algorithm has high security and has good robustness.

A. Kanso et al. [9] presented a novel encryption algorithm which uses 3D chaotic map. This algorithm has three tenets rearranging, mixing and scrambling procedure of digital image. This algorithm overcomes different assaults, for example, differential, statistical and casuality assaults. Results demonstrate that this algorithm has great security and is effective.

Arnold cat map and Hilbert transformation can meet the demands of image encryption methods over the internet. Input binary flow of image can be encrypted by S-DES but with the few keys will bring risks. X Y Yu et al. [11] presented an image encryption method based on chaotic map and S-DES. By applying the sensitivity of logistic chaotic map, large quantities of key is generated and key is real-time.

Liang Zhao et al. [12] presented an algorithm which presents attacks- chosen-plaintext attack and chosen-ciphertext attack. A correlation is additionally made between these assaults and Li Lo assault [32] which was likewise proposed to original image encryption algorithm. These attacks have less computational complexity then Li Lo attack. An improved encryption scheme with the self

correlation is proposed to overcome the drawbacks of original image encryption method. This algorithm is highly secured than original one. This algorithm can be further improved for future work.

Lu Xu et al. [14] exhibited a novel image encryption algorithm which separates the image into blocks in vertical or horizontal directions. The logistic map is utilized to make swapping control tables. The swapping control table is utilized to swap the pixel in the present block or other blocks. To diffuse the pixels of cipher image, the diffusion index scheme is utilized. This algorithm can adequately vanquish known-plaintext and chosen-plaintext assaults. It can likewise be all around utilized for double image scrambling.

Xingyuan Wang et al. [15] proposed a novel image encryption algorithm which encrypts the image by combining chaotic mapping and reversible cellular automata (RCA). Intertwining logistic map is utilized to permute the pixel value of an image and also change the value of pixel. The cipher image is generated through reversible cellular automata after many generations on bit level. This algorithm has protection of information perfectly and also satisfied confusion and diffusion properties.

Omid Mirzaei et al. [16] presented an image encryption scheme which is based on total shuffling and parallel encryption algorithm. To confuse the pixels of an original image, two chaotic systems have been used. First, digital image is divided into different blocks and shuffle the position of each block. To encrypt each pixel in each of four blocks, different values are used. These values are:-values generated from chaotic sequence, pixel value in original image and pixel value obtained from another block. This algorithm is very fast, possesses high security and has large key space.

Ana Cristina Dascalesu et al. [17] presented a novel chaotic map based algorithm which generates random permutations for image scrambling by high-shift factor. With this algorithm, fixed points are less. The image is scrambled by random permutations with high move factor. This algorithm is efficient and encryption speed is fast. It can also be used for real-time scrambling.

C.K. Huang et al. [18] proposed an algorithm which encrypts the image by row shuffling, column shuffling and gray level encryption. This algorithm first shuffles

the pixels of the image by row shuffling. Then this cipher image is shuffled by column shuffling. To enhance the security of encryption, gray level encryption is implemented. This algorithm is highly secure and cipher image is greatly changed after encryption.

2.4 Image Scrambling based on cellular automata

Rong-Jian Chen et al. [19] presented an algorithm which encrypts the image by altering of the pixel position of an image and changing the pixel values of an image. Scan patterns produced by SCAN strategy is utilized to permute the pixel value of an image. Cell automata are utilized to alter the pixel value of an image. Because of CA property, this algorithm satisfies confusion and diffusion property. This algorithm has extensive number of keys and lossless.

Ruisong Ye et al. [20] presented a novel image scrambling and watermarking scheme based on cellular automata. The chaotic features of cellular automata are analyzed and compute the fractal box size of cellular automata. Digital image scrambling can be used first for the watermarking scheme. This algorithm is vigorous against assaults, for example, cropping, noising and compression.

Maryam Habibipour et al. [21] presented an image encryption algorithm which replaces the pixel values of an image by indefinite cellular automata and chaos theory. Based on chaotic sequence, cellular automata rules are defined and these rules are stored in private key. This algorithm has large key space, symmetric private key, diffusion, confusion and pixel value replacement.

WEI Qin et al. [22] presented an algorithm to encrypt an image based on weighted and p-interval CA. Generate the new matrix with two-dimension p-interval and weighted approach which includes optional parameters that gives large number of security keys. The encryption speed of this algorithm is fast.

Abdel Latif Abu Dalhoum et al. [23] presented an algorithm which scrambles the digital image using 2D cellular automata. This algorithm provides high security as it scramble pixel locations of an image using double scrambling-image is scrambled in both vertical directions and horizontal directions. If algorithm is known to attacker then even image cannot be decode. With the usage of GA cellular automata, the

speed of encryption is improved. This algorithm can scramble the image of any size and can encode colour image, grayscale image and binary image.

LOU Yuefang et al. [24] exhibit a novel image encryption algorithm which depends on 2-D cell automata and enhanced standard map. To upgrade the pseudo-randomness of the algorithm, chaotic sequences are used to decide the state move rules of every cell. With the standard map, the chaotic sequence is produced which is utilized to scramble the digital image. As per parallel computation and pseudorandom quality, the pixel values of an image are changed. This algorithm has substantial key space, profoundly secure and can oppose chosen plaintext assault. The cipher image has good diffusion property.

Chuan Peng et al. [25] proposed an algorithm for image encryption utilizing couple chaotic system and couple cell automata. The chaotic sequence is produced utilizing couple chaotic system which has bigger key space and more complex dynamic attributes than general chaotic system. To begin with, digital image is separated into symmetric parts and scramble the image utilizing couple chaotic system and after that encoded utilizing couple toggle cell automata. This algorithm has substantial key space and can oppose brute assault and differential assault

Subrata Nandi at al. [26] encrypts the image using 1-D group cellular automata. This algorithm is similar to symmetric key encryption. As group cellular automata possess cyclic nature, so it is easy for encode and decode. This algorithm is lossless scheme. It can also be applied to colour images.

Samaneh Zamani et al. [27] proposed an image encryption scheme utilizing hyper chaotic system and Fuzzy cell automata. Hyper chaotic system has complex dynamic attributes than chaotic system. To upgrade the security and speed of algorithm, four hyper chaotic system is utilized. Plain image is separated into four sections and each sub-image has its own hyper chaotic system. Pixels in two adjoining sub pictures are chosen to change their positions. In encryption stage, five 1-D Fuzzy cell automata is utilized. To take care of the issue of recursive principles in administer choosing process, two diverse encryption strategies are utilized for even and odd cells. This algorithm is profoundly secure, for example, confusion and diffusion property and touchy to little changes in the key.

Ping Ping et al. [28] scramble the image using life-like cellular automata. To obtain scrambling matrix, a life-like cellular automata with an initial configuration is keep running for a few generations. The different CA initial configurations are used to achieve good diffusion property. This algorithm effectively lowers the correlation coefficient and can resist noise attack.

Ping Ping et al. [29] proposed CA based image scrambling technique which permute image at gray level and alter the pixel position. Firstly change over the image into binary image. With the assistance of scrambling network created by 2-D cell automata, the binary image is permuted at bit-level. This algorithm gives higher security by changing the pixel position and pixel value of an image. This approach is powerful to known-plaintext assault and chosen-plaintext assault. This algorithm can be enhanced to digital image of any size.

Abdel Latif Abu Dalhoum et al. [30] convert the digital image into meaningless form for the security reasons. Cellular automata have lot of parameters that show complexity and each parameter is differing in terms of complexity and behaviour. This paper has used simple cellular automata instead of 2D cellular automata. The parameters that were tested in this algorithm- the number of generations effect on scrambling, boundary types-periodic and static, rules. This algorithm when compared to scrambling techniques with 2D cell automata gives comparable outcomes without redundancy and gives better outcomes with reiteration.

Xingyuan Wang et al. [31] presented a novel image encryption algorithm which uses Langton’s Ant cellular automata to scramble the image. The thought is to combine 2D basic attributes of the image with "chessboard" and let the Langton's Ant creep on it. We can get the scrambled image with the result of each step of cellular automata. This algorithm is secure and resist to common attacks.

Chapter 3

Problem Statement and Objectives

3.1 Problem Statement

With the immense growth of multimedia technology, data is communicated over the internet. So, there is a requirement to secure the information communicated over the internet. There are lot of traditional encryption methods to secure the data transmitted over the internet such as AES, DES and RSA algorithm. As images contain lot of information rather than text, images are great carrier of information communicated over the internet. Traditional encryption techniques have many disadvantages such as encryption speed is slow, the singleness of secret key, structure complexity and also it is difficult to secure the images that contains lot of information with these algorithms.

Conventional algorithms have following disadvantages which it less efficient:-

- Traditional encryption scheme is good regarding to safety but not excellent and encryption's effect is not good. It is easy to decipher the traditional encryption algorithm because conventional encryption algorithm encrypts the image by considering the image as information and data stream. So, it is very easy to crack the encryption algorithm and actual information will be revealed. There is requirement of strict security because of confidential data. Hence, it does not secure the images transferred over the internet.
- Traditional encryption algorithm is expensive and time consuming.
- Traditional encryption algorithms are very complex to use and hence people use algorithm incorrectly. This could lead to fail to encrypt data when they wish to encrypt the data and encode the data when they do not require encrypting the data.

3.2 Thesis Objectives

Modern image encryption algorithms securely transmit the images over the internet.

The objective of thesis is:-

- To study the various encryption algorithms based on spatial domain, chaotic sequences.
- To propose a new algorithm based on chaotic sequences and flipping.
- To propose a new algorithm based on pixel shuffling and diffusion.
- Validate the proposed algorithm with the simulation results.

Chapter 4

Implementation

Because of absence of safety efforts, some encryption algorithms cannot encode the image safely. This leads to that some action to be taken to send the image to other end securely as it may contain confidential information. To resolve the above problem, image is scrambled to transfer from one end to other end instead of plain image. With the different scrambling techniques, image is scrambled at the sender side and descrambling is performed at the receiver side and then original image is retrieved.

4.1 Scrambling

Scrambling is a technique of converting original image into meaningless form so that it cannot appear originally. With the help of mathematical transformations, the positions of the pixel of an image are changed than their current position. In this way, we transfer encoded form of image over the internet rather than original image. Fig 4.1 shows scrambling and descrambling process of an image where symmetric encryption is used and at sender side and receiver side, same key is used.

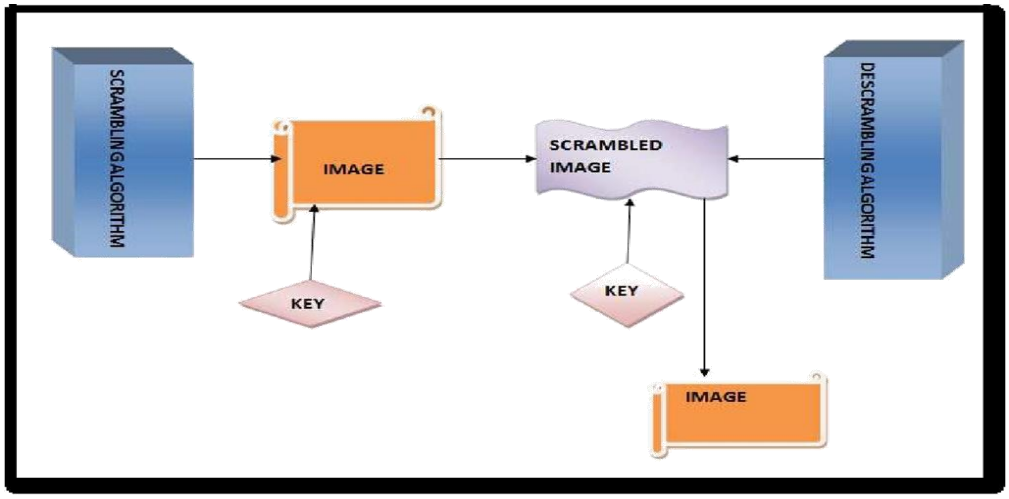


Fig 4.1 Process of scrambling and descrambling an image

4.2 Image Encryption Algorithm using chaotic sequences and flipping

Step1: Read the image R of size $U \times V$ where U is the width of the image and V is the height of the image. R (d, e) denote the image pixel value (d=1,2,....U ; e=1,2.....V).

Step 2: Generate a chaotic sequence p_r(r=1, 2...U× V) utilizing (1) where μ and x_0 are keys.

Step 3: Multiply chaotic sequence with 256 to make it regular numbers h_g(g=1, 2 ...U× V).

Step 4:Convert 1D h_g into 2D H(d, e)(d=1,2,...U ;e=1,2,....V).

Step 5: To alter the pixel value of an image, bit exclusive operation is performed on pixels of an image and chaotic matrix.

Step 6: To alter the position of pixel, flip the pixels of an image in horizontal direction and vertical direction. Fig 4.2 demonstrates the flowchart to encode the image.

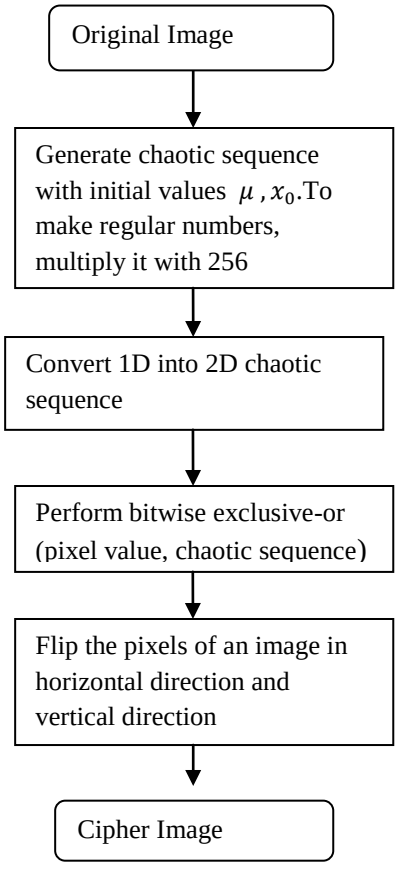


Fig 4.2 Flowchart to encrypt an image

4.3 Image Encryption Algorithm of pixel shuffling and diffusion phase

To enhance the security of information transmitted over the internet, another image encryption algorithm is proposed. In this image encryption algorithm, first the image is divided into four blocks and generate chaotic matrix with Ikeda Map. Each block of image is scrambled with column shuffling and row shuffling with the chaotic matrix. All the scrambled blocks of an image combined to get cipher image. All the pixels of scrambled image are diffused with dynamic index based diffusion.

Divide the image into four equal blocks. Suppose the size of plain image is $P\ X\ Q$. Divide it into four equal blocks img1, img2, img3, img4 which have size $P'\ X\ Q'$ where $P'= P/2$ and $Q'= Q/2$.

4.3.1 Block Scrambling

Use the key (x_o, y_0, u) and Ikeda Map to generate chaotic sequence. Use Eq. (1) and Eq. (2), iterate the chaotic sequence m times where $m = P'Q'$ and obtain the sequence x , y.

The Ikeda Map equation is given as follows:-

$$x_{k+1} = \left(1 + u * \left((x_k cos\ t_k) - (y_k sin\ t_k)\right)\right) mod\ 1, u \geq 0.6 \quad (1)$$

$$y_{k+1} = \left(u * \left((x_k sin\ t_k) + (y_k cos\ t_k)\right)\right) mod\ 1, u \geq 0.6 \quad (2)$$

$$t_k = 0.4 - \left(\frac{6}{1 + x_k^2 + y_k^2}\right) \quad (3)$$

Use Eq. (4) to quantify sequence x,

$$d = floor(x\ \times\ 10^{14}) \quad (4)$$

Eq.(4) is used to quantify sequence y and obtain the sequence s.

$$A1 = reshape(d, P', Q') \quad (5)$$

$$A2 = reshape(s, P', Q') \quad (6)$$

4.3.2 Shuffling

Step 1:- Perform column indexing and shuffling on $img1(p, q)$ and $A1(p, q)$ with the use of function $sortrows(\bullet)$. The function $sortrows(\bullet)$ performs index sorting such as ascending order of $\bullet$ sequence. Fig. 4.3 shows the example of column indexing and shuffling.

Step 2:- If p is equal to P', if not repeat Step1. Else, when $p = P'$, the column indexing and shuffling is completed and image P_{e1} is obtained.

Step 3:- Perform row indexing and shuffling on P_{e1} and $A2(p, q)$, one by one with the function $sortrows(\bullet)$. Fig. 4.4 shows the example of row indexing and shuffling

Step 4:- If q is equal to Q', if not repeat Step3. Else, when $q = Q'$, the row indexing and shuffling is completed and image P_{e2} is obtained.

Step 5:- Repeat Step1~4 for other three blocks of plain image such as img2, img3, img4.

Step 6:- Combine all the scrambled blocks of plain image to a cipher image S which has same size $P\ X\ Q$. Fig 4.5 shows the flowchart of confusion stage.

15	12	7	11
14	2	13	10
16	5	3	17
9	8	4	6

img1

7	13	16	6
10	8	12	5
17	15	2	14
4	9	11	3

A1

9	2	3	6
15	8	4	10
14	12	13	11
16	5	7	17

P_{e1}

Fig 4.3 Example of Column Shuffling

9	2	3	6
15	8	4	10
14	12	13	11
16	5	7	17

P_{e1}

7	13	16	6
10	8	12	5
17	15	2	14
4	9	11	3

A2

6	9	2	3
10	8	15	4
13	11	12	14
17	16	5	7

P_{e2}

Fig 4.4 Example of Row Shuffling

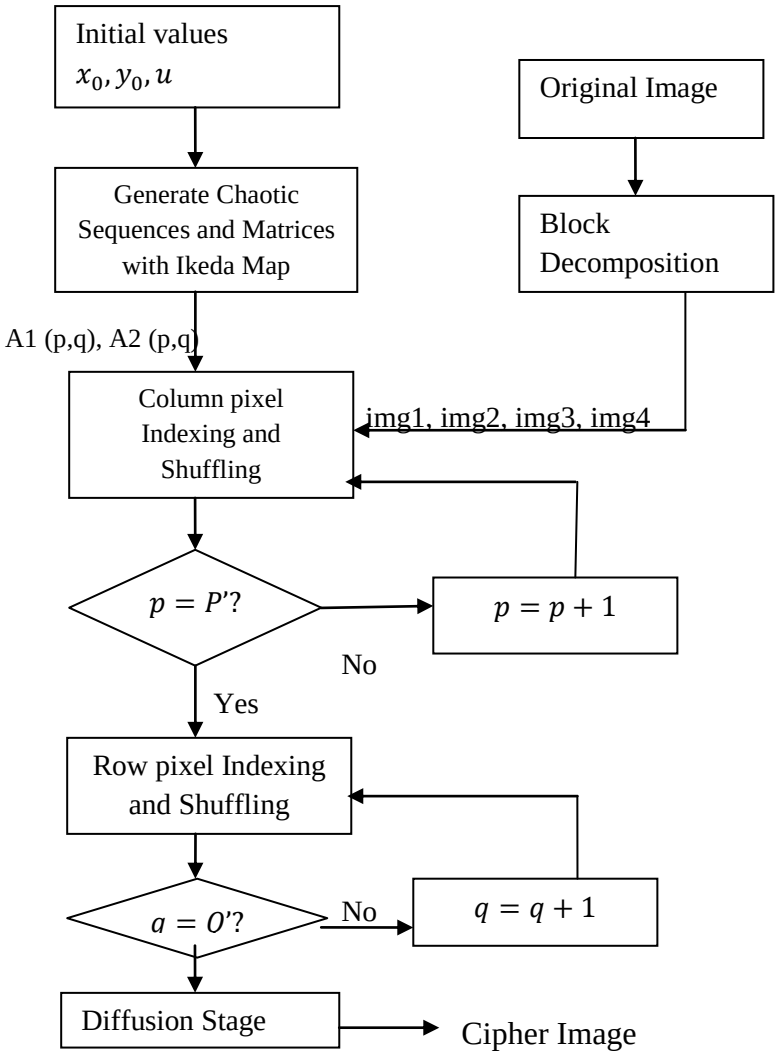


Fig 4.5 Flowchart of Confusion Stage

4.3.3 Diffusion Phase

Step 1:- Convert the cipher image into a sequence h , having the size $n = P\ X\ Q$.

Step 2:- Create chaotic sequence with Logistic map with two initial values z_0, r. Use Eq.(7) to generate chaotic sequence n times.

The Logistic map equation is given as follows:-

$z_{k+1} = rz_k(1 - z_k)\ , r \in (0,4), z_k \in (0,1)$ (7)

Step 3:- The Eq. (8) is used to quantify the chaotic sequence z.

$k = \ mod(floor(z \times\ 10^{14}\ ), 256)$ (8)

Step 4:- Except the first element, add the elements in sequence h.

$sum = \sum_{i=2}^{T} h(i)$ (9)

Step 5:- Set s_0 with the Eq. (10):-

$$s_0 = mod(sum, 256) \quad (10)$$

Step 6:- Encrypt the first element of sequence h by Eq. (11). The first encrypted value is used to change other pixel values in image. So, with the first value, the cipher image gets widely changed.

$$h(1)=s_0 \oplus h(1) \oplus z(1) \quad (11)$$

Step 7:- From $i = 2\ to\ n-1$, repeat Step 8~9.

Step 8:- Calculate dynamic indexes pt_1 and pt_2, which are used for encrypting i^{th} element in h.

$$pt_1 = floor\left(\frac{mod\left(\left(h(i-1)+z(i)\right), 256\right)}{256} \times (i-1)\right) + 1 \quad (12)$$

$$pt_2 = floor\left(\frac{mod\left(\left(h(i-1)+z(i)\right), 256\right)}{255} \times (T-i-1)\right) + i + 1 \quad (13)$$

Step 9:- Since for different plain image, the first encoded value and dynamic indexes pt_1 and pt_2 will be distinct. This leads to different i^{th} encrypted value for a plain image.

$$h(i) = h(i) \oplus z(i) \oplus h(pt_1) \oplus h(pt_2) \quad (14)$$

Step 10:- Set $i = n$, utilize Eq. (12) to find index pt_1 and encode the last element by Eq.(13)

$$h(i) = h(i) \oplus z(i) \oplus h(pt_1) \quad (15)$$

Step 11:- Transform the sequence h into a cipher image R. Fig 4.6 shows the flowchart of diffusion stage.

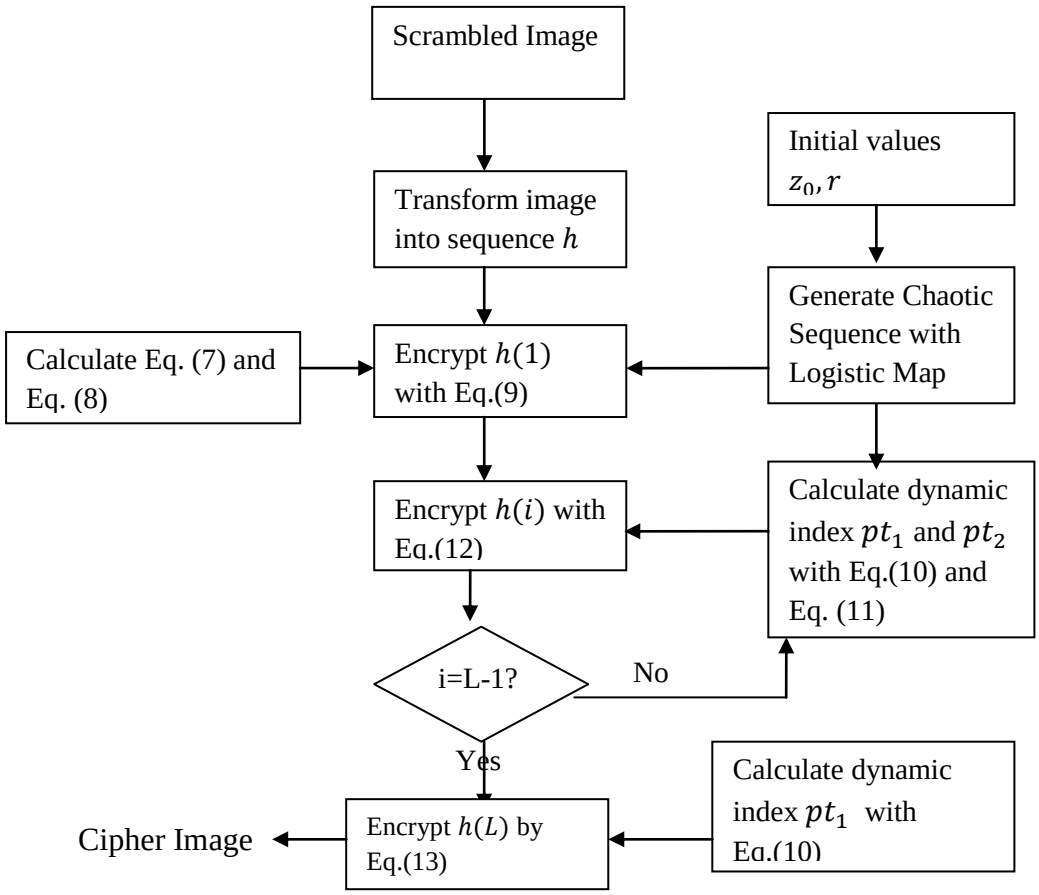


Fig 4.6: Flowchart of diffusion phase

4.4 Image Decryption Algorithm using chaotic sequences and flipping

Turn around the steps of image encryption algorithm to create the original image. Since bitwise exclusive-or operation, flipping are reversible process so scrambled image can be changed into original image.

4.5 Image Decryption Algorithm of pixel shuffling and diffusion phase

Step 1:- Convert the cipher image into the sequence h.

Step 2:- Generate Chaotic Sequence with Logistic Map having keys z_0, r.

Step 3:- Calculate index pt_1 with Eq.(12). Decrypt the last element of sequence such as $h(L)$ with Eq.(13).

Step 4:- Repeat Step 4 from $i = L - 1\ to\ 2$.

Step 5:- Calculate index pt_1 and pt_2 by Eq.(12) and Eq.(13). Decrypt the element $h(i)$ with Eq. (12).

Step 6:- Add the elements in sequence h except the first one.

Step 7:- Calculate s_0 to decode the first element of sequence h.

Step 8:- Convert the sequence h into image $n = P \times Q$.

Step 9:- Divide the resultant image into four blocks img1, img2, img3, img4.

Step 10:- Repeat Step 2.2.1 and Step 2.2.2 to generate the unique chaotic sequence and matrix $A1$ and $A2$.

Step 11:- Generate a sequence matrix D having size same as img1. Fig. 4.7 shows the sequence matrix D.

Step 12:- In order to obtain recovery matrix D_{0r} , perform row indexing and shuffling on sequence matrix D and $A2$ with the function $sortrows(\bullet)$.

Step 13:- Perform row indexing and shuffling on P_{e2} and D_{0r} with the function $sortrows(\bullet)$.

Step 14:- If $p \neq P'$, repeat step 13. Else when $p = P'$, the image P_{e2} is obtained.

Step 15:- Generate a sequence matrix $D1$ having size same as img2. Fig. 4.8 shows the sequence matrix $D1$.

Step 16:-In order to get restoration matrix D_{1r}, perform column indexing and shuffling on sequence matrix D_1 and $A1$ with the function $sortrows(\bullet)$.

Step 17:- Perform column indexing and shuffling on P_{e1} and D_{1r} with the use of function $sortrows(\bullet)$.

Step 18:- If $q \neq Q'$, repeat step 17. Else when $q = Q'$, the image img1 is obtained.

Step 19:- Repeat Step 11 to 18 for image blocks img2, img3 img4.

Step 20:- Combine all the blocks img1, img2, img3, img4 to obtain the original image.

1	2	3	4
1	2	3	4
1	2	3	4
1	2	3	4

Fig. 4.7 Sequence Matrix D

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

Fig 4.8 Sequence Matrix D1

Chapter 5

Experimental Observation

5.1 Key Space Analysis

Key space refers to necessity of keys to encode a picture. In chaotic sequence and flipping algorithm, the keys are μ, x_0 while in pixel shuffling and diffusion algorithm, Ikeda chaotic map and logistic map is used to create a chaotic sequence which is used to encrypt an image. In this paper, the keys used are x_0, y_0, z_0, μ, u. The key space of each of initial value x_0, y_0, z_0 is 10^{16}. The key space of each of μ, u is 10^{14}. So, the total number of keys required in pixel shuffling and diffusion algorithm to encrypt an image are 10^{76}. This leads that pixel shuffling and diffusion proposed algorithm has large key space rather than chaotic sequence and flipping algorithm.

5.2 Histogram Analysis

Number of pixel values in range [0,255] in graph represents Histogram. In order to resist attacks, encrypted image's histogram should be uniformly distributed. It can be seen from in the chaotic sequence and flipping algorithm, histogram is not uniformly distributed while in the pixel shuffling and diffusion algorithm, histogram is uniformly distributed. Fig.5.1 and Fig. 5.2 shows Elaine image and its histogram. Fig 5.3 and Fig 5.4 shows encrypted image and its histogram of pixel shuffling and diffusion algorithm. Fig 5.5 and Fig 5.6 shows encrypted image and its histogram of chaotic sequence and flipping algorithm. It can be concluded that the histogram of original image and decrypted image are same in case of pixel shuffling and diffusion algorithm.

Fig. 5.1 Original Image

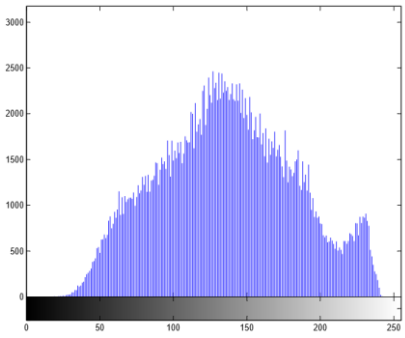


Fig 5.2Histogram of Original Image

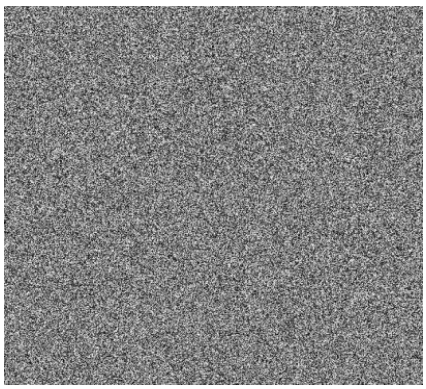


Fig 5.3 Encrypted Image with pixel shuffling and diffusion algorithm

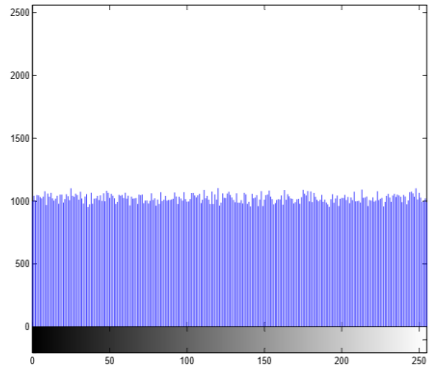


Fig 5.4 Encrypted Image's Histogram of pixel shuffling and diffusion algorithm

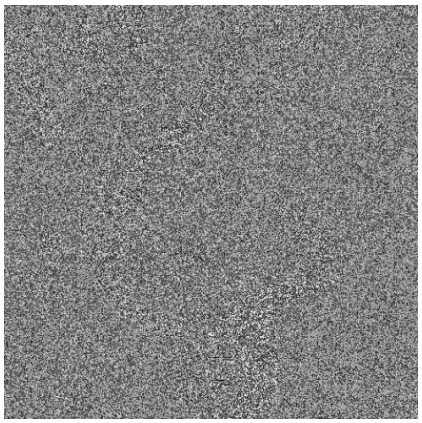


Fig 5.5 Encrypted Image with chaotic sequence and flipping algorithm

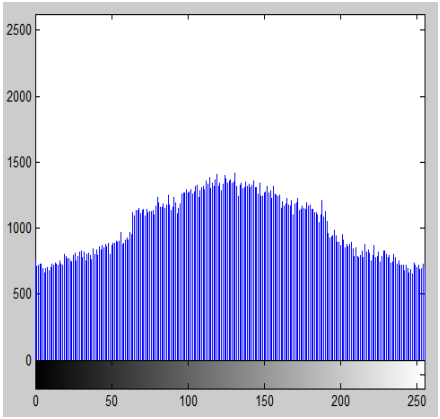


Fig 5.6 Encrypted Image's Histogram of chaotic sequence and flipping algorithm

5.3 Entropy Analysis

The formula of information entropy is given as follows:-

$$E(m) = \sum_{i=0}^{2^s-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{16}$$

where m_i is the symbol, $p(m_i)$ is the probability of message and s is the number of bits required to represent message. For uniformly distributed encrypted image, entropy should be near to 8. Table.5.1 represents Elaine image's entropy and Cipher image's entropy with chaotic sequence and flipping algorithm and pixel shuffling and diffusion algorithm. Cipher image's entropy of pixel shuffling and diffusion algorithm is near to 8 while with the chaotic sequence and flipping algorithm, it is 7.9639. This can be concluded that pixel shuffling and

diffusion algorithm gives better entropy than the chaotic sequence and flipping algorithm.

Table 5.1: Information Entropy

Image	**Entropy**
Original Image	7.5060
Chaotic Sequence and flipping Algorithm	7.9639
Pixel shuffling and diffusion Algorithm	7.9993

5.4 Key Sensitivity Analysis

Both algorithms are highly sensitive to initial keys. With minor change in initial key, cipher image cannot be decrypted to original one. In case of pixel shuffling and diffusion algorithm, the original image is encrypted with keys 0.01234567891236, 3.987654327, 0.6754567898, 0.9876674567, 1.564321976. With the slight difference in these keys 0.01234567891237, 3.987654328, 0.6754567899, 0.9876674568, 1.564321977, the cipher image cannot be decrypted to original one. In case of chaotic sequence and flipping algorithm, the image is encrypted with keys 0.01234567891236, 3.987654327 and decrypted with 0.01234567891237, 3.987654328 keys. In Figure 5.7 shows Elaine image. Figure 5.8 shows the cipher image and Figure 5.9 shows the decrypted image with the wrong keys in case of pixel shuffling and diffusion algorithm. Fig 5.10 shows the cipher image and Fig 5.11 shows the decrypted image with the wrong keys in case of chaotic sequence and flipping algorithm.

Fig 5.7 Elaine Image

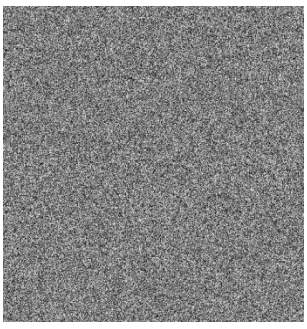


Fig 5.8 Encrypted Image with second algorithm

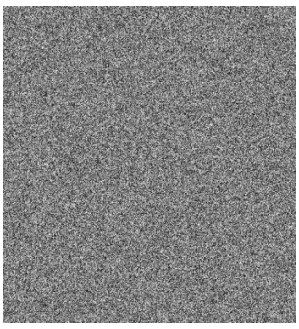


Fig 5.9 Decrypted Image with incorrect keys in second algorithm

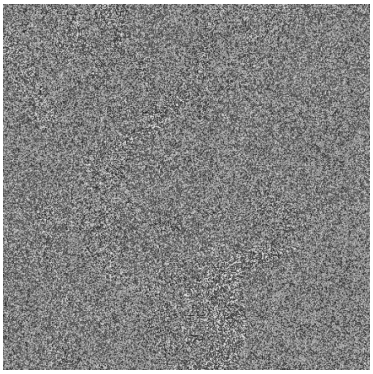


Fig 5.10 Encrypted Image with chaotic sequence and flipping algorithm

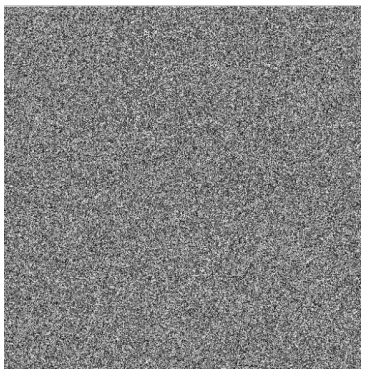


Fig 5.11 Decrypted Image with incorrect keys in chaotic sequence and flipping algorithm

5.5 NPCR and UACI

With the small modification in original image, the cipher image should get widely changed to resist differential attacks. The NPCR (number of pixels changed rate) and UACI (unified average changing intensity) are two factors which can used to test the resistance against differential attacks. The NPCR and UACI can be calculated with the following formula:-

$$NPCR = \sum_{p=1}^{M}\sum_{q=1}^{N}\frac{D(p,q)}{M \times N} \times 100\% \quad (17)$$

$$UACI = \sum_{p=1}^{M}\sum_{q=1}^{N}\frac{C_1(p,q) - C_2(p,q)}{M \times N \times 255} \times 100\% \quad (18)$$

where C_1 is the encrypted image produced by encoding the plain image and C_2 is the cipher image produced by changing one pixel in the plain image. $D(p,q)$ can be calculated with the formula:-

$$D(p,q) = \begin{cases} 0 \; if \; C_1(p,q) = C_2(p,q) \\ 1 \; if \; C_1(p,q) \neq C_2(p,q) \end{cases} \quad (19)$$

With the change in one bit in original image, the cipher image is completely changed. Table 5.2 shows the results of NPCR and UACI with both algorithms. With the result of NPCR and UACI, it can be seen that pixel shuffling and diffusion algorithm is secure against differential attacks but the chaotic sequence and flipping algorithm cannot resist against attacks.

Table 5.2: NPCR and UACI

Algorithm	NPCR	UACI
Chaotic sequence and flipping algorithm	38.14%	50.86%
Pixel shuffling and diffusion	99.61%	33.46%

5.6 Correlation Coefficient Analysis

Pixels of original image are highly correlated. A good encryption algorithm should decrease the correlation coefficient between the pixels of an image. 3000 pairs of adjacent pixels of an image has been chosen in vertical, diagonal and horizontal to compare and analyze the correlation between adjacent pixels of original image and cipher image. Correlation Coefficient can be calculated with formula given as:-

$$r_{pq} = cov(p,q)/\sqrt{D(p)D(q)} \tag{20}$$

$$E(p) = \frac{1}{R}\sum_{i=1}^{R} p_i \tag{21}$$

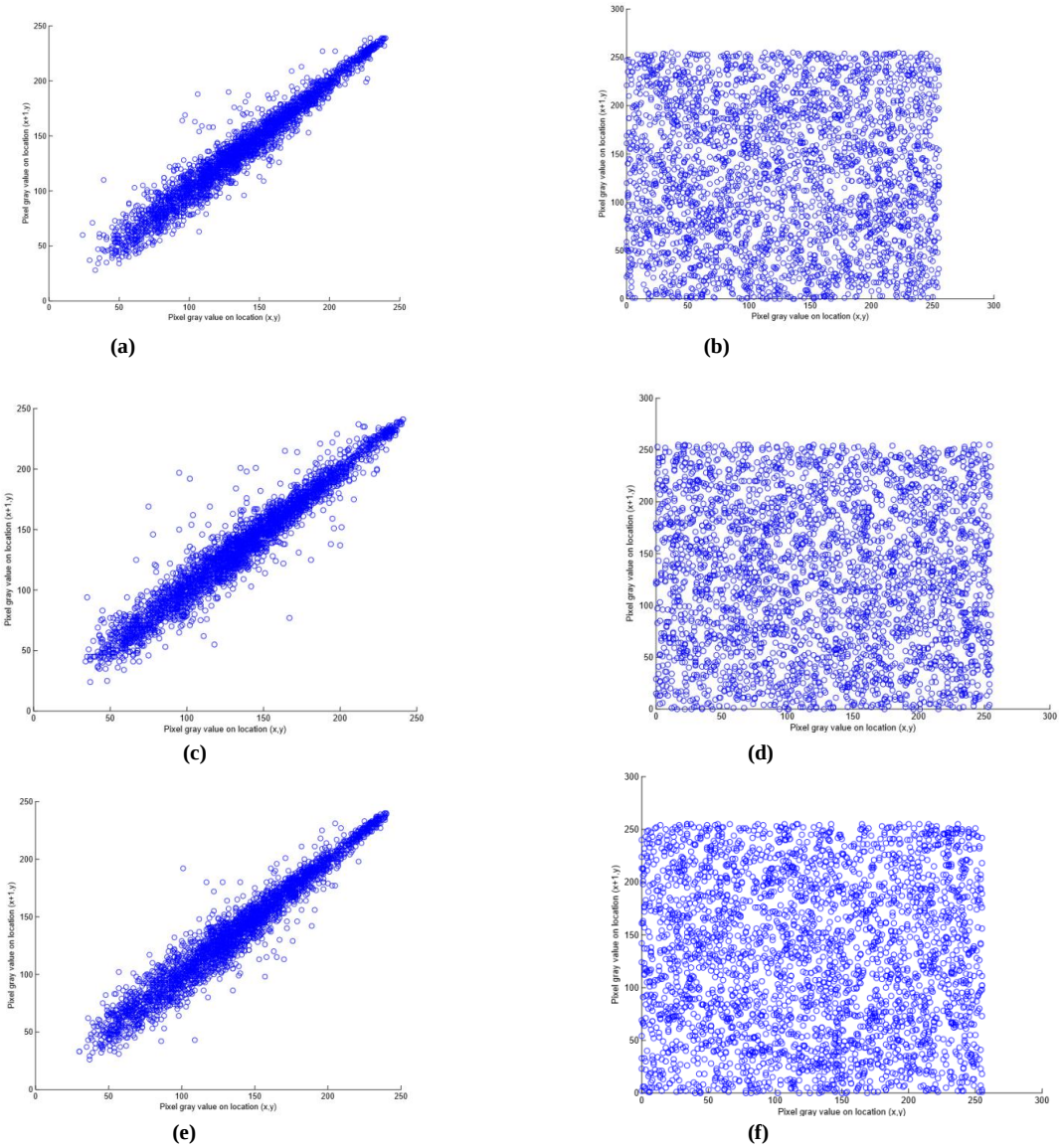
$$D(p) = \frac{1}{R}\sum_{i=1}^{R} (p_i - E(p))^2 \tag{22}$$

$$cov(p,q) = \frac{1}{R}\sum_{i=1}^{R} \big(p_i - E(p)\big)\big(q_i - E(q)\big) \tag{23}$$

where p, q are pixel value of an image. R is the summation of all pixels of an image. Fig.5.12 shows the correlation plot of two adjacent pixels of an image in vertical, diagonal and horizontal direction before encryption and after encryption in case of pixel shuffling and diffusion algorithm. Table 5.3 shows the correlation coefficient in all the three directions of chaotic sequence and flipping and pixel shuffling and diffusion algorithm. It proves that two adjacent pixels of an image after encryption have low correlation.

Table 5.3:Correlation Coefficient

Image	Vertical	Diagonal	Horizontal
Elaine Image	0.9769	0.9731	0.9738
Chaotic sequence and flipping Algorithm	-0.0150	-0.0062	0.0046
Pixel shuffling and diffusion Algorithm	-0.0073	0.0012	-0.0129



(a) **(b)** **(c)** **(d)** **(e)** **(f)**

Fig.5.12 Correlation Plot of pixel shuffling and diffusion algorithm(a-b) Vertical Correlation of Elaine Image and Encrypted Image (c-d)Diagonal Correlation of Elaine Image and Encrypted Image(e-f) Horizontal Correlation of Elaine Image and Encrypted Image

Chapter 6
Conclusion and Future Scope

6.1 Conclusion

To securely transfer the data over the internet with the immense growth of multimedia technology, techniques are required. Encryption is among of this technique that securely transfers the images. Many traditional encryption techniques have been used to secure the data transferred over the internet such as AES, DES and RSA algorithm. But, it is easy to decipher the traditional encryption algorithm because conventional encryption algorithm encrypts the image by considering the image as text data. Traditional encryption algorithms are complex to use, time consuming and easy to crack. So, an algorithm of image encryption is proposed which encrypts the image by changing the pixel positions as well as pixel values such as satisfy the confusion and diffusion property. But while transmitting the image over the internet, hackers attack the image by some technique. So, to enhance the security of algorithm, another image encryption algorithm is proposed which involves scrambling of blocks and diffusion phase dynamically. This algorithm divides the image into blocks. Each block of image is scrambled with the chaotic sequences by performing row shuffling and column shuffling. All the scrambled blocks of image combined to give cipher image. The pixels of scrambled image are diffused with dynamic index based diffusion. The dynamic index is generated for each pixel of scrambled image. A comparative study on both algorithms shows that second algorithm is more secure, can resist against attacks and is widely changed after the encryption than first algorithm.

6.2 Future Scope

In this research work, two new encryption techniques are proposed. The pixel shuffling and diffusion algorithm is better than chaotic sequence and flipping algorithm as it can defeat attacks by attackers and cipher image is widely changed after encryption. But the pixel shuffling and diffusion algorithm can be further improved:-

- The pixel shuffling and diffusion algorithm can be further enhanced for 3D images.

- The chaotic map can be changed such that which provides more chaotic behaviour.

REFERENCES

[1] Min Li, Tiang Liang, Yu-jie He," Arnold Transform Based Image Encryption Method", *Published by Atlantis Press,* 2012.

[2] Ping Ping, Yingchi Mao, Xin Lv, Feng Xu, Guoyan Xu, "An Image Encryption Algorithm Using Discrete Henon Map", *Proceedings of the International Conference on Information and Automation,* August 2015.

[3] LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin, "Image Encryption Algorithm Based on Chaos Theory and Sorting Transformation", *International Journal of Computer Science and Network Security,* 2008 (8),pp.64-68.

[4] Guodong Ye, "Image Scrambling encryption algorithm of pixel bit based on chaos map", *Pattern Recognition Letters,* 2010 (31), pp.347-354.

[5] Wang Yanling,"Image Encryption Method Based on Chaotic Sequences and Mapping", *First International Workshop on Education Technology and Computer Science,* 2009,pp 453-457.

[6] M.Y. Mohamed Parvees, J. Abdul Samath, I. Kaspar Raj, B. Parameswaran Bose, "A Colour Byte Encryption Technique for Efficient Image Encryption Based on Combined Chaotic Map", *International Conference on Electrical, Electronics and Optimization Techniques(ICEEOT),*2016,pp 1067-1072.

[7] Lingling Wu, Jianwei Zhang, Weitao Deng, Dongyan He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm", *The 1st International Conference on Information Science and Engineering,* 2009, pp 1164-1167.

[8] Liu Huiying, Xu Caiyun, Kong jun, Du Ying, "A novel secure arithmetic image coding algorithm based on Two-dimension Generalized Logistic Mapping", *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control,* 2015,pp 671-674.

[9] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on 3D chaotic map ", *Commun Nonlinear Sci Numer Simulat,* 2012 (17),pp 2943-2959.

[10] Yang Zou, Xialon Tian, Shaowei Xia, Yali Song, "A Novel Encryption Algorithm Based On Sudoku Puzzle",*4th International Congress on Image and Signal Processing,* 2011,pp 737-740.

[11] X Y Yu, J Zhang, H E Ren, G S Xu, X Y Luo,"Chaotic Image Encryption Algorithm Based on S-DES", *International Symposium on Instrumentation Science and Technology,* 2006 (48),pp 349-353.

[12] Liang Zhao, Avishek Adhikari, Di Xiao, Kouichi Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption", *Commun Nonlinear Sci Numer Simulat,* 2012 (17),pp 3303-3327.

[13] Xiuli Chai, Zhihua Gan, Yiran Chen, Yushu Zhang, "A visually secure encryption scheme based on compressive sensing", *Signal Processing* , 2017(134), pp 35-51.

[14] Lu Xu, Xu Gou, Zhi Li, Jian Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion", *Optics and Lasers in Engineering,* 2017(91),pp 41-52.

[15] Xingyuan Wang, Dapeng Luan, "A novel image encryption algorithm using chaos and reversible cellular automata", *Commun Nonlinear Sci Numer Simulat,* 2013(18),pp 3075-3085.

[16] Omid Mirzaei, Mahdi Yaghoobi, Hassan Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos", *Nonlinear Dyn,* 2012(67), pp 557-566.

[17] Ana Cristina Dascalesu, Radu Eugen Boriga, "A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling", *Nonlinear Dyn,* 2013(74), pp 307-318.

[18] C.K. Huang, C.W. Liao, S.L. Hsu, Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", *Telecommun Syst,* 2013(52), pp 563-571.

[19] Rong-Jian Chen, Yi-Te Lai, Jui-Lin Lai, "Image Encrypted System Using Scan Patterns and 2-D Cellular Automata", *The 2004 IEEE Asia-Pacific Conference on Circuits and Systems,*2009, pp 6-9.

[20] Ruisong Ye, Huiliang Li ,"A Novel Image Scrambling and Watermarking Scheme Based on Cellular Automata", *International Symposium on Electronic Commerce and Security,* 2008, pp 938-941.

[21] Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati-Q, Zohreh souzanchi-k, "An Image Encryption System by Indefinite Cellular Automata and Chaos", *2nd*

International Conference on Signal Processing Systems(ICSPS), 2010(3), pp 23-27.

[22] WEI Qin, LIU Quan , LI Fen, "A Novel Algorithm for Image Encryption Based on Weighted and p-interval CA", *Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science,* 2010, pp 440-444.

[23] Abdel Latif Abu Dalhoum, Basel A. Mahafzah, Aiman Ayyal Awwad, Ibrahim Aldamari, Alfonso Ortega, Manuel Alfonseca, "Digital Image Scrambling Using 2D Cellular Automata", *14th International Symposium on Multimedia,* 2012, pp 28-36.

[24] LOU Yuefang, HU Tianqiao, "A Novel Image Scrambling System Based on Cellular Automata and Improved Chaotic System", *5th International Congress on Image and Signal Processing (CISP),* 2012, pp 1139-1142.

[25] Chuan Peng, Yuanxiang Li, "A New Algorithm for Image Encryption based on Couple Chaotic System and Cellular Automata", *International Conference on Mechatronic Sciences, Electric Engineering and Computer(MEC),* 2013, pp 1645-1648.

[26] Subrata Nandi, Satyabrata Roy, Siddhartha Nath, Sayan Chakraborty, Wahiba Ben Abdessalem Karaa, Nilanjan Dey, "1-D Group Cellular Automata Based Image Encryption Technique", *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),*2014, pp 521-526.

[27] Samaneh Zamani, Mahdi Javanmard, Nima Jafarzadeh, Mostafa Zamani, "A Novel Image Encryption Scheme Based on Hyper Chaotic Systems and Fuzzy Cellular Automata", *22nd Iranian Conference on Electrical Engineering,* 2014, pp 1136-1141.

[28] Ping Ping, Xin Lv, Yingchi Mao, Rongchi Qi, "Image Scrambling based on Life-Like Cellular Automata", *The 10th International Conference on Computer Science & Education,*2015, pp 345-348.

[29] Ping Ping, Feng Xu, Md Shaiful Islam Babu, Xin Lv, Yingchi Mao, "Image Scrambling Scheme based on Bit-Level Permutation and 2-D Cellular Automata", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing,* 2015, pp 413-416.

[30] Abdel Latif Abu Dalhoum, Alia Madain, “Digital image scrambling based on elementary cellular automata”, *Multimedia Tools Appl,* 2016(75),pp 17019-17034.

[31] Xingyuan Wang, Dahai Xu, “A novel image encryption scheme using chaos and Langton’s Ant cellular automata”, *Nonlinear Dyn,* 2015(79), pp 2449-2456.

[32] Ye GD, ”Image scrambling encryption algorithm of pixel bit based on chaos map”, Pattern Recognit Lett, 2010(31),pp 347-354.

[33] “The process of asymmetric encryption”, https://msdn.microsoft.com/en-us/library/ ff650720.aspx.

[34] “The process of symmetric encryption”, https://msdn.microsoft.com/en-us/library/ ff650720.aspx

[35] “VonNeumann Neighborhood”, http://mathworld.wolfram.com/VonNeumann Neighborhood.html

[36] “Moore Neighborhood”, http://mathworld.wolfram.com/MooreNeighborhood .html

VIDEO PRESENTATION

- https://youtu.be/5VPbU4FjhN8

LIST OF PUBLICATIONS

- Priyanka Takkar, Ashish Girdhar, Dr. V. P. Singh, "Image Encryption Algorithm Using Chaotic Sequence and Flipping", *International Conference on Computing Communication and Automation*, 2017. **(Accepted)**
- Priyanka Takkar, Ashish Girdhar, Dr. V. P. Singh, "A Pixel Shuffling and Diffusion Based Image Encryption Algorithm", *Signal Processing*, 2017. **(Communicated)**

Priyanka_14-07-2017

by Priyanka Takkar

FILE	PRIYANKA_THESIS.PDF (1.7M)		
TIME SUBMITTED	14-JUL-2017 04:10PM	WORD COUNT	8797
SUBMISSION ID	830802140	CHARACTER COUNT	46809

Chapter 1

Introduction

A lot of data is communicated over the internet with the immense growth of multimedia technology. Information transmitted over the internet can be edited or replicated by unauthorized users. Because of its broad sharing, security of data is an incredible research zone. Data transmitting over the web is of various sorts, for example, data, sound, image, video and so forth. Image is better than data regarding more content, redundancy and intensity value's frequency. There is prerequisite of continuous image encryption calculations to scramble the image amid transmission.

1.1 Need of Security

Information security is required to carry out the following tasks:-

- To keep the information protected from unauthorized users.
- To keep the information protected from being altered or duplicated from unauthorized users.
- To securely transfer the information to the authenticated users.

1.2 Image Encryption

Encryption is a procedure to change over original message, for example, plain image into cipher image, for example, its scrambled shape. Encryption algorithms utilizes key to encode or unscramble the information. Encryption and Decryption of information is performed utilizing key and calculation. These days, data security is getting to be noticeably imperative in information storage and transmission. Images are generally utilized as a part of various procedures. In this manner, security of image information from unapproved clients is required. Image encryption assumes an imperative part in the field of data covering up. Image encryption changes the data into indistinguishable shape so no unapproved clients approach original data or some other sort of data conveyed over the web.

Image encryption is a strategy that changes digital image into disarranged one to make it outwardly confused. The purpose behind the image encryption is to protect the original image's content. There are two stages in image encryption- Confusion

stage and diffusion stage. Confusion phase realigns the pixel value of an image while diffusion phase alters the pixel value of an image.

1.2.1 Types of Encryption

There are two sorts of encryption: - one is Symmetric key encryption and another is asymmetric key encryption. There two are examined as takes after:-

- **Asymmetric key Encryption**

Asymmetric key encryption scrambles the information at the sending end and decodes the information at the receiving end with distinctive keys. It scrambles the information with the public key while decodes the information with private key. Private key is kept secured while public key is shared. Fig 1.1 demonstrates the asymmetric key encryption.

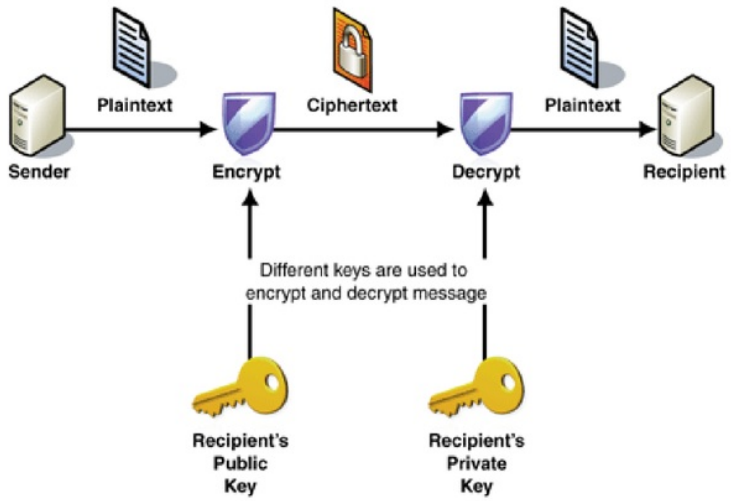


Fig 1.1 Asymmetric Encryption Technique[33]

- **Symmetric key Encryption**

Symmetric key encryption encrypts the data at the sending end and decrypts the data at receiving end with the same key. It is fast method than asymmetric key encryption. If key is random then encryption method performs better. We can also say Symmetric key encryption is known as Scrambling. Fig 1.2 shows the symmetric key encryption.

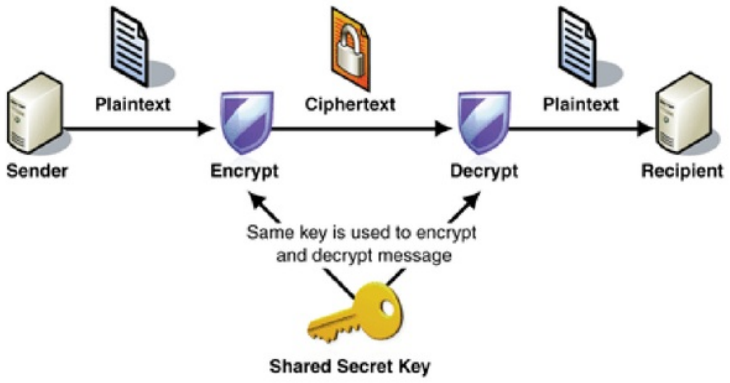


Fig 1.2 Symmetric Encryption Technique[34]

1.3 Security Attacks

These are the types of attacks occurred on image encryption scheme to get the information:-

1.3.1 Known plaintext Attack

A known plaintext attack is type of attack when hacker attacks on both plaintext and ciphertext. This type of attack helps hackers to obtain secret keys.

1.3.2 Chosen plaintext Attack

A chosen plaintext attack is type of attack when hacker gets ciphertext for a random plaintext. The goal of this attack is to get information by lowering the security of information.

1.3.3 Ciphertext-only Attack

A Ciphertext-only attack or known ciphertext attack is a type of attack when hacker attacks only have information of ciphertext. Hacker doesn't have any information regarding to plaintext. But in practical, hacker has some information like in which language plaintext is written.

1.3.4 Chosen ciphertext Attack

A chosen ciphertext attack is type of attack when hacker decrypts the cipher text and collects the information. This information is then used to crack the secret key.

1.4 Security Services

1.4.1 Data Confidentiality

Confidentiality is to keep the information secure from unauthorized users. It also leads to the procedures to prevent the disclosure of confidential data from unauthorized users. Encryption is the method of protecting information. Encryption ensures that only authenticated people can read the information such as people who know the secret key. Encryption is widely used in most of the protocols. An example of confidentiality is security protocol such as SSL/TLS which ensures security. To ensure confidentiality, permission of file and access control is used to restrict access.

1.4.2 Data Integrity

To maintain the accuracy, consistency and reliable information leads to Data integrity. The process of protecting information from unauthorized users for being altered is known as integrity. Data should not be changed in communication and integrity ensures that data received is same to the original form. Only correct information is relevant. Checksums is applied with the data for the verification of data. To restore the affected data, Backup is available.

1.4.3 Data Availability

Availability refers to ensure that authorized users are able to get the information whenever they required. A very common attack is to deny the access to the information. With the help of DDoS attack, high profile websites have been blocked. The aim of DDoS attack is deny users to access the resources of website. With the help of Backup, data is available to unauthorized users. Redundancy is appropriate for sensitive information. It is also important to maintain the updated information that should be available to users.

1.4.4 Access Control

To limit and control the access to applications for users is Access Control. To achieve this, each entity who is trying to access is first authenticated in order to provide the access rights to individual. Restriction of access provided to every individual is known as Access control. Fig 1.3 shows CIA Triad.

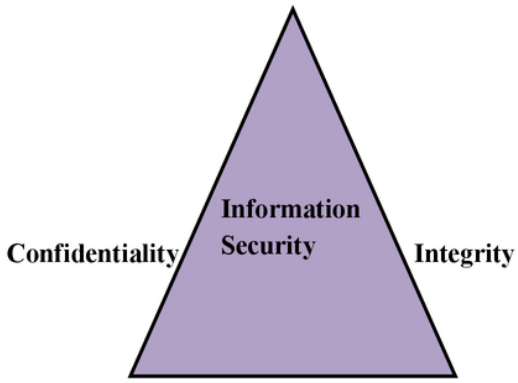


Fig 1.3 CIA Triad

1.5 Security Mechanisms

1.5.1 Encipherment

Encipherment refers to hiding or covering information. Encipherment leads to keep the information protected from unauthorized users. It helps to provide data confidentiality. Encipherment converts the plain text into cipher text.

1.5.2 Decipherment

Decipherment is the procedure to convert cipher text into plain text. Decipherment is performed at the receiver side. Encipherment and decipherment require the use of key and initialization variable, which is required for randomness of cipher text.

1.5.3 Data Integrity

Different schemes have been used to check the integrity of data. Check value is used to see whether the data integrity is preserved or not. The check value is send by the sender and receiver also creates its own check value and compares the both check values to check the integrity of the message.

1.5.4 Authentication Exchange

Digital signatures are bind to the document at the creation time. A digital signature is considered as an authentication. Key management mechanism is considered as another authentication as only users can access the data that has key.

1.5.5 Access Control

The keys or passwords can be used as access control methods to allow users to access data.

1.6 Merits of Encryption

1.6.1 Provides security

During the transmission of data, there is possibility of data being attacked. Encryption provides security as the encrypted form or ciphertext cannot be read by unauthorized users.

1.6.2 Maintains Integrity

Information is even pirated by unauthorized users. With the help of encryption algorithms, we are able to detect the information at the receiving end has been altered. This allows reacting for cyber attack.

1.6.3 Protects Privacy

Encryption is used to secure sensitive information. As there is lot of sensitive information for military, encryption is used to keep information protected from unauthorized users. This helps to ensure privacy.

1.6.4 Part of Compliance

Organizations that have people's personal information require strict compliance to secure that information. HIPAA, FIPS and other regulations used security methods such as encryption to keep the data secure.

1.6.5 Protects Data across Devices

Nowadays, smart phones are widely used and data transferring from one device to another device requires security. Encryption can protect data across devices even during transferring of data. Advanced security such as authentication also helps to detect unauthorized users.

1.7 Applications of Encryption

1.7.1 Steganography

Encryption can be applied to steganography. Steganography is technique of embedding secret message into cover media. Secret message is encrypted and then embedded to cover media and transmit over the internet.

1.7.2 Digital Watermarking

Advanced watermarking is utilized to give the legitimacy of an archive. Encoded credibility is hard to duplicate. Encryption keeps copyright from unapproved clients. With the encryption, it is hard to remove watermark.

1.7.3 Multipurpose Internet Mail Exchange (MIME)

MIME (Multipurpose Internet Mail Exchange) is utilized for encoding heterogeneous information sorts inside a single message. Messages are encoded utilizing base64, for example, encode non-content information with content information. MIME is utilized for encoding any content, pictures and applications.

1.7.4 Secure Electronic Transaction (SET)

SET (Secure Electronic Transaction) is convention created by Visa and MasterCard. It utilizes public key to guarantee secure installment.

1.8 Chaotic Map

Chaotic map is utilized to produce disordered sequences and these arrangements are then utilized as a part of image encryption. Chaotic map is much agreeable for image encryption because of its fundamental qualities. Chaotic map is subtype of non-direct dynamical frameworks. Chaotic map is broadly utilized in light of its properties, for example, deterministic, periodicity, ergodicity, non-linear, irregular behaviour. A minor change in the underlying estimations of confused framework prompts noteworthy change in the result.

Advantages of chaotic System:-

- Parameter of chaotic map and introductory condition is required to generate chaotic map.
- The chaotic succession will be enormously changed with the minor change in beginning condition.
- It generally creates same chaotic sequence with one beginning condition.
- To recover an original message, exact knowledge of initial conditions and system parameters are required.
- Due to highly sensitive nature of initial values and parameters, chaotic system is robustness and effectiveness.
- Chaotic system is deterministic.

1.9 Cellular Automata

Cell automata contain number of indistinguishable cells and cells are arranged in rectangular matrix in at least one measurement. Every one of the cells all the while refresh their cell states by applying move capacity with the end goal that as indicated by the predefined nearby control of association between the neighbours of the cell. Consider the information is the condition of the cell and neighbouring conditions of cell. A cellular automaton is widely used in image encryption due to its complex behaviour and generates useful operations. In terms of living space, cellular automata can be 1-D, 2-D, 3-D or higher dimensions.

The following categories of 1-D Cellular Automata:-

- Ordered Behaviour
- Periodic Behaviour
- Chaotic Behaviour
- Complex Behaviour

While ordered and periodic behaviour is predictable, chaotic behaviour is unpredictable and complex behaviour is somewhere in the move from periodic to chaotic and indicates complex conduct.

1.9.2 Types of cellular automata:-

(a) Uniform cellular automata

Same state move manage for every one of the cells of cell automata then those cell automata is known as uniform cell automata.

(b) Hybrid Cellular automata

Diverse state move govern for every one of the cells of cell automata then those cell automata is known as hybrid cell automata.

1.9.3 Boundary Conditions of Cellular Automata:-

Boundary condition is required in case of finite grids to determine which cell is left neighbour of furthest left cell and which cell is correct neighbour of furthest right cell.

There are three types of boundary conditions:-

- Periodic: - 1-D rows become circles such that their extraordinary cells wind up noticeably nearby each other.
- 2-D matrices progress toward becoming toroids with the end goal that their extraordinary furthest left segment will be neighbour to furthest right segment and best column will be neighbour to base line.
- Static: - Extreme cells are connected to permanent zero state cells.

1.9.4 Neighbourhood of Cellular Automata:-

- **1-D Cellular Automata**

In the event of 1-D cell automata, the cell itself, one cell to its quick left and another cell to its prompt right. For example, a b c

where ' a' is the cell itself, 'b' is immediate left neighbour of 'a' and 'c' is immediate right neighbour of 'a'.

- **2-D Cellular Automata**

There are two neighbourhood methods are used in case of 2-D cellular automata:-

(a) Vonneumann Neighborhood

The Von Neumann neighbourhood of range t is given as:-

$$NH(p_0, q_0, t) = [(p, q): |p - p_0| + |q - q_0| \leq t]$$

And number of cells in each neighbourhood is $2t(t + 1) + 1$. A range of one is commonly used leads to five neighbours. Fig 1.4 shows that Vonneumann neighbourhood.

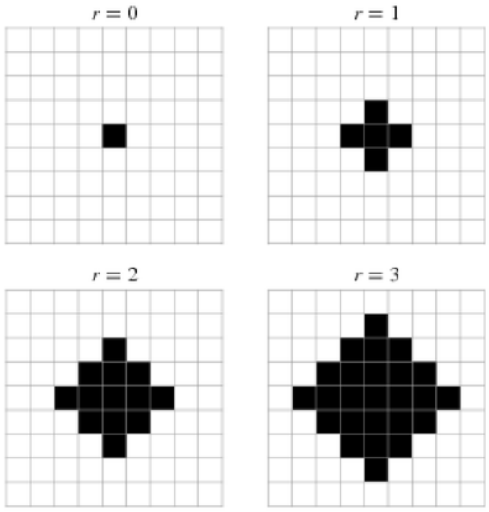


Fig 1.4 Vonneumann Neighbourhood [35]

(b) Moore Neighbourhood

The Moore neighbourhood of range t is given as:-

$$NH(p_0, q_0, t) = [(p, q): |p - p_0| \leq t, |q - q_0| \leq t]$$

And the number of cells in each neighbourhood is $(2t + 1)^2$. A range of one is commonly used leads to nine neighbours. Fig 1.5 shows the Moore neighbourhood.

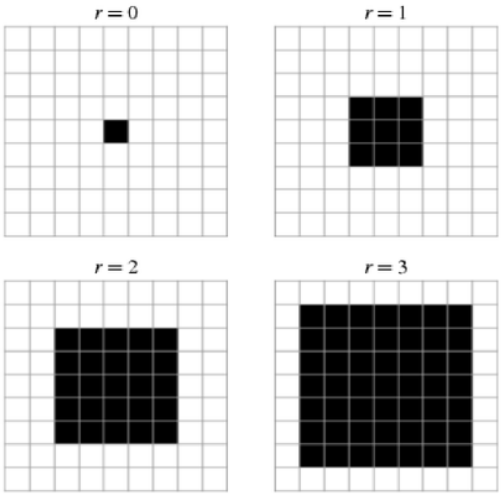


Fig 1.5 Moore Neighbourhood [36]

Chapter 2

Literature Survey

2.1 Related Work

To encrypt an image, many image encryption algorithms have been proposed by different researchers. Conventional scrambling change the pixel positions while total scrambling change the pixel positions as well as pixel values. Total scrambling is better than conventional scrambling because histogram is changed after total scrambling that leads to more secure but histogram is same in case of conventional scrambling. Different image scrambling techniques based on spatial domain, chaotic map and cellular automata have been discussed.

2.2 Image Scrambling based on spatial domain

Min Li et al. [1] proposed an algorithm which scrambles the non-square image by dividing the non-square image into different square regions. The traditional Arnold transform scrambles only square images. Each square region of image is scrambled different number of times to enhance the security of algorithm. It restores the image correctly with the keys which keep the image safe and algorithm has reliable transmission.

Due to periodicity of Arnold transformation, it is widely used. But a lot of time gets wasted to find its periodicity. Lingling Wu et al. [7] presented an improved anti-arnold based transformation which descrambles the image with the same iteration steps as with scrambling the image. With this algorithm, a lot of time get save to restore an image.

Ping Ping et al. [2] proposed an algorithm based on non-linear map known as Henon map. It is easy for attackers to discover the connection between plain image and cipher image which is scrambled with the linear map. The keys of this algorithm are the parameters of henon map and with the iteration of henon map, the image pixels are realigned. The non-linear property enhance the security of algorithm while the limitation of this algorithm it can be only applied to square images.

Yang Zou et al. [10] proposed an image scrambling algorithm in light of Sudoku Puzzle. Sudoku puzzle is a diversion where each incentive from 1-N seems just once in each line and section. Since in Sudoku puzzle, the pre-filled units and their area can be the key of the scrambling. The pre-filled units can be any number from 1-N and can find any place in the puzzle so it is elusive the right key to restore an image. With a specific end goal to upgrade the security of an algorithm, this algorithm scrambles the image both at pixel level and at bits level.

Xiuli Chai et al. [13] displayed an outwardly secure image encryption algorithm in light of compressive detecting. Change the plain image into coefficient grid utilizing DWT and afterward mixed by plain image crisscross way and after that encodes into compressed cipher image by compressive sensing. This cipher image is embedded over the carrier and after that get outwardly secure cipher image. This algorithm has high security. Size is same in both plain image and cipher image. This encryption technique has high affectability to the plain image. This algorithm can likewise overcome chosen-plaintext and known-plaintext attacks.

2.3 Image Scrambling based on chaotic map

LIU Xiangdong et al. [3] proposed an algorithm based on chaotic system and sorting transformation. With the sorting of chaotic sequences, the algorithm calculates permuting address codes. The complexity of this algorithm gets reduce as this algorithm does not require knowing probability density function of the disordered orbits ahead of time. This algorithm provides a high level security.

Guodong Ye [4] presented a novel algorithm based on chaotic system and with pixel bit. This paper uses a single chaos map which encrypts both position value and gray value. This method can be used directly to communicate the images over the internet. This method can be enhanced to high dimensional chaos map and applied to 3D images.

Wang Yangling [5] presented a method which scrambles the image with the chaotic sequences and mapping. First, chaotic sequence is generated with chaotic map. Each pixel of an image is altered by applying bit-exclusive or operation on pixel value with disordered sequences. Then, image mirror mapping is performed to get the

encrypted image. This calculation is simple and feasible, slow speed of encryption and impact of encryption is great and exceptionally secure.

M.Y. Mohamed Parvees et al. [6] presented an algorithm which has used two chaotic maps-Logistic and Ikeda Map. Logistic map is used to change the position of colour bytes while Ikeda map is used to alter the colour bytes value. The combined chaotic encryption algorithm can encrypts the image of any size. It is very difficult to crack this algorithm by unauthorized person as it uses both chaotic maps. Chaotic maps are implemented at different places which keep algorithm protected and secure.

Lu Huiying et al. [8] presented a novel arithmetic image coding algorithm based on 2D generalized logistic mapping. With the logistic chaotic map, two 2D chaotic sequences are generated according to the size of the image. Image is scrambled by sorting the chaotic sequence. Key stream is generated by optimizing the chaotic sequence, which is used to mask the image data. During the arithmetic coding process, the coding interval order is controlled by the chaotic sequence. This algorithm has high security and has good robustness.

A. Kanso et al. [9] presented a novel encryption algorithm which uses 3D chaotic map. This algorithm has three tenets rearranging, mixing and scrambling procedure of digital image. This algorithm overcomes different assaults, for example, differential, statistical and casuality assaults. Results demonstrate that this algorithm has great security and is effective.

Arnold cat map and Hilbert transformation can meet the demands of image encryption methods over the internet. Input binary flow of image can be encrypted by S-DES but with the few keys will bring risks. X Y Yu et al. [11] presented an image encryption method based on chaotic map and S-DES. By applying the sensitivity of logistic chaotic map, large quantities of key is generated and key is real-time.

Liang Zhao et al. [12] presented an algorithm which presents attacks- chosen-plaintext attack and chosen-ciphertext attack. A correlation is additionally made between these assaults and Li Lo assault [32] which was likewise proposed to original image encryption algorithm. These attacks have less computational complexity then Li Lo attack. An improved encryption scheme with the self

correlation is proposed to overcome the drawbacks of original image encryption method. This algorithm is highly secured than original one. This algorithm can be further improved for future work.

Lu Xu et al. [14] exhibited a novel image encryption algorithm which separates the image into blocks in vertical or horizontal directions. The logistic map is utilized to make swapping control tables. The swapping control table is utilized to swap the pixel in the present block or other blocks. To diffuse the pixels of cipher image, the diffusion index scheme is utilized. This algorithm can adequately vanquish known-plaintext and chosen-plaintext assaults. It can likewise be all around utilized for double image scrambling.

Xingyuan Wang et al. [15] proposed a novel image encryption algorithm which encrypts the image by combining chaotic mapping and reversible cellular automata (RCA). Intertwining logistic map is utilized to permute the pixel value of an image and also change the value of pixel. The cipher image is generated through reversible cellular automata after many generations on bit level. This algorithm has protection of information perfectly and also satisfied confusion and diffusion properties.

Omid Mirzaei et al. [16] presented an image encryption scheme which is based on total shuffling and parallel encryption algorithm. To confuse the pixels of an original image, two chaotic systems have been used. First, digital image is divided into different blocks and shuffle the position of each block. To encrypt each pixel in each of four blocks, different values are used. These values are:-values generated from chaotic sequence, pixel value in original image and pixel value obtained from another block. This algorithm is very fast, possesses high security and has large key space.

Ana Cristina Dascalesu et al. [17] presented a novel chaotic map based algorithm which generates random permutations for image scrambling by high-shift factor. With this algorithm, fixed points are less. The image is scrambled by random permutations with high move factor. This algorithm is efficient and encryption speed is fast. It can also be used for real-time scrambling.

C.K. Huang et al. [18] proposed an algorithm which encrypts the image by row shuffling, column shuffling and gray level encryption. This algorithm first shuffles

the pixels of the image by row shuffling. Then this cipher image is shuffled by column shuffling. To enhance the security of encryption, gray level encryption is implemented. This algorithm is highly secure and cipher image is greatly changed after encryption.

2.4 Image Scrambling based on cellular automata

Rong-Jian Chen et al. [19] presented an algorithm which encrypts the image by altering of the pixel position of an image and changing the pixel values of an image. Scan patterns produced by SCAN strategy is utilized to permute the pixel value of an image. Cell automata are utilized to alter the pixel value of an image. Because of CA property, this algorithm satisfies confusion and diffusion property. This algorithm has extensive number of keys and lossless.

Ruisong Ye et al. [20] presented a novel image scrambling and watermarking scheme based on cellular automata. The chaotic features of cellular automata are analyzed and compute the fractal box size of cellular automata. Digital image scrambling can be used first for the watermarking scheme. This algorithm is vigorous against assaults, for example, cropping, noising and compression.

Maryam Habibipour et al. [21] presented an image encryption algorithm which replaces the pixel values of an image by indefinite cellular automata and chaos theory. Based on chaotic sequence, cellular automata rules are defined and these rules are stored in private key. This algorithm has large key space, symmetric private key, diffusion, confusion and pixel value replacement.

WEI Qin et al. [22] presented an algorithm to encrypt an image based on weighted and p-interval CA. Generate the new matrix with two-dimension p-interval and weighted approach which includes optional parameters that gives large number of security keys. The encryption speed of this algorithm is fast.

Abdel Latif Abu Dalhoum et al. [23] presented an algorithm which scrambles the digital image using 2D cellular automata. This algorithm provides high security as it scramble pixel locations of an image using double scrambling-image is scrambled in both vertical directions and horizontal directions. If algorithm is known to attacker then even image cannot be decode. With the usage of GA cellular automata, the

speed of encryption is improved. This algorithm can scramble the image of any size and can encode colour image, grayscale image and binary image.

LOU Yuefang et al. [24] exhibit a novel image encryption algorithm which depends on 2-D cell automata and enhanced standard map. To upgrade the pseudo-randomness of the algorithm, chaotic sequences are used to decide the state move rules of every cell. With the standard map, the chaotic sequence is produced which is utilized to scramble the digital image. As per parallel computation and pseudorandom quality, the pixel values of an image are changed. This algorithm has substantial key space, profoundly secure and can oppose chosen plaintext assault. The cipher image has good diffusion property.

Chuan Peng et al. [25] proposed an algorithm for image encryption utilizing couple chaotic system and couple cell automata. The chaotic sequence is produced utilizing couple chaotic system which has bigger key space and more complex dynamic attributes than general chaotic system. To begin with, digital image is separated into symmetric parts and scramble the image utilizing couple chaotic system and after that encoded utilizing couple toggle cell automata. This algorithm has substantial key space and can oppose brute assault and differential assault

Subrata Nandi at al. [26] encrypts the image using 1-D group cellular automata. This algorithm is similar to symmetric key encryption. As group cellular automata possess cyclic nature, so it is easy for encode and decode. This algorithm is lossless scheme. It can also be applied to colour images.

Samaneh Zamani et al. [27] proposed an image encryption scheme utilizing hyper chaotic system and Fuzzy cell automata. Hyper chaotic system has complex dynamic attributes than chaotic system. To upgrade the security and speed of algorithm, four hyper chaotic system is utilized. Plain image is separated into four sections and each sub-image has its own hyper chaotic system. Pixels in two adjoining sub pictures are chosen to change their positions. In encryption stage, five 1-D Fuzzy cell automata is utilized. To take care of the issue of recursive principles in administer choosing process, two diverse encryption strategies are utilized for even and odd cells. This algorithm is profoundly secure, for example, confusion and diffusion property and touchy to little changes in the key.

Ping Ping et al. [28] scramble the image using life-like cellular automata. To obtain scrambling matrix, a life-like cellular automata with an initial configuration is keep running for a few generations. The different CA initial configurations are used to achieve good diffusion property. This algorithm effectively lowers the correlation coefficient and can resist noise attack.

Ping Ping et al. [29] proposed CA based image scrambling technique which permute image at gray level and alter the pixel position. Firstly change over the image into binary image. With the assistance of scrambling network created by 2-D cell automata, the binary image is permuted at bit-level. This algorithm gives higher security by changing the pixel position and pixel value of an image. This approach is powerful to known-plaintext assault and chosen-plaintext assault. This algorithm can be enhanced to digital image of any size.

Abdel Latif Abu Dalhoum et al. [30] convert the digital image into meaningless form for the security reasons. Cellular automata have lot of parameters that show complexity and each parameter is differing in terms of complexity and behaviour. This paper has used simple cellular automata instead of 2D cellular automata. The parameters that were tested in this algorithm- the number of generations effect on scrambling, boundary types-periodic and static, rules. This algorithm when compared to scrambling techniques with 2D cell automata gives comparable outcomes without redundancy and gives better outcomes with reiteration.

Xingyuan Wang et al. [31] presented a novel image encryption algorithm which uses Langton's Ant cellular automata to scramble the image. The thought is to combine 2D basic attributes of the image with "chessboard" and let the Langton's Ant creep on it. We can get the scrambled image with the result of each step of cellular automata. This algorithm is secure and resist to common attacks.

30

Chapter 3

Problem Statement and Objectives

3.1 Problem Statement

With the immense growth of multimedia technology, data is communicated over the internet. So, there is a requirement to secure the information communicated over the internet. There are lot of traditional encryption methods to secure the data transmitted over the internet such as AES, DES and RSA algorithm. As images contain lot of information rather than text, images are great carrier of information communicated over the internet. Traditional encryption techniques have many disadvantages such as encryption speed is slow, the singleness of secret key, structure complexity and also it is difficult to secure the images that contains lot of information with these algorithms.

Conventional algorithms have following disadvantages which it less efficient:-

- Traditional encryption scheme is good regarding to safety but not excellent and encryption's effect is not good. It is easy to decipher the traditional encryption algorithm because conventional encryption algorithm encrypts the image by considering the image as information and data stream. So, it is very easy to crack the encryption algorithm and actual information will be revealed. There is requirement of strict security because of confidential data. Hence, it does not secure the images transferred over the internet.
- Traditional encryption algorithm is expensive and time consuming.
- Traditional encryption algorithms are very complex to use and hence people use algorithm incorrectly. This could lead to fail to encrypt data when they wish to encrypt the data and encode the data when they do not require encrypting the data.

3.2 Thesis Objectives

Modern image encryption algorithms securely transmit the images over the internet.

The objective of thesis is:-

- To study the various encryption algorithms based on spatial domain, chaotic sequences.
- To propose a new algorithm based on chaotic sequences and flipping.
- To propose a new algorithm based on pixel shuffling and diffusion.
- Validate the proposed algorithm with the simulation results.

Chapter 4

Implementation

Because of absence of safety efforts, some encryption algorithms cannot encode the image safely. This leads to that some action to be taken to send the image to other end securely as it may contain confidential information. To resolve the above problem, image is scrambled to transfer from one end to other end instead of plain image. With the different scrambling techniques, image is scrambled at the sender side and descrambling is performed at the receiver side and then original image is retrieved.

4.1 Scrambling

Scrambling is a technique of converting original image into meaningless form so that it cannot appear originally. With the help of mathematical transformations, the positions of the pixel of an image are changed than their current position. In this way, we transfer encoded form of image over the internet rather than original image. Fig 4.1 shows scrambling and descrambling process of an image where symmetric encryption is used and at sender side and receiver side, same key is used.

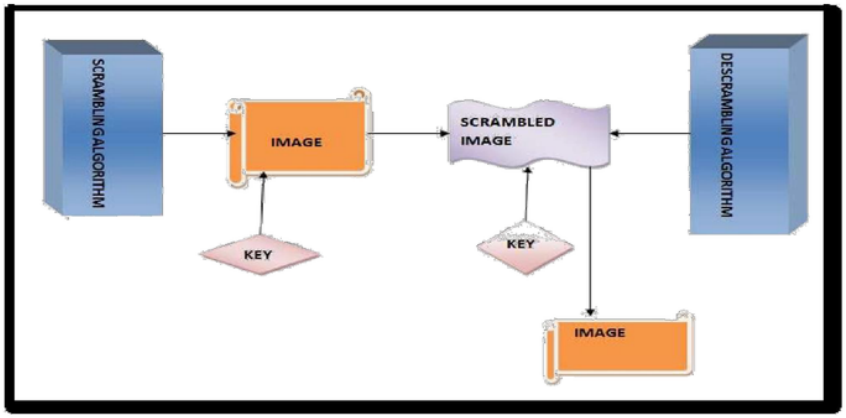


Fig 4.1 Process of scrambling and descrambling an image

4.2 Image Encryption Algorithm using chaotic sequences and flipping

Step1: Read the image R of size $U \times V$ where U is the width of the image and V is the height of the image. R (d, e) denote the image pixel value (d=1,2,....U ; e=1,2.....V).

Step 2: Generate a chaotic sequence p_r(r=1, 2...U× V) utilizing (1) where μ and x_0 are keys.

Step 3: Multiply chaotic sequence with 256 to make it regular numbers h_g(g=1, 2 ...U× V).

Step 4:Convert 1D h_g into 2D H(d, e)(d=1,2,...U ;e=1,2,....V).

Step 5: To alter the pixel value of an image, bit exclusive operation is performed on pixels of an image and chaotic matrix.

Step 6: To alter the position of pixel, flip the pixels of an image in horizontal direction and vertical direction. Fig 4.2 demonstrates the flowchart to encode the image.

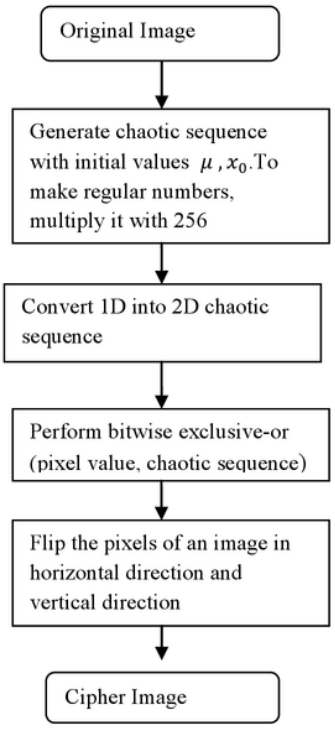


Fig 4.2 Flowchart to encrypt an image

4.3 Image Encryption Algorithm of pixel shuffling and diffusion phase

To enhance the security of information transmitted over the internet, another image encryption algorithm is proposed. In this image encryption algorithm, first the image is divided into four blocks and generate chaotic matrix with Ikeda Map. Each block of image is scrambled with column shuffling and row shuffling with the chaotic matrix. All the scrambled blocks of an image combined to get cipher image. All the pixels of scrambled image are diffused with dynamic index based diffusion.

Divide the image into four equal blocks. Suppose the size of plain image is $P\ X\ Q$. Divide it into four equal blocks img1, img2, img3, img4 which have size $P'\ X\ Q'$ where $P' = P/2$ and $Q' = Q/2$.

4.3.1 Block Scrambling

Use the key (x_o, y_0, u) and Ikeda Map to generate chaotic sequence. Use Eq. (1) and Eq. (2), iterate the chaotic sequence m times where $m = P'Q'$ and obtain the sequence x , y.

The Ikeda Map equation is given as follows:-

$$x_{k+1} = \left(1 + u * \left((x_k cos\ t_k) - (y_k sin\ t_k)\right)\right) mod\ 1, u \geq 0.6 \quad (1)$$

$$y_{k+1} = \left(u * \left((x_k sin\ t_k) + (y_k cos\ t_k)\right)\right) mod\ 1, u \geq 0.6 \quad (2)$$

$$t_k = 0.4 - \left(\frac{6}{1 + x_k^2 + y_k^2}\right) \quad (3)$$

Use Eq. (4) to quantify sequence x,

$$d = floor(x\ \times\ 10^{14}) \quad (4)$$

Eq.(4) is used to quantify sequence y and obtain the sequence s.

$$A1 = reshape(d, P', Q') \quad (5)$$

$$A2 = reshape(s, P', Q') \quad (6)$$

4.3.2 Shuffling

Step 1:- Perform column indexing and shuffling on $img1(p, q)$ and $A1(p, q)$ with the use of function $sortrows(\bullet)$. The function $sortrows(\bullet)$ performs index sorting such as ascending order of $\bullet$ sequence. Fig. 4.3 shows the example of column indexing and shuffling.

Step 2:- If p is equal to P', if not repeat Step1. Else, when $p = P'$, the column indexing and shuffling is completed and image P_{e1} is obtained.

Step 3:- Perform row indexing and shuffling on P_{e1} and $A2(p, q)$, one by one with the function $sortrows(\bullet)$. Fig. 4.4 shows the example of row indexing and shuffling

Step 4:- If q is equal to Q', if not repeat Step3. Else, when $q = Q'$, the row indexing and shuffling is completed and image P_{e2} is obtained.

Step 5:- Repeat Step1~4 for other three blocks of plain image such as img2, img3, img4.

Step 6:- Combine all the scrambled blocks of plain image to a cipher image S which has same size $P\ X\ Q$. Fig 4.5 shows the flowchart of confusion stage.

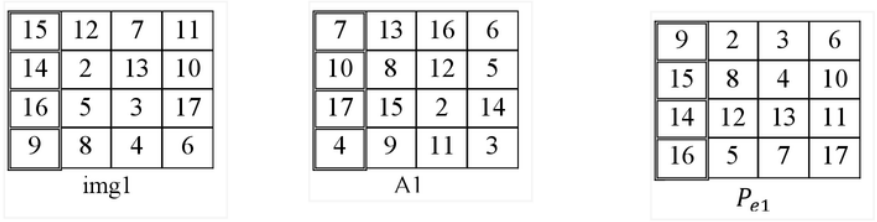


Fig 4.3 Example of Column Shuffling

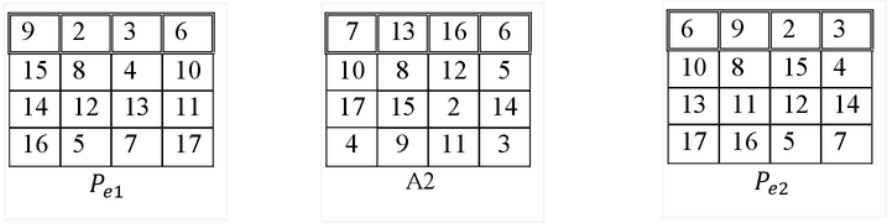


Fig 4.4 Example of Row Shuffling

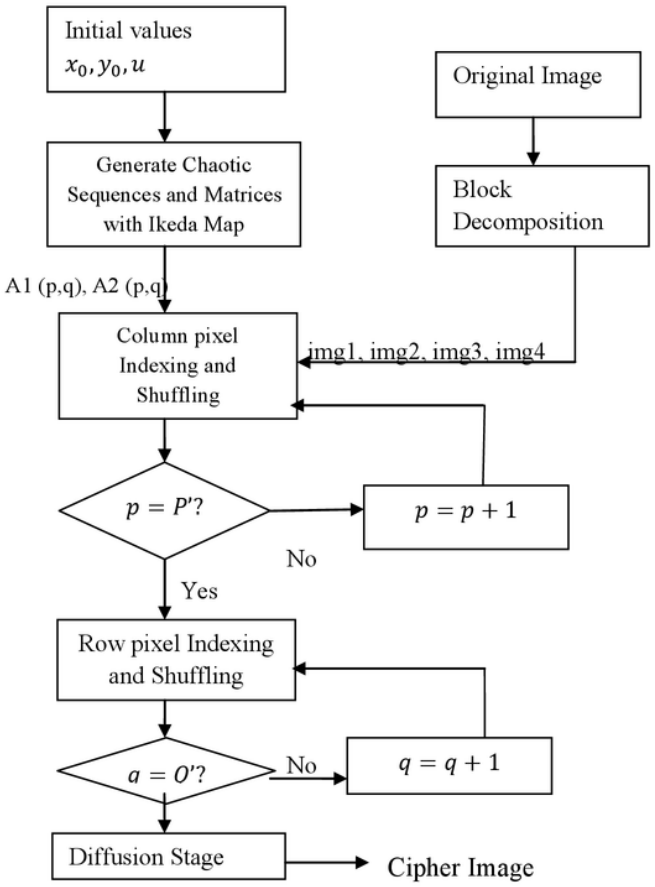


Fig 4.5 Flowchart of Confusion Stage

4.3.3 Diffusion Phase

Step 1:- Convert the cipher image into a sequence h , having the size $n = P\ X\ Q$.

Step 2:- Create chaotic sequence with Logistic map with two initial values z_0, r. Use Eq.(7) to generate chaotic sequence n times.

The Logistic map equation is given as follows:-

$$z_{k+1} = rz_k(1 - z_k)\ , r \in (0,4), z_k \in (0,1) \quad (7)$$

Step 3:- The Eq. (8) is used to quantify the chaotic sequence z.

$$k = mod(floor(z \times 10^{14}), 256) \quad (8)$$

Step 4:- Except the first element, add the elements in sequence h.

$$sum = \sum_{i=2}^{T} h(i) \quad (9)$$

Step 5:- Set s_0 with the Eq. (10):-

$$s_0 = mod(sum, 256) \quad (10)$$

Step 6:- Encrypt the first element of sequence h by Eq. (11). The first encrypted value is used to change other pixel values in image. So, with the first value, the cipher image gets widely changed.

$$h(1)=s_0 \oplus h(1) \oplus z(1) \quad (11)$$

Step 7:- From $i = 2\ to\ n-1$, repeat Step 8~9.

Step 8:- Calculate dynamic indexes pt_1 and pt_2, which are used for encrypting i^{th} element in h.

$$pt_1 = floor\left(\frac{mod\left(\left(h(i-1)+z(i)\right), 256\right)}{256} \times (i-1)\right) + 1 \quad (12)$$

$$pt_2 = floor\left(\frac{mod\left(\left(h(i-1)+z(i)\right), 256\right)}{255} \times (T-i-1)\right) + i + 1 \quad (13)$$

Step 9:- Since for different plain image, the first encoded value and dynamic indexes pt_1 and pt_2 will be distinct. This leads to different i^{th} encrypted value for a plain image.

$$h(i) = h(i) \oplus z(i) \oplus h(pt_1) \oplus h(pt_2) \quad (14)$$

Step 10:- Set $i = n$, utilize Eq. (12) to find index pt_1 and encode the last element by Eq.(13)

$$h(i) = h(i) \oplus z(i) \oplus h(pt_1) \quad (15)$$

Step 11:- Transform the sequence h into a cipher image R. Fig 4.6 shows the flowchart of diffusion stage.

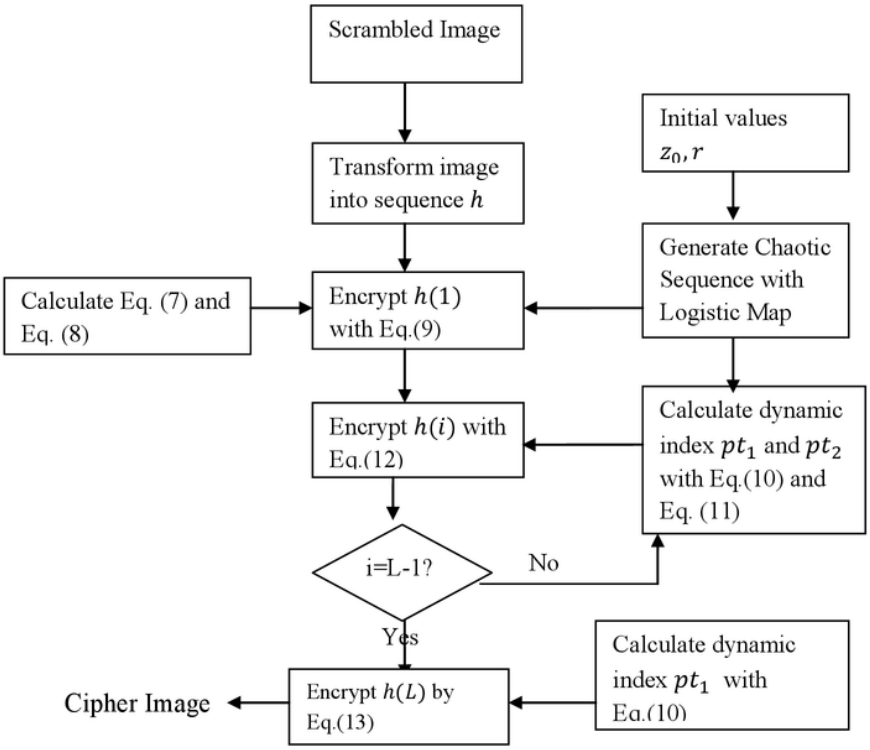


Fig 4.6: Flowchart of diffusion phase

4.4 Image Decryption Algorithm using chaotic sequences and flipping

Turn around the steps of image encryption algorithm to create the original image. Since bitwise exclusive-or operation, flipping are reversible process so scrambled image can be changed into original image.

4.5 Image Decryption Algorithm of pixel shuffling and diffusion phase

Step 1:- Convert the cipher image into the sequence h.

Step 2:- Generate Chaotic Sequence with Logistic Map having keys z_0, r.

Step 3:- Calculate index pt_1 with Eq.(12). Decrypt the last element of sequence such as $h(L)$ with Eq.(13).

Step 4:- Repeat Step 4 from $i = L - 1$ *to* 2.

Step 5:- Calculate index pt_1 and pt_2 by Eq.(12) and Eq.(13). Decrypt the element $h(i)$ with Eq. (12).

Step 6:- Add the elements in sequence h except the first one.

Step 7:- Calculate s_0 to decode the first element of sequence h.

Step 8:- Convert the sequence h into image $n = P \times Q$.

Step 9:- Divide the resultant image into four blocks img1, img2, img3, img4.

Step 10:- Repeat Step 2.2.1 and Step 2.2.2 to generate the unique chaotic sequence and matrix $A1$ and $A2$.

Step 11:- Generate a sequence matrix D having size same as img1. Fig. 4.7 shows the sequence matrix D.

Step 12:- In order to obtain recovery matrix D_{0r}, perform row indexing and shuffling on sequence matrix D and $A2$ with the function $sortrows(\bullet)$.

Step 13:- Perform row indexing and shuffling on P_{e2} and D_{0r} with the function $sortrows(\bullet)$.

Step 14:- If $p \neq P'$, repeat step 13. Else when $p = P'$, the image P_{e2} is obtained.

Step 15:- Generate a sequence matrix $D1$ having size same as img2. Fig. 4.8 shows the sequence matrix $D1$.

Step 16:-In order to get restoration matrix D_{1r}, perform column indexing and shuffling on sequence matrix D_1 and $A1$ with the function $sortrows(\bullet)$.

Step 17:- Perform column indexing and shuffling on P_{e1} and D_{1r} with the use of function $sortrows(\bullet)$.

Step 18:- If $q \neq Q'$, repeat step 17. Else when $q = Q'$, the image img1 is obtained.

Step 19:- Repeat Step 11 to 18 for image blocks img2, img3 img4.

Step 20:- Combine all the blocks img1, img2, img3, img4 to obtain the original image.

1	2	3	4
1	2	3	4
1	2	3	4
1	2	3	4

Fig. 4.7 Sequence Matrix D

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

Fig 4.8 Sequence Matrix D1

Chapter 5

Experimental Observation

5.1 Key Space Analysis

Key space refers to necessity of keys to encode a picture. In chaotic sequence and flipping algorithm, the keys are μ, x_0 while in pixel shuffling and diffusion algorithm, Ikeda chaotic map and logistic map is used to create a chaotic sequence which is used to encrypt an image. In this paper, the keys used are x_0, y_0, z_0, μ, u. The key space of each of initial value x_0, y_0, z_0 is 10^{16}. The key space of each of μ, u is 10^{14}. So, the total number of keys required in pixel shuffling and diffusion algorithm to encrypt an image are 10^{76}. This leads that pixel shuffling and diffusion proposed algorithm has large key space rather than chaotic sequence and flipping algorithm.

5.2 Histogram Analysis

Number of pixel values in range [0,255] in graph represents Histogram. In order to resist attacks, encrypted image's histogram should be uniformly distributed. It can be seen from in the chaotic sequence and flipping algorithm, histogram is not uniformly distributed while in the pixel shuffling and diffusion algorithm, histogram is uniformly distributed. Fig.5.1 and Fig. 5.2 shows Elaine image and its histogram. Fig 5.3 and Fig 5.4 shows encrypted image and its histogram of pixel shuffling and diffusion algorithm. Fig 5.5 and Fig 5.6 shows encrypted image and its histogram of chaotic sequence and flipping algorithm. It can be concluded that the histogram of original image and decrypted image are same in case of pixel shuffling and diffusion algorithm.

Fig. 5.1 Original Image

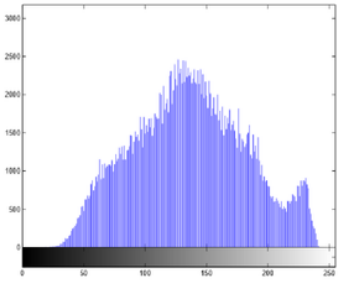


Fig 5.2Histogram of Original Image

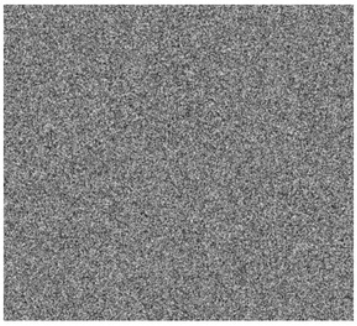


Fig 5.3 Encrypted Image with pixel shuffling and diffusion algorithm

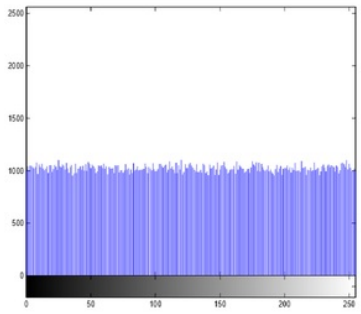


Fig 5.4 Encrypted Image's Histogram of pixel shuffling and diffusion algorithm

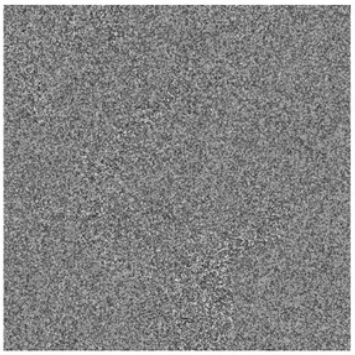


Fig 5.5 Encrypted Image with chaotic sequence and flipping algorithm

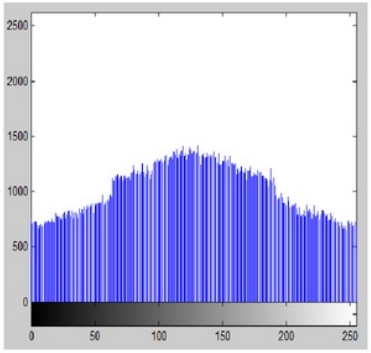


Fig 5.6 Encrypted Image's Histogram of chaotic sequence and flipping algorithm

5.3 Entropy Analysis

The formula of information entropy is given as follows:-

$$E(m) = \sum_{i=0}^{2^s-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{16}$$

where m_i is the symbol, $p(m_i)$ is the probability of message and s is the number of bits required to represent message. For uniformly distributed encrypted image, entropy should be near to 8. Table.5.1 represents Elaine image's entropy and Cipher image's entropy with chaotic sequence and flipping algorithm and pixel shuffling and diffusion algorithm. Cipher image's entropy of pixel shuffling and diffusion algorithm is near to 8 while with the chaotic sequence and flipping algorithm, it is 7.9639. This can be concluded that pixel shuffling and

diffusion algorithm gives better entropy than the chaotic sequence and flipping algorithm.

Table 5.1: Information Entropy

Image	Entropy
Original Image	7.5060
Chaotic Sequence and flipping Algorithm	7.9639
Pixel shuffling and diffusion Algorithm	7.9993

5.4 Key Sensitivity Analysis

Both algorithms are highly sensitive to initial keys. With minor change in initial key, cipher image cannot be decrypted to original one. In case of pixel shuffling and diffusion algorithm, the original image is encrypted with keys 0.01234567891236, 3.987654327, 0.6754567898, 0.9876674567, 1.564321976. With the slight difference in these keys 0.01234567891237, 3.987654328, 0.6754567899, 0.9876674568, 1.564321977, the cipher image cannot be decrypted to original one. In case of chaotic sequence and flipping algorithm, the image is encrypted with keys 0.01234567891236, 3.987654327 and decrypted with 0.01234567891237, 3.987654328 keys. In Figure 5.7 shows Elaine image. Figure 5.8 shows the cipher image and Figure 5.9 shows the decrypted image with the wrong keys in case of pixel shuffling and diffusion algorithm. Fig 5.10 shows the cipher image and Fig 5.11 shows the decrypted image with the wrong keys in case of chaotic sequence and flipping algorithm.

Fig 5.7 Elaine Image

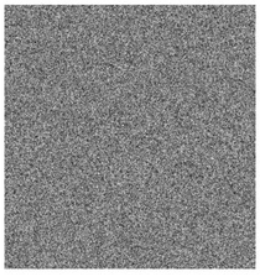


Fig 5.8 Encrypted Image with second algorithm

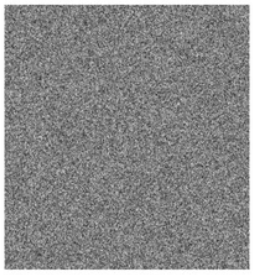


Fig 5.9 Decrypted Image with incorrect keys in second algorithm

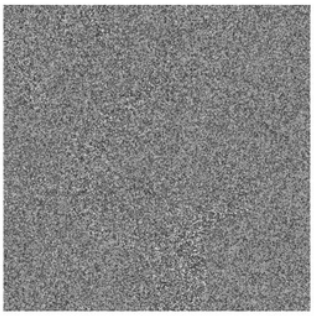


Fig 5.10 Encrypted Image with chaotic sequence and flipping algorithm

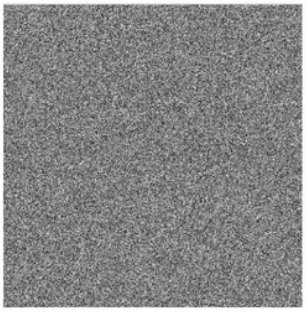


Fig 5.11 Decrypted Image with incorrect keys in chaotic sequence and flipping algorithm

5.5 NPCR and UACI

With the small modification in original image, the cipher image should get widely changed to resist differential attacks. The NPCR (number of pixels changed rate) and UACI (unified average changing intensity) are two factors which can used to test the resistance against differential attacks. The NPCR and UACI can be calculated with the following formula:-

$$NPCR = \sum_{p=1}^{M}\sum_{q=1}^{N}\frac{D(p,q)}{M \times N} \times 100\% \quad (17)$$

$$UACI = \sum_{p=1}^{M}\sum_{q=1}^{N}\frac{C_1(p,q) - C_2(p,q)}{M \times N \times 255} \times 100\% \quad (18)$$

where C_1 is the encrypted image produced by encoding the plain image and C_2 is the cipher image produced by changing one pixel in the plain image. $D(p,q)$ can be calculated with the formula:-

$$D(p,q) = \begin{cases} 0 \; if \; C_1(p,q) = C_2(p,q) \\ 1 \; if \; C_1(p,q) \neq C_2(p,q) \end{cases} \quad (19)$$

With the change in one bit in original image, the cipher image is completely changed. Table 5.2 shows the results of NPCR and UACI with both algorithms. With the result of NPCR and UACI, it can be seen that pixel shuffling and diffusion algorithm is secure against differential attacks but the chaotic sequence and flipping algorithm cannot resist against attacks.

Table 5.2: NPCR and UACI

Algorithm	NPCR	UACI
Chaotic sequence and flipping algorithm	38.14%	50.86%
Pixel shuffling and diffusion	99.61%	33.46%

5.6 Correlation Coefficient Analysis

Pixels of original image are highly correlated. A good encryption algorithm should decrease the correlation coefficient between the pixels of an image. 3000 pairs of adjacent pixels of an image has been chosen in vertical, diagonal and horizontal to compare and analyze the correlation between adjacent pixels of original image and cipher image. Correlation Coefficient can be calculated with formula given as:-

$$r_{pq} = cov(p,q)/\sqrt{D(p)D(q)} \tag{20}$$

$$E(p) = \frac{1}{R}\sum_{i=1}^{R} p_i \tag{21}$$

$$D(p) = \frac{1}{R}\sum_{i=1}^{R} (p_i - E(p))^2 \tag{22}$$

$$cov(p,q) = \frac{1}{R}\sum_{i=1}^{R} (p_i - E(p))(q_i - E(q)) \tag{23}$$

where p, q are pixel value of an image. R is the summation of all pixels of an image. Fig.5.12 shows the correlation plot of two adjacent pixels of an image in vertical, diagonal and horizontal direction before encryption and after encryption in case of pixel shuffling and diffusion algorithm. Table 5.3 shows the correlation coefficient in all the three directions of chaotic sequence and flipping and pixel shuffling and diffusion algorithm. It proves that two adjacent pixels of an image after encryption have low correlation.

Table 5.3:Correlation Coefficient

Image	Vertical	Diagonal	Horizontal
Elaine Image	0.9769	0.9731	0.9738
Chaotic sequence and flipping Algorithm	-0.0150	-0.0062	0.0046
Pixel shuffling and diffusion Algorithm	-0.0073	0.0012	-0.0129

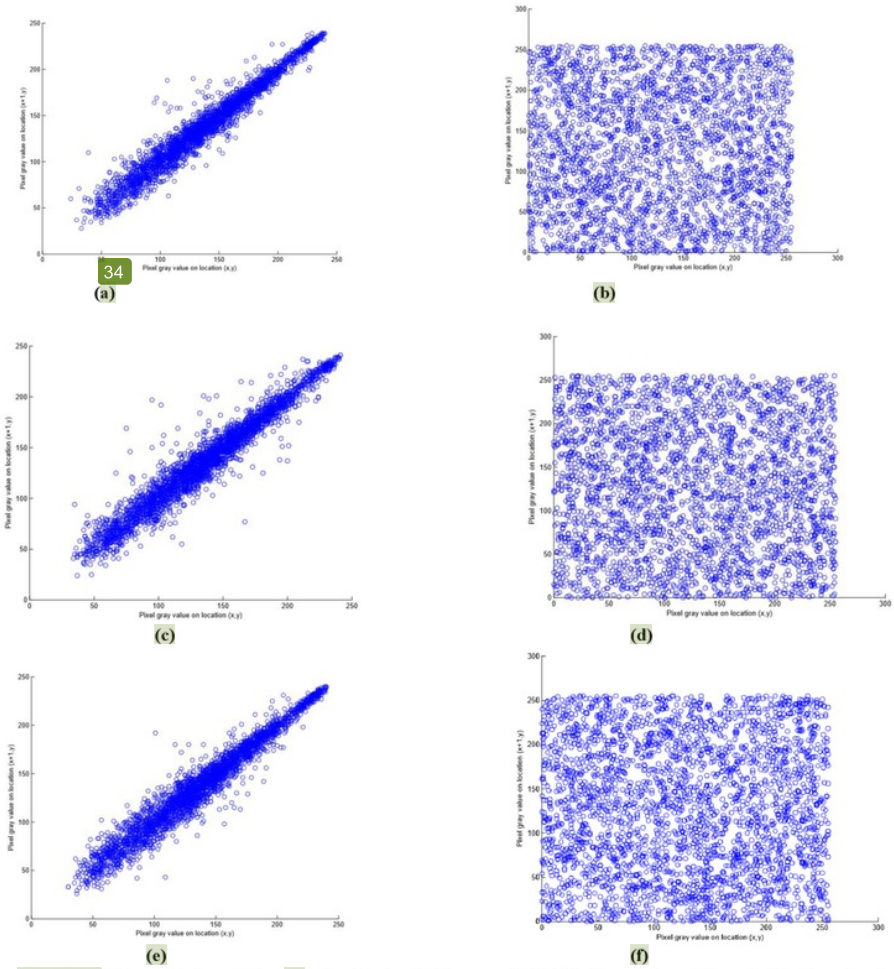


Fig.5.12 Correlation Plot of pixel shuffling and diffusion algorithm(a-b) Vertical Correlation of Elaine Image and Encrypted Image(c-d)Diagonal Correlation of Elaine Image and Encrypted Image(e-f) Horizontal Correlation of Elaine Image and Encrypted Image

Chapter 6
Conclusion and Future Scope

6.1 Conclusion

To securely transfer the data over the internet with the immense growth of multimedia technology, techniques are required. Encryption is among of this technique that securely transfers the images. Many traditional encryption techniques have been used to secure the data transferred over the internet such as AES, DES and RSA algorithm. But, it is easy to decipher the traditional encryption algorithm because conventional encryption algorithm encrypts the image by considering the image as text data. Traditional encryption algorithms are complex to use, time consuming and easy to crack. So, an algorithm of image encryption is proposed which encrypts the image by changing the pixel positions as well as pixel values such as satisfy the confusion and diffusion property. But while transmitting the image over the internet, hackers attack the image by some technique. So, to enhance the security of algorithm, another image encryption algorithm is proposed which involves scrambling of blocks and diffusion phase dynamically. This algorithm divides the image into blocks. Each block of image is scrambled with the chaotic sequences by performing row shuffling and column shuffling. All the scrambled blocks of image combined to give cipher image. The pixels of scrambled image are diffused with dynamic index based diffusion. The dynamic index is generated for each pixel of scrambled image. A comparative study on both algorithms shows that second algorithm is more secure, can resist against attacks and is widely changed after the encryption than first algorithm.

6.2 Future Scope

In this research work, two new encryption techniques are proposed. The pixel shuffling and diffusion algorithm is better than chaotic sequence and flipping algorithm as it can defeat attacks by attackers and cipher image is widely changed after encryption. But the pixel shuffling and diffusion algorithm can be further improved:-

- The pixel shuffling and diffusion algorithm can be further enhanced for 3D images.

- The chaotic map can be changed such that which provides more chaotic behaviour.

REFERENCES

[1] Min Li, Tiang Liang, Yu-jie He," Arnold Transform Based Image Encryption Method", *Published by Atlantis Press,* 2012.

[2] Ping Ping, Yingchi Mao, Xin Lv, Feng Xu, Guoyan Xu, "An Image Encryption Algorithm Using Discrete Henon Map", *Proceedings of the International Conference on Information and Automation,* August 2015.

[3] LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin, "Image Encryption Algorithm Based on Chaos Theory and Sorting Transformation", *International Journal of Computer Science and Network Security,* 2008 (8),pp.64-68.

[4] Guodong Ye, "Image Scrambling encryption algorithm of pixel bit based on chaos map", *Pattern Recognition Letters,* 2010 (31), pp.347-354.

[5] Wang Yanling,"Image Encryption Method Based on Chaotic Sequences and Mapping", *First International Workshop on Education Technology and Computer Science,* 2009,pp 453-457.

[6] M.Y. Mohamed Parvees, J. Abdul Samath, I. Kaspar Raj, B. Parameswaran Bose, "A Colour Byte Encryption Technique for Efficient Image Encryption Based on Combined Chaotic Map", *International Conference on Electrical, Electronics and Optimization Techniques(ICEEOT),*2016,pp 1067-1072.

[7] Lingling Wu, Jianwei Zhang, Weitao Deng, Dongyan He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm", *The 1st International Conference on Information Science and Engineering,* 2009, pp 1164-1167.

[8] Liu Huiying, Xu Caiyun, Kong jun, Du Ying, "A novel secure arithmetic image coding algorithm based on Two-dimension Generalized Logistic Mapping", *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control,* 2015,pp 671-674.

[9] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on 3D chaotic map ", *Commun Nonlinear Sci Numer Simulat,* 2012 (17),pp 2943-2959.

[10] Yang Zou, Xialon Tian, Shaowei Xia, Yali Song, "A Novel Encryption Algorithm Based On Sudoku Puzzle",*4th International Congress on Image and Signal Processing,* 2011,pp 737-740.

[11] X Y Yu, J Zhang, H E Ren, G S Xu, X Y Luo,"Chaotic Image Encryption Algorithm Based on S-DES", *International Symposium on Instrumentation Science and Technology,* 2006 (48),pp 349-353.

[12] Liang Zhao, Avishek Adhikari, Di Xiao, Kouichi Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption", *Commun Nonlinear Sci Numer Simulat,* 2012 (17),pp 3303-3327.

[13] Xiuli Chai, Zhihua Gan, Yiran Chen, Yushu Zhang, "A visually secure encryption scheme based on compressive sensing", *Signal Processing* , 2017(134), pp 35-51.

[14] Lu Xu, Xu Gou, Zhi Li, Jian Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion", *Optics and Lasers in Engineering,* 2017(91),pp 41-52.

[15] Xingyuan Wang, Dapeng Luan, "A novel image encryption algorithm using chaos and reversible cellular automata", *Commun Nonlinear Sci Numer Simulat,* 2013(18),pp 3075-3085.

[16] Omid Mirzaei, Mahdi Yaghoobi, Hassan Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos", *Nonlinear Dyn,* 2012(67), pp 557-566.

[17] Ana Cristina Dascalesu, Radu Eugen Boriga, "A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling", *Nonlinear Dyn*, 2013(74), pp 307-318.

[18] C.K. Huang, C.W. Liao, S.L. Hsu, Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", *Telecommun Syst,* 2013(52), pp 563-571.

[19] Rong-Jian Chen, Yi-Te Lai, Jui-Lin Lai, "Image Encrypted System Using Scan Patterns and 2-D Cellular Automata", *The 2004 IEEE Asia-Pacific Conference on Circuits and Systems,*2009, pp 6-9.

[20] Ruisong Ye, Huiliang Li ,"A Novel Image Scrambling and Watermarking Scheme Based on Cellular Automata", *International Symposium on Electronic Commerce and Security,* 2008, pp 938-941.

[21] Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati-Q, Zohreh souzanchi-k, "An Image Encryption System by Indefinite Cellular Automata and Chaos", *2nd*

International Conference on Signal Processing Systems(ICSPS), 2010(3), pp 23-27.

[22] WEI Qin, LIU Quan , LI Fen, "A Novel Algorithm for Image Encryption Based on Weighted and p-interval CA", *Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science,* 2010, pp 440-444.

[23] Abdel Latif Abu Dalhoum, Basel A. Mahafzah, Aiman Ayyal Awwad, Ibrahim Aldamari, Alfonso Ortega, Manuel Alfonseca, "Digital Image Scrambling Using 2D Cellular Automata", *14th International Symposium on Multimedia,* 2012, pp 28-36.

[24] LOU Yuefang, HU Tianqiao, "A Novel Image Scrambling System Based on Cellular Automata and Improved Chaotic System", *5th International Congress on Image and Signal Processing (CISP),* 2012, pp 1139-1142.

[25] Chuan Peng, Yuanxiang Li, "A New Algorithm for Image Encryption based on Couple Chaotic System and Cellular Automata", *International Conference on Mechatronic Sciences, Electric Engineering and Computer(MEC),* 2013, pp 1645-1648.

[26] Subrata Nandi, Satyabrata Roy, Siddhartha Nath, Sayan Chakraborty, Wahiba Ben Abdessalem Karaa, Nilanjan Dey, "1-D Group Cellular Automata Based Image Encryption Technique", *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),*2014, pp 521-526.

[27] Samaneh Zamani, Mahdi Javanmard, Nima Jafarzadeh, Mostafa Zamani, "A Novel Image Encryption Scheme Based on Hyper Chaotic Systems and Fuzzy Cellular Automata", *22nd Iranian Conference on Electrical Engineering,* 2014, pp 1136-1141.

[28] Ping Ping, Xin Lv, Yingchi Mao, Rongchi Qi, "Image Scrambling based on Life-Like Cellular Automata", *The 10th International Conference on Computer Science & Education,*2015, pp 345-348.

[29] Ping Ping, Feng Xu, Md Shaiful Islam Babu, Xin Lv, Yingchi Mao, "Image Scrambling Scheme based on Bit-Level Permutation and 2-D Cellular Automata", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing,* 2015, pp 413-416.

[30] Abdel Latif Abu Dalhoum, Alia Madain, "Digital image scrambling based on elementary cellular automata", *Multimedia Tools Appl,* 2016(75),pp 17019-17034.

[31] Xingyuan Wang, Dahai Xu, "A novel image encryption scheme using chaos and Langton's Ant cellular automata", *Nonlinear Dyn,* 2015(79), pp 2449-2456.

[32] Ye GD, "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognit Lett, 2010(31),pp 347-354.

[33] "The process of asymmetric encryption", https://msdn.microsoft.com/en-us/library/ ff650720.aspx.

[34] "The process of symmetric encryption", https://msdn.microsoft.com/en-us/library/ ff650720.aspx

[35] "VonNeumann Neighborhood", http://mathworld.wolfram.com/VonNeumann Neighborhood.html

[36] "Moore Neighborhood", http://mathworld.wolfram.com/MooreNeighborhood .html

VIDEO PRESENTATION

- https://youtu.be/5VPbU4FjhN8

LIST OF PUBLICATIONS

- Priyanka Takkar, Ashish Girdhar, Dr. V. P. Singh, "Image Encryption Algorithm Using Chaotic Sequence and Flipping", *International Conference on Computing Communication and Automation*, 2017. **(Accepted)**
- Priyanka Takkar, Ashish Girdhar, Dr. V. P. Singh, "A Pixel Shuffling and Diffusion Based Image Encryption Algorithm", *Signal Processing*, 2017. **(Communicated)**

Priyanka_14-07-2017

ORIGINALITY REPORT

%10	%2	%9	%2
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to ABV-Indian Institute of Information Technology and Management Gwalior Student Paper	%1
2	Xu, Lu, Xu Gou, Zhi Li, and Jian Li. "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion", Optics and Lasers in Engineering, 2017. Publication	%1
3	Chai, Xiuli, Zhihua Gan, Yiran Chen, and Yushu Zhang. "A visually secure image encryption scheme based on compressive sensing", Signal Processing, 2017. Publication	%1
4	Zou, Yang, Xiaolin Tian, Shaowei Xia, and Yali Song. "A novel image scrambling algorithm based on Sudoku puzzle", 2011 4th International Congress on Image and Signal Processing, 2011. Publication	<%1

5	Ping Ping, Feng Xu, Md Shaiful Islam Babu, Xin Lv, Yingchi Mao. "Image Scrambling Scheme Based on Bit-Level Permutation and 2-D Cellular Automata", 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2015 Publication	<%1
6	C. K. Huang. "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", Telecommunication Systems, 06/04/2011 Publication	<%1
7	www.seg.inf.uc3m.es Internet Source	<%1
8	www.ijcit.com Internet Source	<%1
9	Ping, Ping, Feng Xu, and Zhi-Jian Wang. "Image encryption based on non-affine and balanced cellular automata", Signal Processing, 2014. Publication	<%1
10	Li, C.. "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks", Signal Processing, 201104 Publication	<%1

11	Wang, Leyuan, Hongjun Song, and Ping Liu. "A novel hybrid color image encryption algorithm using two complex chaotic systems", Optics and Lasers in Engineering, 2016. Publication	<%1
12	www.ijetr.org Internet Source	<%1
13	Awwad , Aiman Mamdouh Ahmad Ayyal. "Digital Image Scrambling Method Based on Two Dimensional Cellular Automata : A Test of the Lambda Value", University of Jordan, 2009. Publication	<%1
14	Liu, Hongjun, Xingyuan Wang, and Abdurahman Kadir. "Color image encryption using Choquet fuzzy integral and hyper chaotic system", Optik - International Journal for Light and Electron Optics, 2013. Publication	<%1
15	Zhou, Nanrun, Shumin Pan, Shan Cheng, and Zhihong Zhou. "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing", Optics & Laser Technology, 2016. Publication	<%1
16	journal.iis.sinica.edu.tw Internet Source	<%1

17	Liu, Xiangdong, Xueye Ang, and Cunrui Wang. "A Chaotic Image Scrambling Scheme Based on Sorting Transformation", 2010 International Workshop on Chaos-Fractal Theories and Applications, 2010. Publication	<%1
18	"INVESTIGATIONS OF LIFE-LIKE CELLULAR AUTOMATA FOR IMAGE SCRAMBLING", Control and Intelligent Systems, 2016. Publication	<%1
19	Zamani, Samaneh, Mahdi Javanmard, Nima Jafarzadeh, and Mostafa Zamani. "A novel image encryption scheme based on hyper chaotic systems and fuzzy cellular automata", 2014 22nd Iranian Conference on Electrical Engineering (ICEE), 2014. Publication	<%1
20	Zhao, L.. "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption", Communications in Nonlinear Science and Numerical Simulation, 201208 Publication	<%1
21	Advances in Intelligent Systems and Computing, 2016. Publication	<%1
	Hanchinamani, Gururaj and Kulakarni,	

22	Linganagouda. "Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform", International Journal of Hybrid Information Technology, 2014. Publication	<%1
23	Huiliang Li. "A Novel Image Scrambling and Watermarking Scheme Based on Cellular Automata", 2008 International Symposium on Electronic Commerce and Security, 08/2008 Publication	<%1
24	Ye, Guodong, and Xiaoling Huang. "A novel block chaotic encryption scheme for remote sensing image", Multimedia Tools and Applications, 2015. Publication	<%1
25	Haohao Yuan and Lianyuan Jiang. "Image Scrambling based on Spiral Filling of Bits", International Journal of Signal Processing, Image Processing & Pattern Recognition, 2015. Publication	<%1
26	Communications in Computer and Information Science, 2014. Publication	<%1
27	Submitted to Sunway College Student Paper	<%1
28	Submitted to American Intercontinental University Online	<%1

	Student Paper	
29	Gao, T.. "A new image encryption algorithm based on hyper-chaos", Physics Letters A, 20080121 Publication	<%1
30	soar.wichita.edu Internet Source	<%1
31	Nandi, Subrata, Satyabrata Roy, Siddhartha Nath, Sayan Chakraborty, Wahiba Ben Abdessalem Karaa, and Nilanjan Dey. "1-D group cellular automata based image encryption technique", 2014 International Conference on Control Instrumentation Communication and Computational Technologies (ICCICCT), 2014. Publication	<%1
32	www.iita-conference.org Internet Source	<%1
33	dspace.thapar.edu:8080 Internet Source	<%1
34	publikationen.bibliothek.kit.edu Internet Source	<%1
35	Guesmi, Ramzi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, and Mounir Samet. "A novel design of Chaos based S-Boxes using genetic algorithm techniques", 2014 IEEE/ACS	<%1

11th International Conference on Computer Systems and Applications (AICCSA), 2014.
Publication

36	gala.gre.ac.uk Internet Source	<%1
37	X Y Yu. "Chaotic Image Scrambling Algorithm Based on S-DES", Journal of Physics Conference Series, 10/01/2006 Publication	<%1
38	Liu, Ye, Jun Wang, Jinghui Fan, and Lihua Gong. "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences", Multimedia Tools and Applications, 2015. Publication	<%1
39	Wang Yanling. "Image Scrambling Method Based on Chaotic Sequences and Mapping", 2009 First International Workshop on Education Technology and Computer Science, 03/2009 Publication	<%1
40	Ye, G.. "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognition Letters, 20100401 Publication	<%1
41	www.scribd.com Internet Source	<%1

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	< 10 WORDS
EXCLUDE BIBLIOGRAPHY	ON		