Image Encryption using 2D Cellular Automata

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

Master of Technology

in

Computer Science and Applications

Submitted By

Tejaswita Priyam

(Roll No. 601203029)

Under the supervision of:

Dr. Rupali Bhardwaj

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Image Encryption using 2D Cellular Automata"**, in partial fulfillment of the requirements for the award of 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. Rupali Bhardwaj* and refers other researcher's work which are duly listed in the reference section.

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

Tejaswita Priyam

Tejaswita Priyam

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

Dr Rupali Bhardwaj
Assistant Professor
CSED
Thapar University

Countersigned by

Dr. Deepak Garg
Head
Computer Science and Engineering Department
Thapar University Patiala

Dr. S. S. Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

The successful completion of any task would be incomplete without acknowledging the people who made it possible and whose constant guidance and encouragement secured the success. First of all, I would like to express my gratitude to **Dr. Rupali Bhardwaj, Assistant Professor,** Computer Science and Engineering Department, Thapar University, Patiala for introducing me to document cellular automata and for all her guidance and support. This thesis work was enabled and sustained by her vision and ideas. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own and at the same time the guidance to recover when my steps faltered. Her patience and support helped me overcome many crisis situations and finish this dissertation. She has been a source of inspiration for me.

I am grateful to **Dr. Deepak Garg**, Head of Department, and **Dr. Singara Singh, Assistant Professor,** Department of Computer Science and Engineering Department, entire faculty and staff of Computer Science and Engineering Department and then friends who devoted their valuable time and helped me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work. Last but not the least I would like to express my heartfelt thanks to my parents and my friends who with their thought provoking views, veracity and whole hearted co-operation helped me in doing this dissertation.

Lastly, I would also like to thank my parents for their years of unyielding love and encouragement. They have always wanted the best for me and I admire their determination and sacrifice.

Tejaswita Priyam

Tejaswita Priyam

(601203029)

ABSTRACT

This thesis sums up problems associated with trivial Arnold cat map and 2D Cellular automata scrambling technique. An exploratory study is performed over scrambling of gray scale image using Arnold cat map and 2D Cellular automata's both variants i.e. Moore neighborhood and Vonneumann neighborhood. Firstly, we scramble the gray scale image using both techniques i.e. Arnold transform and 2D Cellular automata and then make a comparative study about effectiveness of scrambling by both the mentioned techniques, we conclude which technique scrambles image with high scrambling degree measured by scrambling degree parameters GDD and Correlation Coefficient. Later, we focused on improving scrambling degree by using combination of both techniques i.e. Arnold and 2D Cellular automata. For combined technique of scrambling we first scramble image with one of the variant of 2D Cellular automata and then we scramble through Arnold cat map. Further a comparison between individual Arnold and 2D Cellular automata with combined scrambling technique's performance is obtained. A conclusion is drawn about scrambling degree of this combined technique whether it improves scrambling degree parameters i.e. GDD and Correlation Coefficient than previous methods or not. Apart from improving scrambling degree this combined technique ensures that this scrambling technique doesn't possess periodicity property even after using Arnold transform while scrambling.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

With huge growth in internet, multimedia has become a great carrier of information. The multimedia can be edited, replicated easily by spreading over internet or by some other medium [18, 26], which causes problem of not being able to give even any copy right proof if once it is pirated. So copyright is legally not protected [22]. Trivial encryption is done over multimedia contents for their secure transmission but with improvement in speed of computer and with use of parallel processing they can be easily deciphered by algorithms [29]. Images are one of a kind of multimedia technology, as far as understandability or expressive world is concerned images play best role at that. Images are quite intuitive for believing or seeing and they are informative too. We need to provide secured way of transmitting images like any other multimedia. Due to lack of guaranteed secure transmission of images by traditional encryption schemes, transmission of image has become very big problem so, two encryption methods i.e. digital watermarks and digital scrambling is proposed as a solution. Digital image scrambling means creating confusion in image elements to make it non informative for sake of protecting it from theft, manipulation of content and privacy measures. At present there are many technologies for scrambling images like Arnold Cat Map, Hilbert curve transform, Josephus traversing and chaos sequence, 2D cellular automata's Game of Life [8, 33]. Images means collection of atomic units called pixel, which represents some color value. Images can be thought of as a matrix containing pixel values of each pixel of whole image. Primarily the basic idea behind scrambling of image is to change position of pixels of image through matrix transformation working according to formula of proposed algorithm. In this way high quality of confusion is created in image within few evolutions or we can say rounds [7]. Scrambling is used to create a non intelligible image which prevents human or computer vision system from recognizing the true content. First image is scrambled or we can say encrypted in a way to transmit it securely i.e. distortion is created, and then it is descrambled to get back actual image by using descrambling algorithm of proposed scheme. Only authorized person is capable of descrambling the scrambled image as only he/she will be given all possible keys used while scrambling. One cannot find any difference between original and descrambled image which we finally get. Scrambling is not only used for encrypted transmission of

electronic media but also for preprocessing and/or post processing for watermarked images [24, 27]. Image scrambling has attracted researchers in recent years. Different scrambling scheme produces different results of same image and which performs better is difficult issue to analyze.

1.1 Scrambling Techniques

There are dozens of scrambling schemes present today and we have focused on Arnold transform and 2D cellular automata transform for our research.

1.1.1 2D Arnold Cat Map

This is a classical scheme of scrambling images proposed by Russian mathematician Vladimir I. Arnold in the 1960s. It changes position of pixels in image and hence breaks relationship of adjacent pixels of image and creates chaos all over the image so the image doesn't remain what it was originally. A mathematical equation is used for producing noise all over image that is given by Eq. (1.1) and Eq. (1.2) [14].

$$Xn + 1 = [Xn + a * Yn] \bmod (N). \quad (1.1)$$

$$Yn + 1 = [b * Xn + (a * b + 1)Yn] \bmod (N). \quad (1.2)$$

Here Xn, Yn is current position of a pixel, Xn+1, Yn+1 is new positions of same pixel after application of above mathematical formula a particular number of time. N is dimension of image, as Arnold Cat Map is only applicable on square images, a and b are controlling parameters they work as keys. Other than a, b number of time we apply the rule to image is too a key for proposed scrambling scheme. Any algebraic equation can be written in terms of matrix, so the matrix representation of Arnold Cat Map is shown in Eq. (1.3) [10, 12, 23].The general form of Arnold Cat Map can be given by the transformation- $\mathbf{F}: T^2 \rightarrow T^2$ from torus **T** to itself.

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } N) \quad (1.3)$$

Modified Arnold's transform can be represented by Eq. (1.4) or Eq. (1.5) [15].

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} i+1 & i \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } N) \quad (1.4)$$

OR

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} i & i+1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } N) \quad (1.5)$$

Here, i € (1, 2, 3….., N-1). X', Y' is new position of pixel and X, Y is current position of pixel, and N is dimension of image. Arnold's Cat Map shows periodic behavior so, after particular iteration from scrambled image original image is recovered [15].

1.1.1.1 Demerits of Arnold Cat Map

1. It has periodic behavior i.e. after particular iterations it comes back to original image. So, anyone can use its periodic feature to extract actual information [13].
2. Arnold's Cat Map works only on square images. It cannot work upon any rectangular image which is a major disadvantage [19, 23].
3. It is less secure as controlling parameters are very few so it can be invaded easily [19, 30].

Hence, it is less secure and not very robust against attacks.

1.1.2 2D Cellular Automata (Game of Life)

The universe of Game of Life is a two dimensional cellular automata devised by J. H. Conway in 1970 called as Conway's Game Of Life is actually an infinite orthogonal grid which is of cells each of which is either dead or alive. A dead cell is denoted by a '0' and a live cell by '1'. Game of Life is an example of uniform and synchronous cellular automata having local state transition functions. The neighborhood consists of either Von Neumann type or Moore type as mentioned above. Initially we just need to provide initial state to each cell and further no input is required to see how it evolves. There are some rules regarding Game of Life and those rules are applied to all pixels/cells of infinite grid and same rules are applied to all of them and they change their state simultaneously according to applied rule. The rules are applied for many evolutions and for each evolution change in state of cells are noticed. Each cell's next state depends upon current state of its neighbors.

1.1.2.1 Different Types of Neighborhood of 2D Cellular Automata

In our experiment the image is considered as rectangular grid. Each cell of that grid represents a pixel of image. Before we scramble the image using cellular automata we need to know the status of neighbors of a particular cell. The structure of neighbors includes Von Neumann and Moore neighborhood [2, 28], as discussed below.

A. Von Neumann Neighborhood

This neighborhood is a diamond shaped neighborhood around the cell (x_0, y_0) and can be defined as Eq. (1.6) [6].

$$N^v(x_0, y_0) = \{(x, y): |x - x_0| + |y - y_0| \leq r \quad (1.6)$$

Here (x, y) are possible neighbors of current cell (x_0, y_0) and r is the radius which represents neighborhood's dimension. If r=1 this implies only immediate vicinity of current cell is taken as neighbors belonging to it, i.e. top, bottom, left, right cells around current cell as seen in Figure (1.1).

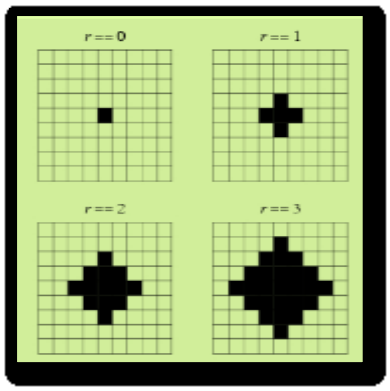


Figure 1.1: Vonneumann neighborhood

B. Moore Neighborhood

This is square neighborhood around current cell (x_0, y_0) and its definition can be seen by Eq. (1.7) [6].

$$N^m(x_0, y_0) = \{(x, y): |x - x_0| \leq r, |y - y_0| \leq r\} \quad (1.7)$$

(x, y) are possible neighborhood current cell, r is the radius representing dimension of neighborhood. Moore neighborhood also include cells at top-right, top-left, bottom-left, bottom-right. In Moore neighborhood diagonal cells to current cell are also considered, hence it is a bit different than Von Neumann neighborhood that can be seen by Figure (1.2).

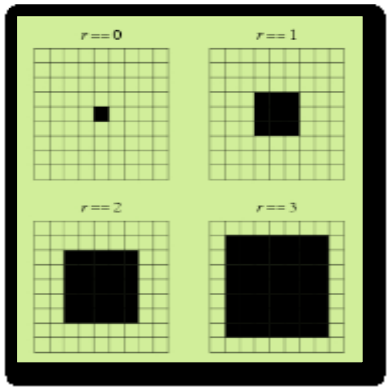


Figure 1.2: Moore neighborhood

We have used both types of neighborhood for our research i.e. Moore neighborhood and Vonneumann neighborhood for scrambling image. Moore neighborhood includes more number of neighbors than Vonneumann neighborhood by including diagonal cell too around current cell. Evolution of cells for radius=1 is shown in Figure 1.1 and Figure 1.2. A cell at one time alive becomes other time dead and a dead cell becomes alive. This transition happens with help of rules defined for Game of Life which is discussed below.

1.1.2.2 Rules of Game of Life [14]

Table 1.2 Rules of Game of Life

	Status of cell at time (t)	Status of cell at time (t+1)	States of neighbors at time (t)
Birth	Dead	Alive	Exactly 3 neighbors alive
Death by overcrowding	Alive	Dead	Four or more neighbors alive
Death by exposure	Alive	Dead	One or none neighbor alive
Survival	Alive	Alive	Two neighbors alive

1.1.2.3 Application Areas of Game of Life [9]

- **Pattern Generation-**Many different types of patterns can be generated by Game of Life such as still lives (the eaters), oscillators, patterns that translate themselves across the board. We require patterns for simulation of forest fire problem, simulation of traffic signal handling, simulation of biological process, simulation of cancer cells growth, simulation of social movements and many more it is a very active area of research.
- **Video Games-** For entertainment purpose some games are developed by Game of Life. Such game is, live cells have one of two colors, and a player wins when all cells of opponent's color are eliminated. When a dead cell has three live neighbors, it becomes live in the same color as the majority of its neighbors, as in the aforementioned immigration.
- **Music**- While composing music Game of Life is used for techniques especially in MIDI sequencing. Sounds are created by using patterns generated by Game of Life.
- **Images**- Rules of Game of Life are used for watermarking in images or for scrambling an image for encryption purpose.
- **Modeling Fluid Flow-**One of the most important application of Game of Life in today's science is modeling fluid flow. Simulating fluid flow is very difficult because of its basic equation the Naiver-stocks differential equation. Game of Life's model for fluid flow is a lattice gas model.

- **Self Organized Critical Phenomenon-** Large scale events that occur rarely like earthquake, avalanche or a stock market crash. In these cases Game of Life deals with trying to understand the latter variety of these incidences which are triggered by some strong forces.

1.1.2.4 Merits of Game of Life

Game of life works excellent for complex sophisticated systems. Areas where complex equations are used and are hard to simulate Game of Life can handle those areas nicely and produces desired result [18, 31]. For complex and very sensitive systems Game of Life works better than Arnold Cat Map. It drastically simplified Von Neumann's ideas, unlike Von Neumann, who created an extraordinarily complex system of states and rules, Conway wanted to achieve a similar "life like" result with the simplest set of rules [2]. Unlike Arnold Cat Map it can work upon rectangular images too for scrambling technique. In Game of Life each cell will have a bigger neighborhood, and that will open up the door to a range of possible applications. Arnold Cat Map is less secure as by repeating the scrambling algorithm a particular number of time the original information can be retrieved but in Game of Life without knowing secret key and descrambling technique no one will be able to recover original message. For these merits of Game of Life we are comparing scrambling technique of 2D cellular automata with classical scrambling technique i.e. Arnold Cat Map, whether it performs better or a way closer to it for good results.

Objective of Thesis: The objective of this research is to find out how good cellular automata performs for scrambling images against classical method of Arnold Cat Map scrambling technique. To analyze performances of both scheme scrambling degree measurement parameters like gray difference and gray degree (GDD) and correlation coefficient is used. A new technique is introduced to improve effects of scrambling where, image is scrambled with a combined application of both the scrambling scheme i.e. Arnold and 2D cellular automata which improves scrambling performance. In our research we try to find out a better way of scrambling by combination of Arnold and 2D cellular automata. A comparison is made among all techniques to conclude how good this new technique performs against trivial methods.

Thesis Plan: This thesis contains six chapters. Chapter-2 is Literature Review, chapter-3 is Problem Statement, chapter-4 is Proposed Solution, chapter-5 is Experimental Results and chapter 6 is Conclusion.

CHAPTER 2
LITERATURE REVIEW

Many discussions have been carried out previously on image encryption. There was a security issue with traditional encryption schemes so another way of encryption taken place that is called scrambling. This chapter provides an immediate look on significant research work on image scrambling using different approaches their methodology experimental effect and conclusions. Among several approaches, scrambling work based on Arnold Cat Map and 2D cellular automata's Game of Life has given special privilege.

Guodong Ye et al. [8] performed double scrambling scheme which scrambles positions and gray scrambling of pixel with help of two keys. Matrix element corresponding to image is converted to its ASCII code, then it is being converted to binary matrix. These binary numbers scrambles themselves. Reverse scrambling like Josephus or chaos sequence is used on previously got matrix, and another binary matrix is obtained. Then after, all binary numbers of matrix is converted to decimal numbers and final matrix is got. They have applied same procedure again on image and encrypted message is obtained. GDD (Gray difference and Gray degree) is used to evaluate scrambling degree of proposed technique which concludes that this scheme gives better security, its restoration is simple because of reversible property of this algorithm, it is suitable to any size gray scale image and it can be extended to multi color image.

Ruisong Ye et al. [24] proposed a watermarking scheme based on cellular automata where, a cellular automata lattice is divided into 2^n parts and then approximated box dimension of evolving configurations of cellular automata is computed by formula defined for it for some iterations then approximation box and chaotic map is obtained is obtained at those iterations. This way the given image is scrambled, after this image is watermarked. This scrambled image is used for pre and post treatment for watermarking. GDD (gray difference and gray degree) is used to evaluate scrambling degree of proposed scheme.

Reema Rhine et al. [22] proposed an image scrambling technique for image hiding where, Rubik's cubic algorithm is applied for scrambling the image and then data hiding is performed. Rubik's cube possesses 6 faces and it can be divided into 54 elements i.e. 6 faces each of 3x3 for scrambling process, then it explores property of

Arnold Cat Map and a comparative analysis is made between both of them. Hidden information is first scrambled by applying Rubik's cubic algorithm an encipher system is applied to encrypt hidden data and stego image is obtained. Here, Rubik's cubic is combined with encipher system for data hiding. A comparison between Arnold Cat Map and this scheme concludes that Rubik's cubic algorithm possess benefits of reversibility, it can work on any shape of image , works on pixels or blocks of pixels, good visual quality, better security.

Prashan Premaratne [21] proposed key based scrambling on image where, a key of length 10 to 100 is obtained which leads to very secure scrambling effect which has probability of less than $5x10^{-300}$ to be descrambled by an invader. User defined pseudorandom integer is generated of key length, This integer is used for row and column wise shuffling of image pixel. For bigger image bigger sequence is required so, periodically user defined sequence is inserted and each sequence is incremented by one to get longer sequence. Once all rows are switched using key sequence, columns are switched using same sequence. After this circular shifting of rows and columns is done using key sequence. This algorithm doesn't affect pixel value of image. This is highly secured position scrambling technique with simple effort.

Saurabh Chandra et al. [25] presented data hiding technique by pixel scrambling using cellular automata. For this purpose R-prime shuffling is used to encrypt the image. Two different R-prime numbers for rows and columns are considered. 2D/3D M-sequence transform is used to scramble 2D/3D image. Rows and columns coefficient matrices are calculated by choosing security keys shift parameter r and distance parameter p. Scrambling done on 2D/3D image by one time. Inverse M-sequence transform is used for descrambling. Compression ratio, peak signal to noise ratio (PSNR) is used to evaluate effectiveness of compression technique.

Md. Moniruzzaman et al. [14] presented a watermarking scheme based on Game of Life of cellular automata. Watermarking is done on a gray scale image with help of Arnold Cat Map, Logistic Map and Game of Life automata. Scrambling on original image is done by Arnold Cat Map, initial random configuration for Game of Life is developed with help of logistic map, and Game of Life is finally used to scramble watermarked image. Scrambled watermarked image is embedded into LSB (least significant bit) plane of original image. After performing inverse Arnold Cat Map, final cat map, logistic map, Game of Life respectively. Using multiple keys ensures

high security and this scheme provides low mean square error and high peak signal to noise which is need for effective watermarking technique.

Omar Adwan et al. [18] presented a watermarking scheme by 2D cellular automata on gray scale image. This scheme is implemented in spatial domain. Gray value of two least significant bit (LSB) of pixel is added with gray value of two least significant bit (LSB) of pixel of host image. Proposed scheme is secured enough to resist attacks because of use of different keys.

Aimam M. Ayyal Awwad et al. [2] proposed a color watermarking scheme based on Conway Game of 2D cellular automata. A gray watermarked image is embedded into blue component of color host image with help of 2D cellular automata on periodic and closed boundary, where two least significant bit (LSB) of pixel of gray watermark image is added to blue value of two least significant (LSB) of pixels of blue band of host image. Similarity between host and watermarked image is measured by peak signal to noise ratio (PSNR), mean square error (MSE), normalized correlation. Results on these parameters ensure about low visible distortion in host image and robustness against various image processing techniques.

Fasal Qadir et al. [6] proposed a digital image scrambling based on 2D cellular automata on gray scale image for periodic and without boundary then gray difference degree (GDD) is used for both scheme and compared. Proposed algorithm provides better scrambling effect than conventional ones and works for any size image.

Abdel Latif et al. [1] proposed an algorithm on various gray scale images and are scrambled with help of 2D cellular automata, then on basis of gray difference degree (GDD) they are compared which concludes that highest GDD corresponds to Moore neighborhood and periodic boundary, while lowest GDD corresponds to Von Neumann and closed boundary. A comparison is made with Ye and Li proposed algorithm to scramble the image and ensures high security and better scrambling effect.

Minati Mishra et al. [15] presented image steganography with modified Arnold Cat Map, where spatial domain least significant bit substitution on 1 bit, 2 bit, 3 bit, 4 bit plane for information embedding is applied. Arnold Cat Map in two different phases is applied twice to ensure security. This is done over 20 different gray scale images. A comparison between least significant bit (LSB) substitution and simple Arnold transform is applied. The research proves that distortion of original image is minimized against the unscrambled three bit substitution method. This method is not

robust against noise because of being spatial domain method but having high security and imperceptibility.

Pawan N. Khade et al. [20] presented paper on 3D Arnold Cat Map and its scrambling effect on colored image, which was proposed by two different authors. R, G, B component's scrambling effect is presented. A histogram comparison between 2D and 3D Arnold Cat Map is presented, then after inverse Arnold transform is presented. This paper concludes that 3D Arnold Cat Map is more secure than 2D and possess uniform scrambling effects.

Min Li et al. [16] presented a new encryption algorithm which improves security of image during transmission. A multi region scrambling technique is presented which splits non square image to multiple square regions and scrambles each region. This new way improves security and can work upon any size image.

Gabreil Peterson [7] discusses and explores properties of Arnold Cat Map. Arnold Cat Map transformation is understood in terms of shear in X and Y planes. Image of earth is successfully scrambled and output at different iterations is shown. A relation between period of an image and its number of rows and columns are established.

Jianghong Bao et al. [10] presented work on period of discrete Arnold cat map and formulae for calculation of minimal period when modulo is prime and when modulo is composite is developed. A relation between period of discrete Cat Map and its modulo for different parameters are developed.

Pan Tian-Gong et al. [19] presented paper with an algorithm of image encryption based on 3D Arnold Cat Map and chaotic map. Image scrambled by 3D Arnold Cat Map and initial value of logistic produces a sequence using math transformation to get keys. Histograms are developed before and after scrambling of image, which concludes that this scheme develops strong keys and faster effects.

Mao Yu Huang et al. [13] has presented a paper that provides an algorithm for image encryption based on Arnold Cat Map and logistic map to improve security. Arnold Cat Map along with chaotic map is being applied on image. Logistic map shuffles image then it is being passed to Arnold Cat Map. This improves security largely. Concludes that this approach has higher security than applying only Arnold Cat Map.

Xiaoqiang Zhang et al. [30] presented paper on two dimensional Arnold transform. A program of collecting sample data is designed by regression analysis of relationship between the order of image and its corresponding period of Arnold transform. This is

done by fitting a regression equation that can be seen as accurate estimation of Arnold transformation period. This estimation is much better than previously proposed ones.

Lingling Wu et al. [12] presented a paper that emphasizes a new anti Arnold transformation algorithm against using periodicity to get anti Arnold transformation algorithm which wastes a lot of time. Contra matrix is used in this approach to get anti Arnold transform. This can work on MxN image too. In this approach there is no need to compute period of image.

Ruisong Ye [23] presented image scrambling along with watermarking scheme based on orbits of Arnold transformation. In this paper each pixel position is disordered by orbit of Arnold transform. With help of chaotic map, initial position of orbit of transform is got. Chaotic map shuffles pixel position of image and scrambled image is used to disorder host image in watermarking to ensure high security. Experiments show that this approach possesses good scrambling effect. Gray difference and Gray degree (GDD) is calculated that evaluates scrambling degree of concerned image. Compared to traditional one good scrambling degree is achieved and watermarking image is robust against attacks as well

Zhenwei Shang et al. [33] team presented an improved Arnold transformation by adding two parameters a, b with help of logistic map to generate parameter sequences. First digital image is made blocked then Arnold transformation is applied with different parameters on each image block. This way it achieves good scrambling effect and has large key space. Correlation analyses of adjacent pixels are implemented to analyze scrambling effect.

Congli Wang et al. [3] presented an evaluation method of image scrambling degree based on adjacent pixels where, formula for gray difference and block uniformity analysis is proposed on a 256x256 gray scale image. Arnold transform is applied and a correlation plot of two adjacent pixels in horizontal direction is provided to analyze distribution of pixels before and after scrambling. Afterwards gray difference and mean square deviation of block uniformity is obtained and scrambling degree graph for 2D Arnold transform, 3D Arnold transform and BLP is plotted and concluded that 3D Arnold produces better scrambling effects than 2D Arnold transform. One biggest advantage of these new methods is that it can be carried out by only using a small part of cipher image's data without any knowledge about plain image.

Xiongjun Li [32] presented a paper on measurement of image scrambling degree based on gray level difference and information entropy where, a new normalized

measure on image scrambling degree based on gray level difference and general entropy is provided. Image is scrambled by Arnold transform and sub affine transform and a compound scrambling method based on chaotic maps shows that new measure has better consistency. A more effective image scrambling degree measure based on these two parameters are shown on different gray scale images, and scrambling degree curve for Arnold transform, Sub affine transform is provided, and concludes that it represents more effective normalized measure of image scrambling degree, based on gray level difference and general entropy which combines three aspects of an image i.e. the discreteness, uniformity in discreteness, scrambling randomness in statistical distribution of image.

Tan Yongjie et al. [27] presented a paper on evaluating scrambling degree based on gray relation where, a new evaluation method of image scrambling is proposed. The definition and features of ideal image scrambling are discussed and then scrambling image is divided into sub images to make some histogram sequences. Finally, gray relevancy of every two sequences are calculated using gray relation analysis. Magic, Arnold, Hilbert, BitXor transforms are used for scrambling and scrambling factor, by the proposed method and SNR methods are presented and compared. Further, a conclusion is made about this proposed scheme that compared to method based on SNR the method proposed is not only efficient, flexible, running without involving original image but also produces better scrambling effects.

While understanding biological evolution and self reproduction, Von Neumann decided to create model for a self-reproducing machine. It is a theoretical machine consisting of cells (homogeneous). Each cell has a state among number of possible states. Each cell's state at next time step is a function of states of its neighbors at current. Cellular automata's cells evolve in discrete time steps according to applied rule [5,17]. Each cell consists of a D-FLIP FLOP (storage element) and combinational logic (CL) which implements next state function. Most fundamental is one dimensional cellular automata in which only horizontal neighbors are concerned but in 2-D cellular automata horizontal as well as vertical neighbors are concerned, 3-D cellular automata takes 3D Cartesian plane. Till now human couldn't go more than three dimensional planes [11]. Figure 2.1 shows a cell of cellular automata [4].

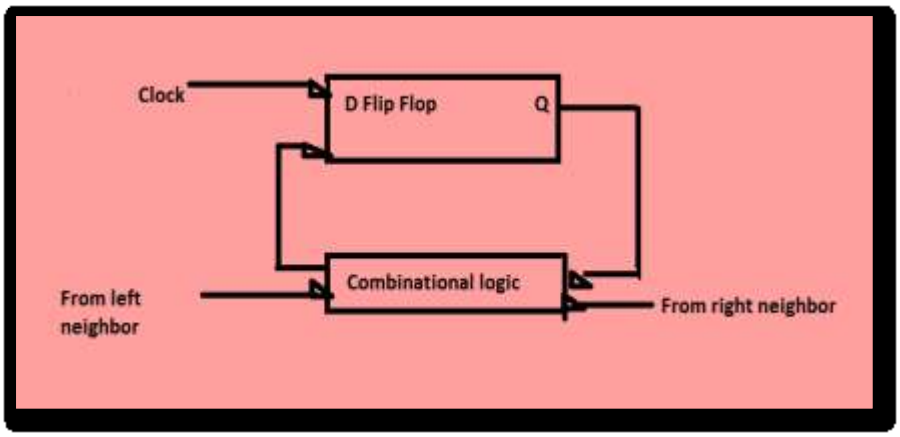


Figure 2.1: A cell of cellular automata

Cellular automata is an infinite array of dimension d, which consists of identical cells identical cells pointed out by Z^d. Each cell belongs to a Finite State Machine (F.S.M) P= (S , δ).

Where :- S is a set representing finite states.

δ is a mapping which represents-

δ: $S*S^h$ "h" is number of neighbors of each cell.

Cellular automata is a regular lattice of infinite dimension consisting of finite state machine which changes their states synchronously (with time), as per a local rule that corresponds to new state of every cell being updated based on previous states of their neighbors and also itself sometimes. On 1D array which consists of *C* consecutive cells, each cell *i* (*i* = 1, 2,. . . ,*C*) can take a particular number of states that is finite i.e. C. At every time step *t,* upcoming state of a cell is being calculated based on its present state as well as local neighbor's present state. In general, state φ*i* is a function at time *t* + 1 based on its 2**k* + 1 neighbors here it means *k* cells are on the left of cell into consideration and *k* cells are on right of it. Here *k* represents radius of cell's neighborhood. The total number of possible permutations for *m* finite states having a radius of *k* is *p* = *m*^(2**k*+1), so to calculate state of cells at next time step with number of all possible rules is *m***p*, which is generally quite big value. Basically, cell's next state at next time step is a function of state of its neighbors, the function can be either linear or of nonlinear type. Subclass of possible rules exists if we talk about cellular automata, as per those rules new state of cells are dependent on sum of the states in their neighborhood only. In this sort of updating rules, for considering m states the number of probable permutation for 2**k* + 1 neighbors is *m*(2*k + 1), hence, number of total possible rules that can be configured will be *m***m*(2**k*+1). For example if we input *m=5 and k* = 2, then here number of possible rules will come

out to be 515 = 3.05 × 1010, which is very less as compared to 5125. This way it represents subclass of totalistic rule or sub-rule which is especially important in famous cellular automaton like Conway's Game of Life, and in the cellular automaton based on partial differential equations (P.D.E). This Game-of-Life is most widely known amongst them which was introduced by John Conway. It is a two-dimensional cellular automata where, each cell is thought of as a square with two possible states, "alive" or "dead", if alive then represented by white square box otherwise for dead black square box. According to local update rule it is being asked from each cell their present state and state of their eight neighbor cells. For a live cell it stays alive (survives) if and only if it has two or three alive neighbors, otherwise it is dead because of loneliness or overcrowding. A dead cell becomes alive if and only if it has exactly three live neighbors. This rule is applied simultaneously to each cell. As the process is repeated over and over again, a dynamical system is obtained that persists amazingly complex behavior. There are different sort of cellular automat to ease the designing and modeling of complex systems.

If cellular automata rules involve using XOR logic only then it is called linear rules. A cellular automata having all cells linear is called linear cellular automata. In linear cellular automata, next state rule applied to each cell uses operation of Galois field GF. A linear cellular automata is also called as GF (q) cellular automata where q is a prime number. If cellular automata rule evolves using only XNOR logic then it is called Complement rules. A cellular automaton having all cells Complement rules is called Complement cellular automata. A cellular automata with combination of XOR and XNOR logics in its rules is called Additive cellular automata. They produce algebraic tools that characterize Additive cellular automata and helps in developing applications in VLSI testing field. Additive cellular automata are based on easily testable FSM, bit-error correcting code, byte error correcting code, and characterization of 2D cellular automata. Additive cellular automata are also used in universal pattern generation, data encryption, and synthesis of easily testable combinational logic. Additive cellular automata based tools are used for fault diagnosis, and a large variety of applications to solve real-life problems. A cellular automata is said to be Programmable cellular automata if it employs control signals. With specification of values of control signal time, programmable cellular automata can explore various functions dynamically. A cellular automata is reversible cellular automata in the way that the cellular automata will return to its initial state always.

Interesting thing about being reversible that means that not only forward but reverse iteration is also possible. Using Reversible rule it is always possible to return to an initial state of cellular automata at any point. One Rule is used for iteration and another rule, reversible to the first one, is used for backward iteration. This type of cellular automata is used in cryptography. In non linear cellular automata we use cellular automata with all possible logic. Apart from this a non linear cellular automata is a powerful pattern recognizer. It is special type of cellular automata, referred as GMACA (Generalized Multiple Attractor Cellular Automata), is implemented for the design. The desired cellular automata model, evolved through an efficient implementation of genetic algorithm, is found to be at the edge of chaos. Cellular automata are mathematical idealizations of complex systems in discrete space and time A Fuzzy cellular automata means cellular automata using fuzzy logics. Application area of fuzzy cellular automata is pattern recognition. It is a special class of cellular automata referred to as Fuzzy cellular automata (FCA) is employed to design the pattern classifier. In simple, cellular automata can handle only the Binary Patterns. In Fuzzy cellular automata, each cell assumes a state and a Rational Value in [0, 1]. If we develop Hybrid System using cellular automata then it is the combination of cellular automata, neural network and fuzzy set or the combination of cellular automata, Fuzzy set and Rough set. A Uniform cellular automata is one that if all cells follow same rule, then the cellular automata is called a Uniform cellular automata.

A Hybrid cellular automata is one that if all cells follow different rules, then the cellular automata is said to be a Hybrid cellular automata The hybrid cellular automata is been especially applied in a linear/additive cellular automata in which the rule set can be analyzed through matrix algebra [4, 17].

A cellular automata is called a null boundary cellular automata if both the left and right neighbors of the leftmost and rightmost terminal cells are connected to logic 0. One-dimensional (1D) cellular automata (CA) over finite fields are studied in which each interior (local) cell is updated to contain the sum of the previous values of its two nearest (left & right) neighbors along with its own cell value. Boundary cells are updated as per Null boundary rule. In Periodic Boundary cellular automata the rightmost cell behaves as the left neighbor of leftmost cell. Similarly, the leftmost cell behaves as the right neighbor of rightmost cell. So, it is like a circular linked list data structure cellular automata and for 2D other than left and right neighbors top and bottom cells also considered. Here, the bottom cell behaves as neighbor of top cell

and top cell as neighbor of bottom. So it becomes something like a toroid. In Reflective Boundary cellular automata the boundary values reflect same value as that of left most cells and right most cells in 1D cellular automata but in 2D cellular automata other than left and right, top and bottom cells are also considered so for them, top cells of boundary reflects values of top most cells and cells of bottom boundary reflects values of bottom most cells. In this way the cells states at the extremities are repeated in order to provide neighboring cell values for them. A Fixed Boundary cellular automata is used where we require boundary values to be fixed values such as while modeling a problem in heat conduction. Thus values along boundary remain constant throughout the simulation in fixed boundary condition [11].

CHAPTER 3

PROBLEM STATEMENT

3.1 Encryption

In the earlier part we have discussed that in this computer era most of the data or information is transferred between distributed systems or within in a network using internet. So here the security of data is primary concern. There are lot of technologies which are used to secure the data between one end to other end like MD-5, ECC algorithm and RSA algorithm using cryptography. Images are great carrier of information for information interchange over internet, with its continuous growth. For sake of secure transmission of any multimedia encryption technologies are used widely. Conventional encryption techniques have many disadvantages such as the structure complexity, the secret key singleness and the slow encryption speed, other than this it is difficult to meet all security measures for images that consist of lots of data. So we can see, for today's world where invading data is very easy while transmitting it for communication purposes [20, 21].

Traditional encryption has following pitfalls which makes it less efficient.

- Conventional encryption scheme is good as far as safety is concerned but not excellent and effect of encryption is not good. It is now possible to decipher encryption algorithm easily because the conventional cipher algorithm only encrypts image by simply treating their information and data stream as usual data stream. So, they can be broken very easily and actual information will be leaked. If it is a confidential data it must be provided strict security. Hence, it does not satisfy people's normal requirement [29].
- The traditional encryption scheme is quite time consuming and costly.
- Some encryption programs are too complicated for the everyday user and they may end up using them incorrectly. This could lead to securing data which they did not wish to encrypt or failing to encode data which they did wish to protect.

3.2 Types of Encryption

There are two types of encryption techniques one is Symmetric key encryption and other is Asymmetric key encryption, which is described below. Both schemes uses key at sending and receiving end to protect data.

3.2.1 Asymmetric Key Encryption

Asymmetric key encryption takes data encrypts it and decrypts it at other end but, at both ends it uses different keys. It encrypts using public key and decrypts using private key. Public key is shared but private key is kept protected. Figure 3.1 shows asymmetric encryption technique.

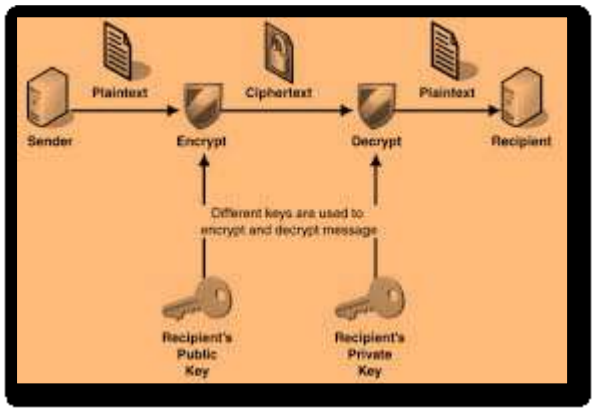


Figure 3.1: Asymmetric encryption technique

3.2.2 Symmetric Key Encryption

Symmetric key encryption takes data encrypts it and decrypts it at other end by using same key for encrypting and decrypting. The key is a string of data if, it is random it performs better. It is faster method. We have used Symmetric key encryption also called as scrambling. Figure 3.2 shows symmetric encryption technique.

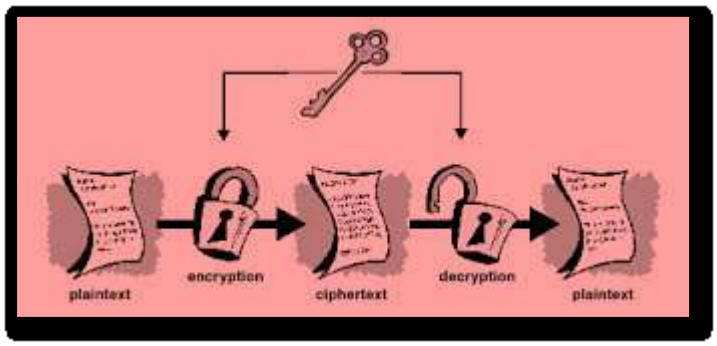


Figure 3.2: Symmetric Key Encryption

3.2.2.1 Arnold Cat Map

It changes position of pixels in image and hence breaks relationship of adjacent pixels of image and creates chaos all over the image so the image doesn't remain what it was originally. A matrix transform is used for producing noise all over image using modified Arnold Cat Map that is given by Eq. (3.1) [15].

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } N) \quad (3.1)$$

Here, (X, Y) is current position of a pixel, (X', Y') is new positions of same pixel after application of above mathematical formula for a particular number of time. N is dimension of image

3.2.2.1.1 Disadvantages of Arnold Cat Map

- Arnold Cat Map is restricted only to square images i.e. they can't be used on rectangular images as per the algorithm. We today require an algorithm that can work upon any shape and size of images, in which Arnold Cat Map is a failure [16].
- Arnold Cat Map has a disadvantage of being periodic in nature. After certain number of rounds it comes to its original state i.e. what original meaningful information was. So it is very easy for anyone to take advantage of this property and just by repeating number of iterations they may invade the scrambled information. We need an algorithm for scrambling our information that is secure from being periodic in nature and hard to be descrambled [20].

Due to some limitations associated with Arnold Cat Map another technique is required which doesn't possess these demerits and other than this, performs more effectively on scrambling than Arnold Cat Map.

CHAPTER 4
PROPOSED SOLUTION

Some typical image encryption methods can't meet demands of high security because of lack of security measures. This imposes some action to be taken to provide a secured way of sending images to other person as they may contain confidential information or some private contents. To provide a solution for above problem we send scrambled images from sender to receiver rather original image. With help of different scrambling techniques different scrambling effects can be created and at receiving end descrambling is performed and actual meaningful image is retrieved. For better security, a scrambling technique can be combined with any traditional encryption methods. So before encrypting, images are first scrambled and then encrypted with encryption algorithms. Here, we are using two different types of scrambling techniques i.e. Arnold Cat Map scrambling and scrambling by Conway's Game of Life algorithm, regarding both an algorithm is provided in this section as well as we provide different scrambling parameters that evaluates degree of scrambling to evaluate which method performs better on these parameters, they are actually some mathematical functions to evaluate effectiveness of scrambling and analyze the results based on them.

4.1 Scrambling

Scrambling is a technique of creating chaos in image and let it not be what it used to appear originally [16, 25]. Positions of all pixels of an image are disturbed and they are displaced to some other position than their current location with help of some mathematical transformations. In this way we send disturbed format of image rather than actual image for secured transmission [23, 29]. Here we work on two different type of scrambling techniques and compare their effectiveness with help of some parameters. Below we present algorithm for scrambling and descrambling by Arnold Cat Map and 2D Cellular Automata (Conway's Game of Life) proposed by other authors and then we present an algorithm for combining these two scrambling techniques that improves performance parameters and overcomes demerits associated with above two methods. Figure 4.1 shows scrambling and descrambling procedure of an image where symmetric encryption is used and same key is used at sender and receiver ends.

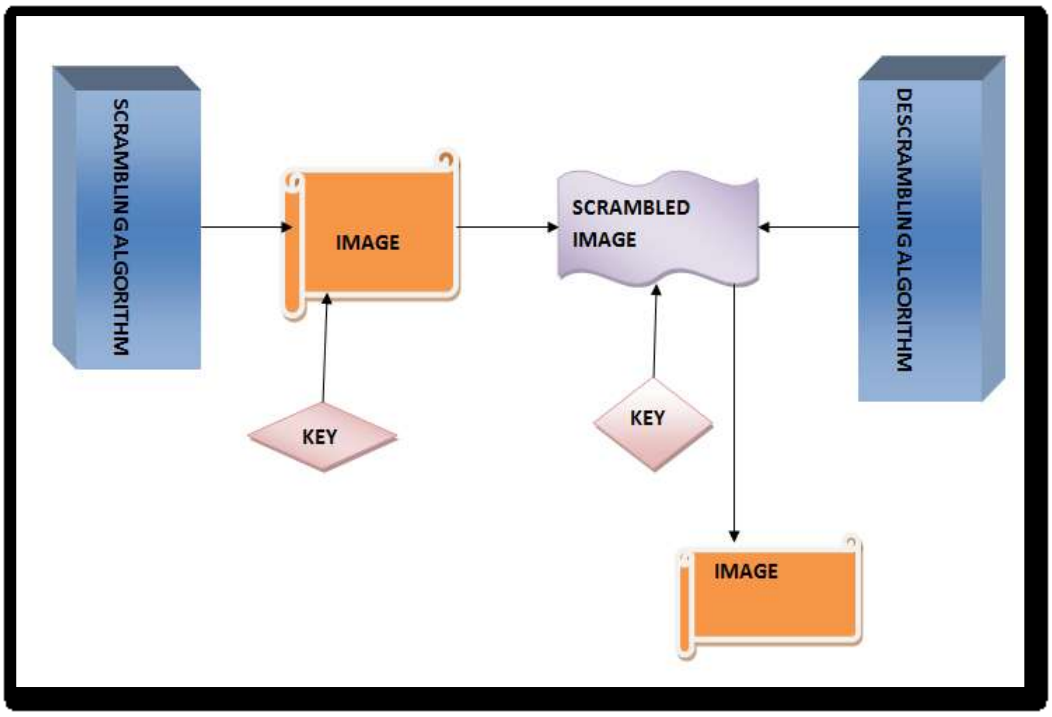


Figure 4.1: Process of scrambling and descrambling in image

4.1.1 Arnold Cat Map Scrambling and Descrambling Algorithm

Algorithm for scrambling and descrambling proposed by Gabriel Peterson [7] is as follow.

1. First read the NxN image and convert it to gray scale image IMG. For a particular number of rounds that works as key repeat until transformed image become equivalent to original image that we have taken.

   A. Calculate the new positions of each and every pixel of image IMG by modified formula of Arnold transform given by Eq. (4.1).

   $$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{Mod } N) \qquad (4.1)$$

   Here, i € (1, 2, 3…..). X', Y' is new position of pixel and X, Y are current position of pixel, N is dimension of image.

   B. Put current pixel at new position calculated, in a new matrix vector for it and do it for all pixels of entire image IMG.

   C. If numbers of rounds become equal to that number for which we want to perform scrambling on image, then show the transformed image at this point of time, this is our scrambled image.

   D. Increment number of rounds each time by 1.

2. When transformed image becomes equivalent to original image at that point of time stop processing. This time number of rounds will give the period of our image for which scrambled image becomes equivalent to original image.
3. Show the transformed image now it will be our descrambled image IMG′.

We have used the periodic nature of Arnold Cat Map here, to get the descrambled image although inverse matrix transform is another method to get the descramble image. Arnold Cat Map is periodic in nature after some iterations called period of image it comes to its original status and each pixel automatically comes to its proper position as in original image, so by using periodic nature of Arnold's transform we can descramble our image after scrambling as after some evolutions it automatically comes to originality.

4.1.2 Game of Life Scrambling and Descrambling Algorithm

Scrambling with Game of Life overcomes problem associated with Arnold Cat Map like it doesn't has periodicity property and it can work on square as well as rectangular images too. Further, for sophisticated system Game of Life has performed so well previously so complex systems where Arnold Cat Map may fail Game of Life of 2D Cellular Automata will perform well.

To scramble by Game of Life proposed algorithm is given by Mr. Fasal Qadir [6] we scramble and descramble by Moore and Vonneumann both with help of following algorithm.

1. First read an MxN image that is to be scrambled and then convert it to gray scale as we have to perform experiment on gray scale image.
2. Create a random array of rows and columns respectively M and N, which stores random binary values in it call it BIN_INIT this is used to produce an initial state of each and every pixel at time t=0.
3. For a particular number of rounds for which we want to apply scrambling algorithm repeat.
   A. Apply Moore neighborhood or Vonneumann neighborhood formula to calculate sum of current states of neighbors of current pixel.
   B. Check this sum according to Game of Life's rule, if sum is greater than 1 or less than 4 the next state of current pixel will be 1 i.e. live cell remains live, if sum is exactly 3 a dead cell becomes alive, otherwise a live cell becomes dead.
   C. Store next state of each cell in a 1D binary array NEXT_STATE.

D. Now for all live cells having value 1 take out their gray value and store sequentially in a separate array and same for cells having value 0 put it in another array.

E. Concatenate both arrays now this is our scrambled image.

4. To descramble the image reverse steps of scrambling technique is applied.

This way we scrambled and descrambled by both Moore and Vonneumann neighborhood and further we have compared all these above scrambling techniques that, which is better for which scrambling degree measurement parameter. Graphs and tables for observation obtained are plotted and provided in next chapter.

4.2 Scrambling Degree Measurement Parameters

Image scrambling techniques are studied in large extent these days. Currently image scrambling is not only used for encryption purposes but also used while pre processing and post processing for watermarked images. A great number of research is employed to achieve good encryption techniques, but study of ways to evaluate scrambling degree to ensure effectiveness of scrambling is somewhat lagging behind comparatively. To evaluate effectiveness of scrambling we use some parameters in this research paper. Scrambling degree is used to evaluate advantages and disadvantages of scrambling techniques. Generally, if the scrambling degree of scrambled/encrypted image is high this simply means higher security. So, scrambling degree measure is therefore is of great importance. Here, we are focusing on gray difference degree (GDD) and correlation coefficient. In our research a comparative study between Arnold Cat Map and cellular automata's Game of Life is carried out.

4.2.1 Gray Difference and Degree (GDD)

Gray difference and degree is combination of gray difference and gray degree. First we calculate gray difference for each pixel of image then we use it to calculate gray degree of image. Gray difference of an image is calculated by Eq.(2)

$$GD(i,j) = 1/4 \sum_{i,j}[G(i,j) - G(i',j')]^2 \quad (4.2)$$

Where, GD(i, j) is gray difference of current pixel (i, j). G(i, j) is gray value of current pixel (i, j) and G (i', j') is gray values of neighbor pixels (i-1, j), (i+1, j), (i, j+1),(i, j-1) of current pixel (i, j).After computing gray difference of each and every pixel in image except pixel's of boundary we can calculate an average gray difference for entire image by summing and then averaging by formula given by Eq.(3).

$$E\big(GD(i,j)\big) = \sum_{i=2}^{M-1} \sum_{j=2}^{N-1} \frac{GD(i,j)}{(M-2)(N-2)} \quad (4.3)$$

E(GD(i, j)) is average gray difference of whole image of dimension MxN and GD(i, j) is gray difference of current pixel (i, j). Now we need to calculate gray degree of image by using two formulas mentioned above. The gray degree is defined by Eq.(4.4).

$$GDD = \frac{(E'(GD(i,j)) - E(GD(i,j)))}{(E'(GD(i,j)) + E(GD(i,j)))} \quad (4.4)$$

Where $E'(GD(i,j))$ is average gray difference of scrambled image and E(GD(i, j)) is average gray difference of original image [1, 8]. GDD is a parameter to evaluate scrambling effect and it lies in [-1, 1] and a GDD close to '1' represents better scrambling effects. As we have used gray value of pixels while calculating GDD let's define gray value of a pixel [24].

4.2.1.1 Gray Value of a Pixel

Each pixel of an image represents a value which describes how bright that pixel is i.e. intensity of a pixel. For gray scale image pixel value is an integer value that represents brightness of a pixel. For most of the images gray value ranges from 0(Black) to 255(white). Maximum gray value of an image depends upon depth of image. For 8 bit image it is 255.

4.2.1.2 GDD Significance

- Greater the value of GDD (gray difference and degree) implies effective scrambling. More it is closer to '1' more it tends toward ideality. So if we are comparing two scrambling techniques the one with greater value of GDD represents better way of scrambling comparatively. Effective scrambling implies security, robustness and makes it hard to be descrambled.GDD (gray difference and gray degree) varies between [-1, 1].
- It provides measures for uniformity of a scrambling technique. In any meaningful image the pixel values of neighbors are correlated i.e. their difference will be small but if we scramble the image then in a good scrambling mechanism the difference of pixel values with its neighbors will be high as they were not originally their neighbors. This way we can evaluate uniformity of scrambling technique using GDD.

4.2.2 Correlation Coefficient

Correlation coefficient is an important parameter of evaluating scrambling degree. It is based on gray value of adjacent pixels of current pixel. It tests gray relation of adjacent pixels in cipher image. In any meaningful image correlation of adjacent

pixels will be high but this strong correlation will be broken when image is scrambled [3]. More the value of correlation is closer to '0' between original and scrambled image implies more effective scrambling is done. Correlation coefficient equal to '0' is ideal scrambling condition between scrambled and original images. Range of correlation coefficient varies in [-1, 1]. Here, a (+1) implies that scrambled image is very similar to original one. A (-1) implies that scrambled image is a negative to original image and just by inverting it we can get original image. A '0' implies there is no relation between scrambled and original image and they are not at all correlated [1]. How a correlation coefficient is measured can be understood by Eq. (4.5).

$$R = \frac{\sum_m \sum_n (A_{mn} - A')(B_{mn} - B')}{\sqrt{\sum_m \sum_n (Amn - A')^2 \, (Bmn - B')^2}} \quad (4.5)$$

Here, R is correlation coefficient, mxn is size of image, Amn, B_{mn} are gray value of original and scrambled images respectively of pixel position at m, n. A', B' are mean gray value of original and scrambled images respectively. If we apply correlation coefficient between original and descrambled image then it will give us a glimpse of how much distortion is employed in descrambled image compared to original image. Here, no noise is introduced in image so, correlation between original and descrambled Image will be '1'.

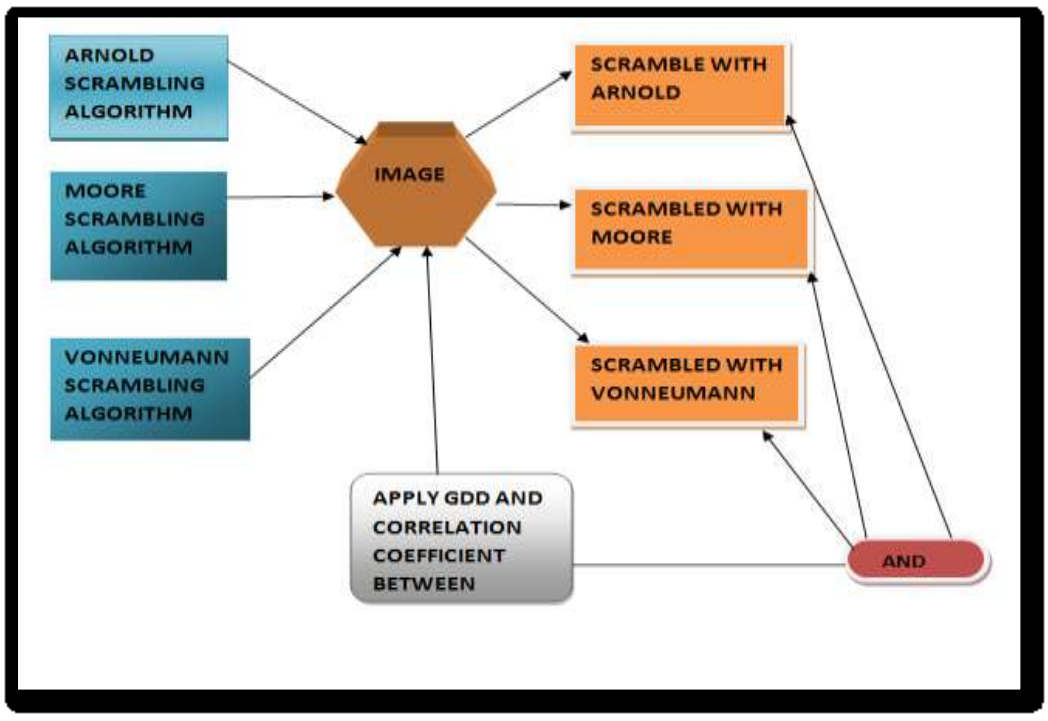


Figure 4.2: Applying scrambling degree parameters between original and scrambled image

4.3 Algorithm of Arnold Concatenated With Game of Life Transform

Here, we present an algorithm for combining Arnold and 2D cellular automata for scrambling and descrambling of image for better scrambling effect.

1. Take an NxN grayscale image IMG and apply Rules of Game of Life by considering Moore neighborhood for one experiment and also by considering Vonneumann neighborhood for other experiment. Apply algorithm of scrambling image by Game of Life provided by Mr. Fasal Qadir [6] once which gives scramble image IMG′.
2. For a particular number of key specified, mostly taken as input by user, for how many times they want to scramble the image do the following.
   A. Scramble the image IMG′, iteratively for a particular value of key by Arnold Cat Map algorithm provided by Gabriel Peterson [7]. This finally is our scrambled image IMG".This is actual, final scrambled image.
   B. Repeat step A until we get the same scrambled image we input after applying Game of Life scrambling technique once.
   C. If we get condition B, this implies that we have descrambled our image form Arnold Cat Map.
3. Apply reverse of scrambling technique by Game of Life once.
4. This image is our finally descrambled image.

4.3.1 Merits of Combined Technique

- After combining Arnold Cat Map and Game of life technique the demerit involved with periodic nature of Arnold Cat Map is removed that even after applying Arnold Cat Map for particular number of iterations one will never be able to get original information just by repeating the algorithm.
- Scrambling degree parameter of this technique rises high and performs better as far as GDD is concerned. We have applied Game of Life just once and for specific number of iterations we used Arnold Cat Map, still GDD rose higher than the method where we applied Game of Life for many iterations. As Game of Life performs much better than Arnold transform still by applying Game of Life just once and Arnold transform for a particular number of iteration, the combination performs better than Game of Life alone.

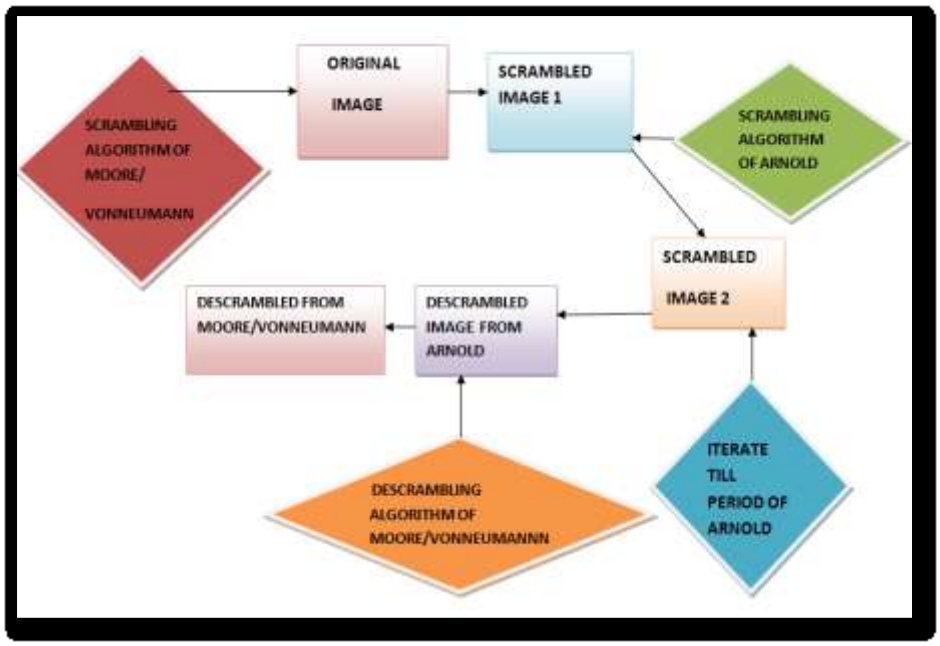


Figure 4.3: 2D cellular automata concatenated with Arnold

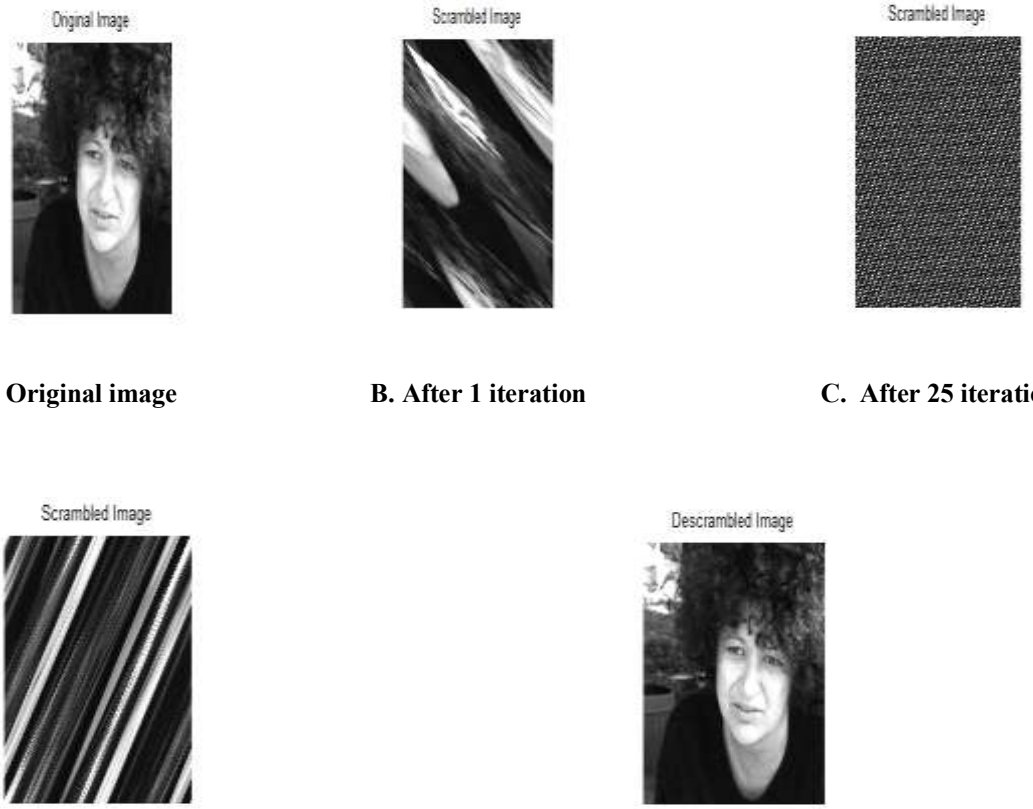
This way we have produced combined effect of scrambling by using combination of Arnold Cat Map and Game of Life transform for both type of neighborhood i.e. Moore and Vonneumann. Combined effect of both neighborhoods along with Arnold transform is compared that which combination is more effective and they are compared to the one technique that was best while scrambling individually by Game of Life's both variants and Arnold transforms. Graphs and tables regarding scrambling parameters are provided in next chapter.

CHAPTER 5

EXPERIMENTAL OBSERVATION

5.1 Arnold Cat Map

Various scrambling techniques have been proposed till now among them Arnold Cat map is widely accepted for its simplicity. We have applied Arnold scrambling algorithm on a 172x172 gray scale arbitrary image. First scrambling of original image is done which gives output as shown in Figure 5.1 for different iterations and graphs for scrambling degree parameters like GDD and correlation coefficient are presented in Figure: 5.2 and Figure: 5.3 for Arnold.



A. Original image **B. After 1 iteration** **C. After 25 iterations**

D. After 130 iterations **E. After 132 iterations**

Figure 5.1: Results of scrambling and descrambling by Arnold cat map

We can see that in Arnold scrambling technique after iterating scrambled image for 132 iterations original image is obtained as this transform has periodic property which is a security risk. To solve this problem associated with Arnold transform we have taken 2D cellular automata to perform scrambling.

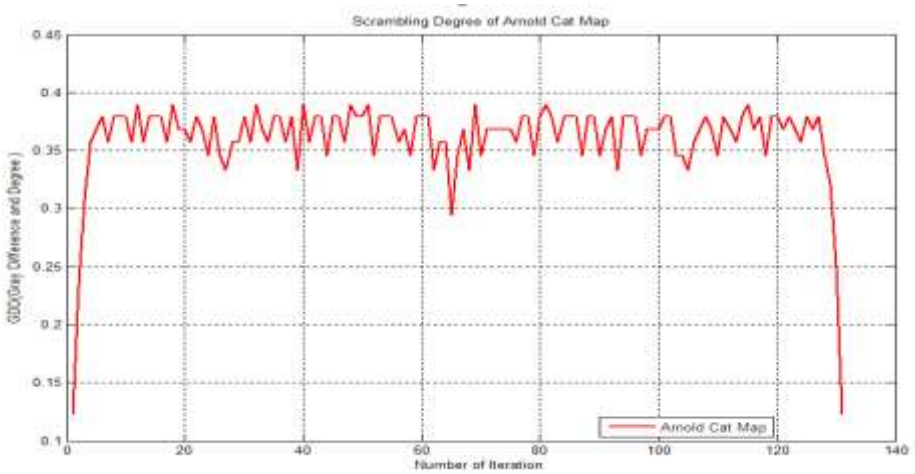


Figure 5.2: Graph of GDD for Arnold cat map

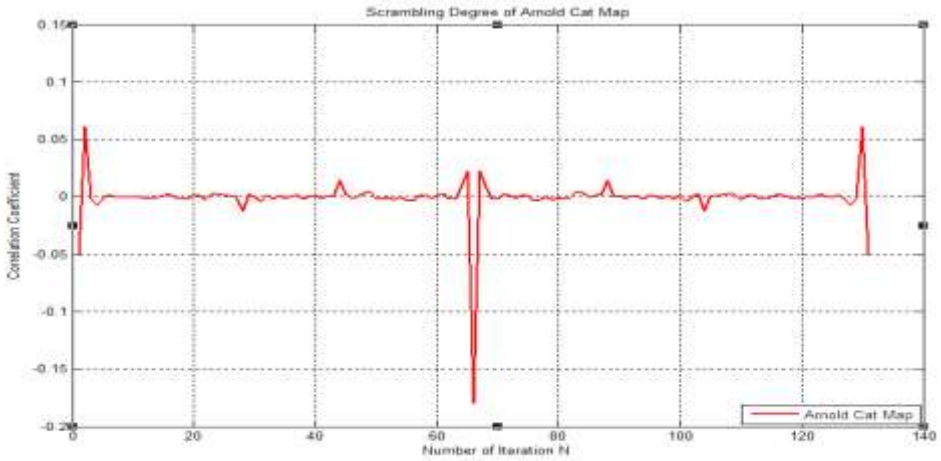


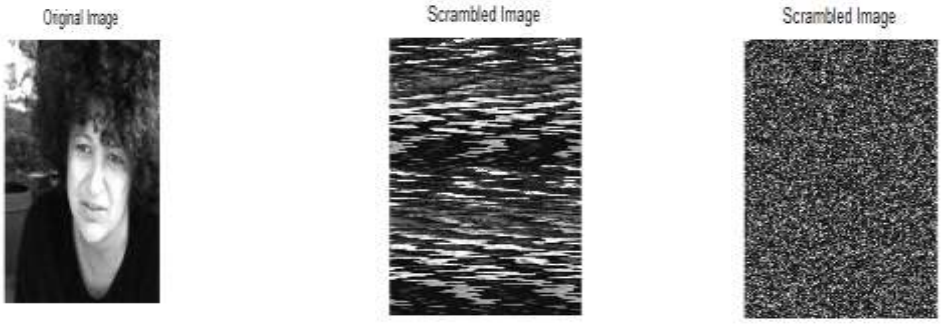
Figure 5.3: Graph of Correlation Coefficient for Arnold cat map

Here, we can clearly see by above outputs that with each number of iteration a different sort of scrambled image is obtained which doesn't give glimpse of actual image. Hence, no one can guess by observing scrambled image what it actually consists of, which certainly promises increased security than encryption. We can also observe the periodic nature of Arnold Cat Map that the period of this image is 132 so, as the number of iteration is coming closer to its period scrambled image comes closer to original image as iteration 130 shows. On number of iteration 132 because of periodic nature of Arnold Cat Map the scrambled image comes to its originality and becomes exactly equivalent to original image which is our descrambled image. To descramble the image only an authorized person is liable to do so and if given descrambling algorithm and keys then, he will be able to get the original image. The keys here are, number of iterations and constants of Arnold transform. Arnold

transform has some limitations as discussed in chapter 1 so we need a better and more secured way of scrambling, for that purpose we are using 2D cellular automata to scramble and descramble images.

5.2 2D Cellular Automata (Game of Life)

Cellular automata is used here for scrambling and descrambling the image on same image which was used for Arnold Cat Map because of its amazing results for complex systems and it works perfectly for images as well. The results of scrambling and descrambling by 2D cellular automata(Conway's Game of Life) for periodic boundary and for both its variants i.e. Moore neighborhood and Vonneumann neighborhood is as follows along with graphs of GDD, correlation coefficient.



A. Original image **B. After 1 iteration of Moore** **C. After 25 iterations of Moore**

D. After 130 iterations of Moore **E. After descrambling**

Figure 5.4: Results of scrambling and descrambling by Moore neighborhood

Figure 5.4 and shows that 2D cellular automata is free from periodicity property and just by iterating scrambled image we do not get original image. For descrambling we need a descrambling algorithm and all keys applied in the algorithm. In this way 2D cellular automata is better than Arnold Cat Map and ensures security while scrambling.

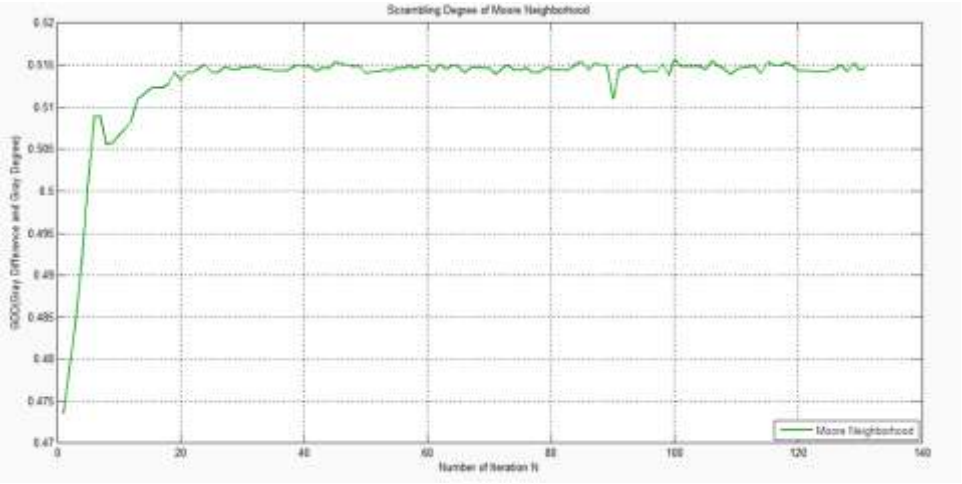


Figure 5.5: GDD of Moore neighborhood

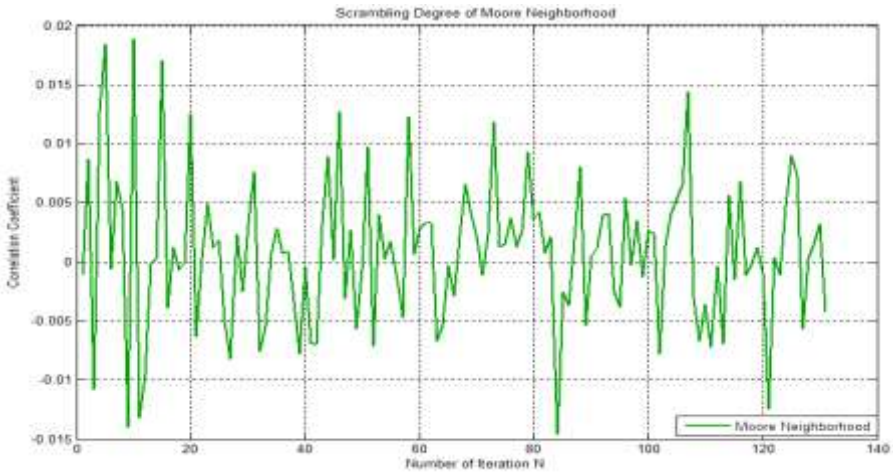
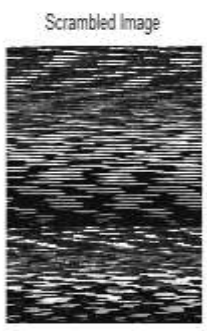


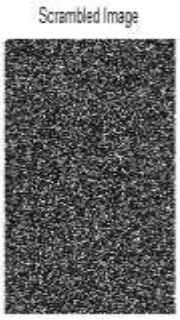
Figure 5.6: Correlation Coefficient of Moore neighborhood

Figure 5.5 shows that Moore scrambling is uniform as approximately parallel line to X- axis is obtained. Obtaining a parallel line to X-axis with Y axis value of 1 is ideal condition of scrambling.

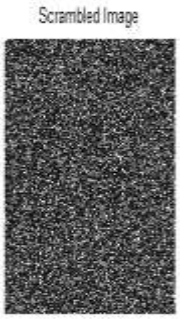
A. Original image



B. After 1 iteration of Vonneumann



C. After 25 iterations of Vonneumann



D.After 130 iterations of Vonneumann **E.After descrambling**

Figure 5.7: Results of scrambling and descrambling by Vonneumann neighborhood

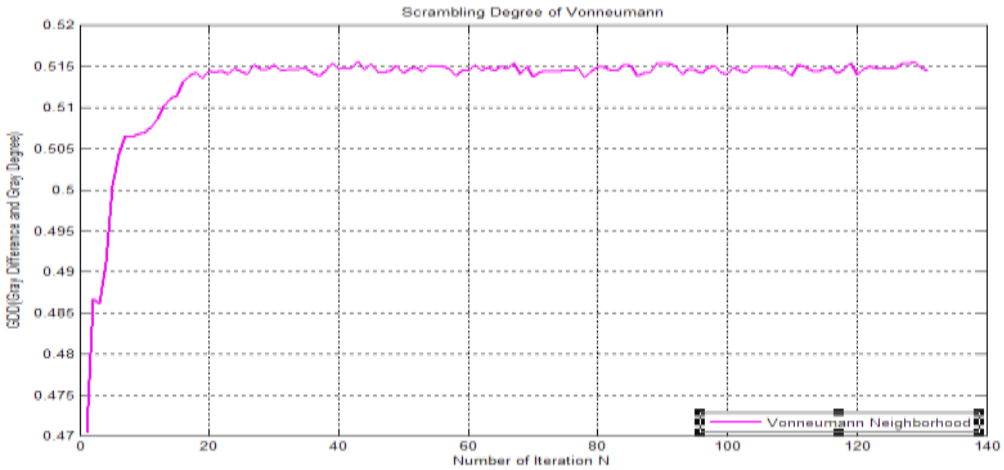


Figure 5.8: GDD of Vonneumann neighborhood

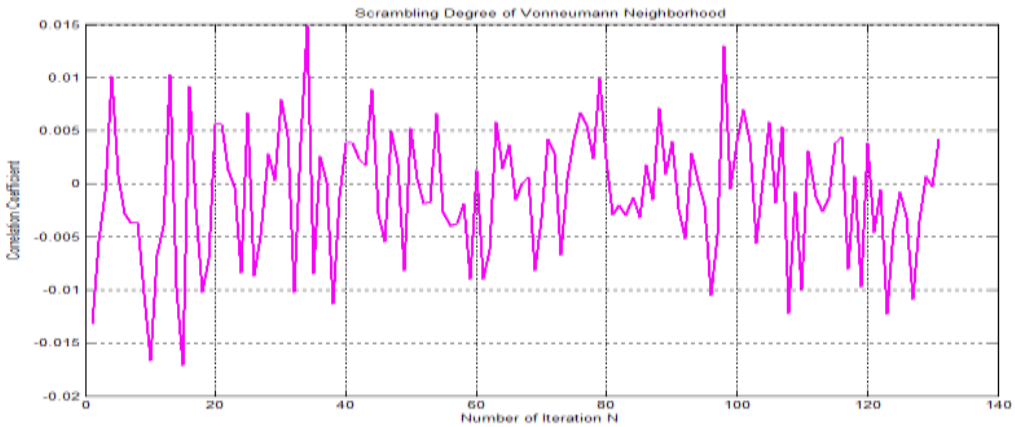


Figure 5.9: Correlation Coefficient of Vonneumann neighborhood

From Figure 5.7 results it is obvious that unlike Arnold Cat Map, Game of life's Vonneumann too doesn't possess periodic nature and as number of iteration comes closer to period of image i.e. 132 the scrambled image do not show closeness to

original image this solved one of the problem associated with Arnold and increases security. Both Moore and Vonneumann scrambles image quite similarly but still in a different way. Here, key is number of iteration.

5.3 Comparative Study of Parameters

Here, we present graphs and table for GDD, correlation coefficient for scrambling by each of the above techniques mentioned, for each iteration and compare what are the effects of which scrambling technique.

5.3.1 Comparative Study of GDD (Gray Difference and Degree)

Table 5.1 is presented for GDD obtained after experiment performed for 131 iterations, which majorly consists of those outputs which make some conclusions about research performed.

Table 5.1: GDD of Arnold, Moore, and Vonneumann scrambling techniques.

S.No.	Number of Iterations	Arnold Cat Map	Moore Neighborhood with Periodic Boundary	Vonneumann Neighborhood with Periodic Boundary
1	2	0.0234	0.4792	0.4768
2	3	0.3077	0.4844	0.4862
3	8	0.3793	0.5055	0.5065
4	10	0.3793	0.5066	0.5070
5	16	0.3793	0.5124	0.5132
6	**18**	**0.3898**	**0.5128**	**0.5143**
7	20	0.3684	0.5132	0.5145
8	30	0.3793	0.5148	0.5152
9	39	0.3333	0.5150	0.5154
10	**43**	**0.3793**	**0.5147**	**0.5157***
11	**45**	**0.3793**	**0.5154**	**0.5153**
12	51	0.3898	0.5142	0.5147
13	54	0.3793	0.5143	0.5151
14	61	0.3793	0.5142	0.5152
15	71	0.3684	0.5139	0.5143
16	**85**	**0.3793**	**0.5154**	**0.5151**

17	89	0.3793	0.5150	0.5153
18	90	0.3455	0.5110	0.5155
19	111	0.3793	0.5147	0.5152
20	**115**	**0.3898**	**0.5154**	**0.5148**
21	122	0.3793	0.5143	0.5150
22	128	0.3455	0.5142	0.5153
23	131	0.1220	0.5147	0.5145

Graph of GDD for all three above mentioned techniques is shown in Figure 5.10.

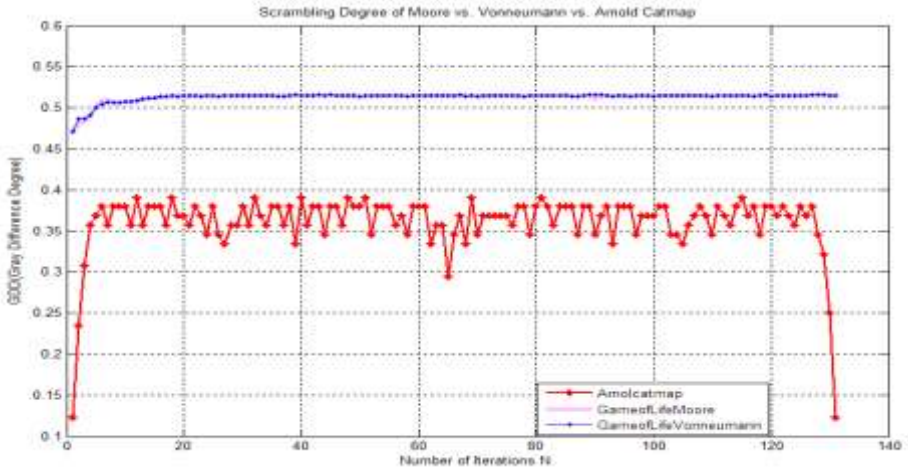


Figure 5.10: Comparative graph of GDD for Arnold, Moore and Vonneumann

We can clearly see by Figure 5.10 that GDD of Moore and Vonneumann is almost closer to each other and they possess a remarkably greater GDD than Arnold Cat Map although Vonneumann performs a bit better than Moore as far as GDD is concerned. For better scrambling greater GDD is required, that we get by 2D cellular automata. Game of Life has uniformity in scrambling while Arnold Cat Map has abrupt effects and it is not uniform. Moore reaches to 0.5154 at iterations 45, 85,115 while Vonneumann reaches 0.5157 at iteration 43 for GDD. So, it is clear that Vonneumann performs better for GDD amongst these three. As we know ideal GDD for scrambled image is '1'.

5.3.2 Comparative Study of Correlation Coefficient

Table for Correlation Coefficient obtained after experiment for 131 observations are given by Table 5.2 which, majorly concerns those outputs which make some conclusions. We are considering closeness to ideality and deviation from ideality too to conclude which technique possess better correlation coefficient.

Table 5.2 Correlation Coefficient of Arnold, Moore, and Vonneumann scrambling techniques

S.No.	Number of Iteration	Arnold Cat Map with Periodic Boundary	Moore Neighborhood with Periodic Boundary	Vonneumann Neighborhood with Periodic Boundary
1	1	-0.0520	-0.0011	-0.1320
2	**5**	**-0.0009**	**0.0184**	**0.000806**
3	6	0.0016	-0.0006	-0.0028
4	**11**	$\mathbf{3.0000e^{-05}}$	**-0.0132**	**-0.0067**
5	13	-0.0009	-0.0002	0.0103
6	**19**	**-0.0016**	$\mathbf{-4.0000e^{-05}}$	**-0.0071**
7	24	0.0024	0.0012	-0.0084
8	**34**	**0.0012**	$\mathbf{6.1000e^{-04}}$	**0.0149**
9	40	0.0011	$-4.2000e^{-04}$	0.0038
10	44	0.0139	0.0089	0.0089
11	**66**	**-0.184***	**-0.0029**	**-0.0015**
12	**67**	**0.0222**	**0.0022**	$\mathbf{3.6e^{-05}*}$
13	71	0.0027	-0.0011	0.0042
14	90	0.0009	$4.8800e^{-04}$	0.0040
15	97	-0.0011	$-2.5000e^{-04}$	-0.0048
16	112	0.0016	$-3.8000e^{-04}$	-0.0012
17	**121**	$\mathbf{3.0000e^{-05}}$	**-0.0125**	**-0.0046**
18	130	0.0609	0.0032	$-2.6000e^{-04}$
19	131	-0.0520	-0.0043	0.0042

Graph of correlation coefficient for all three above mentioned techniques i.e. Arnold transform, Vonneumann, Moore are plotted in Figure 5.11 to provide a comparative study to be made and derive some conclusions about their performances. Among them who ever performs best on a paticular scrambling degree parameter will be further comapared to new scrambling methodology's performance presented in this research work to find out whether new technique gives better performance than these trivial techniques or not.

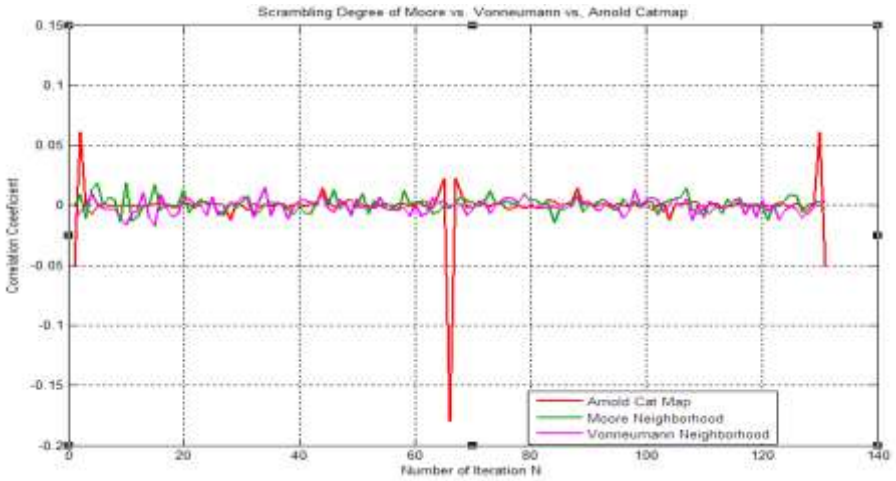


Figure 5.11: Comparative graph of Correlation coefficient for Arnold, Moore and Vonneumann

Correlation Coefficient should ideally be closer to '0' and varies between [-1, 1]. From Figure 5.11 it is obvious that Arnold Cat Map has suffered big deviations from ideality. At iteration 66 correlation coefficient goes to 0.184 and at iteration 130 it goes to 0.06 while maximum deviation from ideality in case of Moore neighborhood is at iteration 5 where correlation goes to 0.0184 which is remarkably lesser than Arnold's. Arnold and Moore both performs similar when matter of closer to ideality i.e. at iteration 11, 121 Arnold's correlation goes to 0.00003 while at iteration 19 Moore's correlation goes to -0.00004 which are approximately closer to each other. Here, most deviated and non uniform results of correlation is of Arnold which attains highest peaks as shown in above graph so we can say Moore performed with uniformity and most of the time its correlation lied below 0.0184 so overall Moore performed well on correlation than Arnold. Between Moore and Vonneumann, they both performed closer to each other when matter of deviation from ideality comes. Vonneumann at iteration 34 given correlation of 0.0149 against 0.0184 of Moore and, Moore attains closer to ideality (i.e. 0) as -0.00004, Vonneumann attains closeness to '0'at iteration 67 as 0.000036. So, overall Vonneumann has performed better by considering all points than Arnold and Moore. It is least deviated from ideality as well as closer to ideality i.e. '0'.

5.4 Concatenating Game of Life and Arnold Cat Map

We have applied Game of Life once on image and then Arnold Cat Map is used for scrambling the image for a particular number of rounds. This improves scrambling

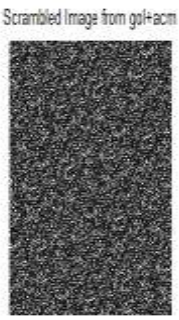
effect and performs even better than the case where Game of Life was applied for many iterations.

5.4.1 Arnold Concatenated with Moore Neighborhood

Here, Game of Life's Moore neighborhood is applied once on image for scrambling and then scrambled image is input to Arnold transform for a particular number of rounds called key and produces finally scrambled image IMG". Output of this combined effect is shown by Figure 5.12.

A. Original image

B. After 1 iteration of (Moore with Arnold)



C. After 25 iterations of (Moore with Arnold)

D.After 130 iterations of (Moore with Arnold)

E. Descrambled image

Figure 5.12: Results of scrambling and descrambling by Moore concatenated with Arnold

Figure 5.12 shows that this technique is free from periodicity property of scrambling technique and hence, just by iterating scrambled image original will not be obtained. This technique scrambles image with two methodologies so even if by iterating scrambled image if we are out of Arnold scrambling i.e. on its period, it is still scrambled with Moore scrambling technique so no one can decode the original information of image that we have to transmit. Here, by doing so we will see in upcoming section of this chapter that performance of Arnold improves because of using Moore in combination and it performs even better than 2D cellular automata

alone. GDD and correlation coefficient both gets improved than previously discussed methods.

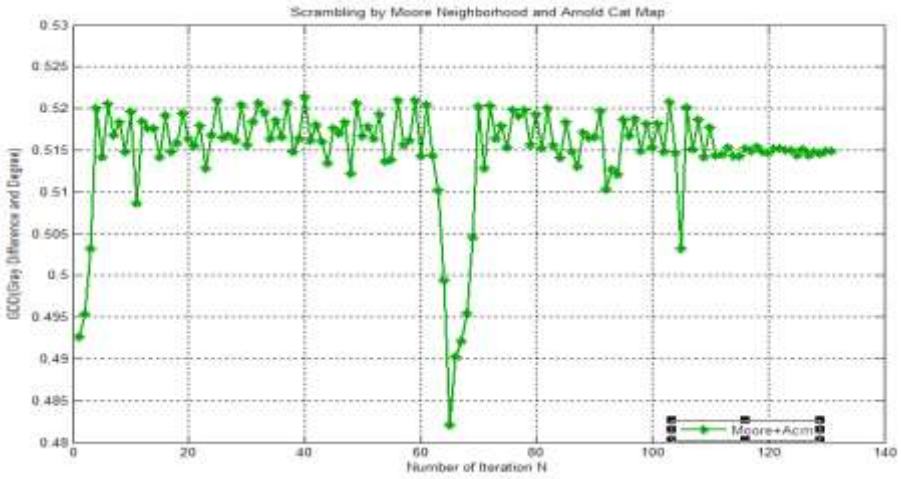


Figure 5.13: GDD of Moore concatenated with Arnold

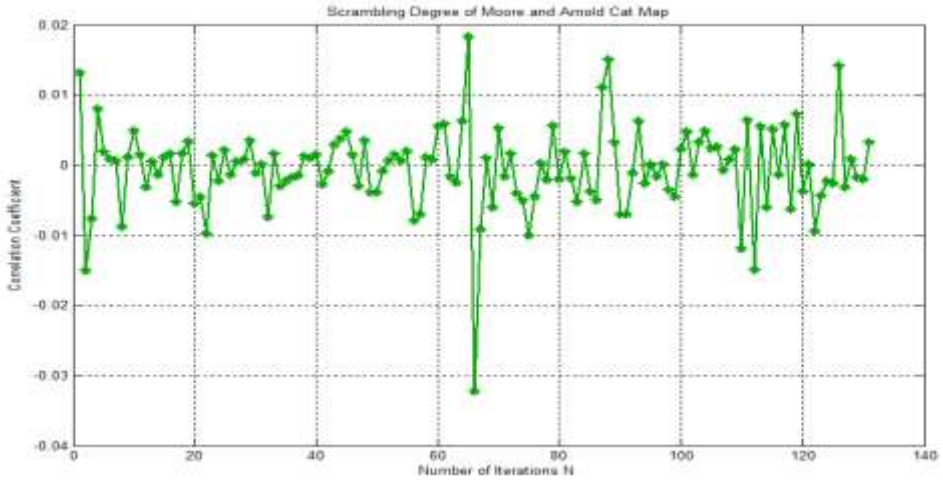


Figure 5.14: Correlation coefficient of Moore concatenated with Arnold

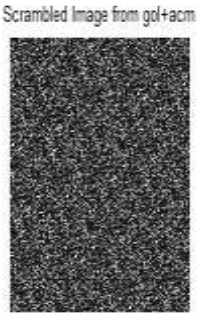
5.4.2 Arnold Concatenated with Vonneumann Neighborhood

Here, Game of Life's Vonneumann neighborhood is applied once on image for scrambling and then scrambled image is input to Arnold transform for a particular number of iteration called as key and produces finally scrambled image IMG". This technique of firstly scrambling through Vonneumann created a better randomness in image and then Arnold is applied for particular number of times, which eventually increases performance and provides better security that now by just iterating scrambled image no one is capable of descrambling it. This technique is not only away from periodicity property but performs best for correlation coefficient and improves it remarkably than other techniques discussed in this research work. After scrambling, descrambling of image is also done and scrambling degree parameters

are computed on scrambled image to determine scrambling effects. Output of this combined effect is shown by Figure 5.15.

A. Original Image

B. After 1 iteration of (Vonnemann with Arnold)



C. After 25 iterations of (Vonneumann with Arnold)

D.After 130 iterations of (Vonneumann with Arnold)

E. Descrambled image

Figure 5.15: Results of scrambling and descrambling by Vonneumann concatenated with Arnold

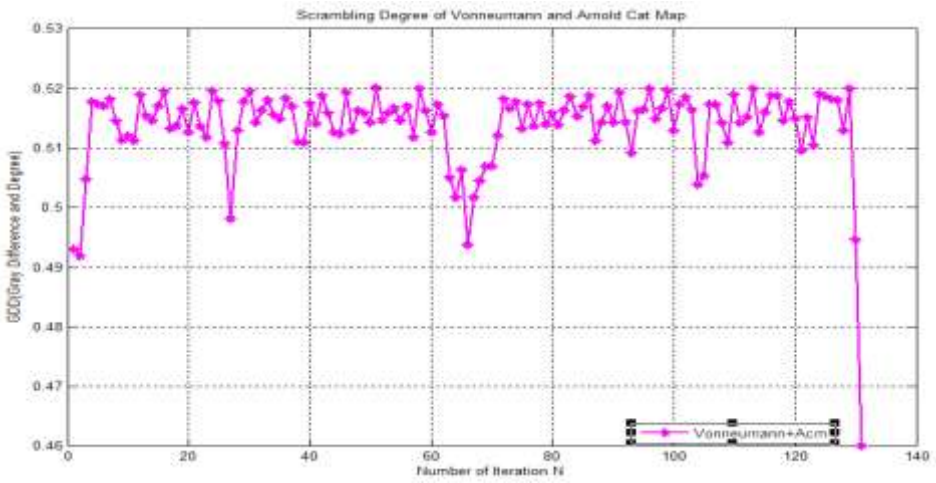


Figure 5.16: GDD of Vonneumann concatenated with Arnold

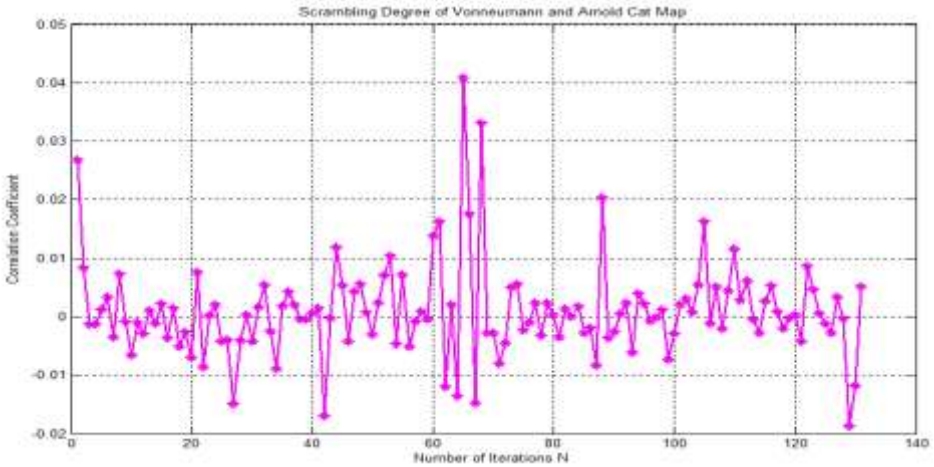


Figure 5.17: Correlation coefficient of Vonneumann concatenated with Arnold

5.4.3 Comparative Study of Parameters for Combined Technique

Here, we present graphs and tables for GDD, correlation coefficient for scrambling, by each of the combined technique i.e. Moore combined with Arnold and Vonneumann combined with Arnold transform. Both experimental results are compared with result of that individual technique (Arnold, Moore, and Vonneumann) which performed better for that scrambling degree parameter.

5.4.3.1 Comparative Study of GDD (Gray Difference and Degree)

Table of GDD for results of combined technique obtained after experimenting for 131 iterations are given by Table 5.3, which majorly concerns those outputs which make some conclusions about research performed.

Table 5.3 GDD of Vonneumann, Vonneumann with Arnold and Moore with Arnold

S.No.	Number of Iterations	Moore with Arnold	Vonneumann with Arnold	Vonneumann
1	2	0.4953	0.4919	0.4819
2	4	0.5200	0.5177	0.4912
3	10	0.5196	0.5121	0.5070
4	19	0.5194	0.5166	0.5136
5	25	0.5209	0.5179	0.5144
6	29	0.5204	0.5177	0.5147
7	37	0.5206	0.5171	0.5139
8	**40**	**0.5214***	**0.5175**	**0.5147**

9	**43**	**0.5160**	**0.5158**	**0.5157**
10	49	0.5206	0.5159	0.5151
11	**51**	**0.5178**	**0.5201**	**0.5144**
12	53	0.5193	0.5159	0.5149
13	56	0.5210	0.5171	0.5150
14	72	0.5203	0.5182	0.5145
15	82	0.5200	0.5163	0.5146
16	103	0.5207	0.5164	0.5143
17	116	0.5152	0.5188	0.5148
18	121	0.5152	0.5095	0.5150
19	130	0.5149	0.4947	0.5148
20	131	0.5149	0.4601	0.5145

Graph of GDD for combined technique by both type of Game of Life's neighborhood are provided and compared by Vonneumann scrambling technique as it performed better as far as GDD is concerned amongst Arnold, Moore and Vonneumann scrambling technique.

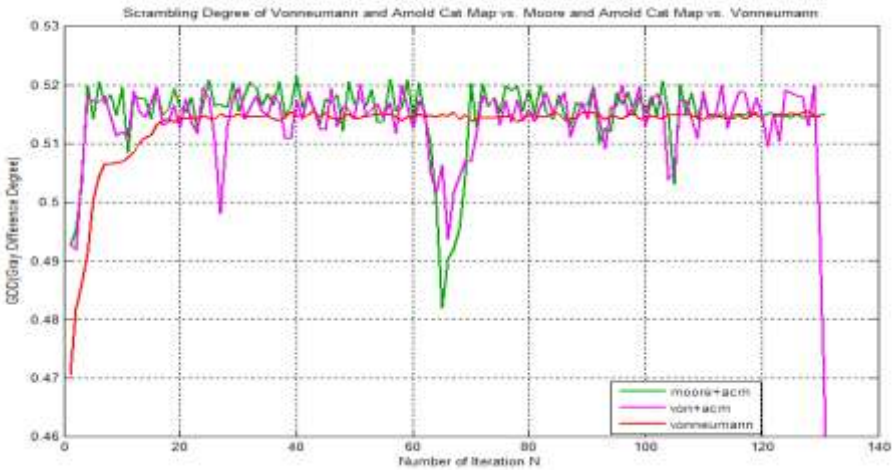


Figure 5.18: GDD of Moore with Arnold vs. Vonneumann with Arnold vs. Vonneumann

Figure 5.18 shows that from above graph it is obvious that by combining Arnold with Moore and Vonneumann there is a remarkable gain in GDD. Among all three trivial methods considered Vonneumann performed better but, here a plot between Vonneumann and combined method is presented which shows that GDD has increased even far ahead than Vonneumann's performance. Moore combined with Arnold attains its maximum GDD as 0.5214 at iteration 40 against GDD of 0.5157 of Vonneumann.

Similarly, maximum GDD of Vonneumann combined with Arnold is 0.5201 as against Vonneumann's 0.5157. So, both combined methods increase GDD and perform better than Vonneumann alone and amongst them best GDD is obtained by Moore combined with Arnold and values 0.5214. Hence, Moore combined with Arnold performs best amongst all techniques we considered till now.

5.4.3.2 Comparative Study of Correlation Coefficient

Table for Correlation Coefficient for combined technique obtained after experiment for 131 iterations is shown by Table 5.4 given below, which majorly concerns those outputs which make some conclusions.

Table 5.4: Correlation Coefficient of Vonneumann, Vonneumann with Arnold and Moore with Arnold

S.No.	Number of Iterations	Moore with Arnold	Vonneuman with Arnold	Vonneumann
1	3	-0.0077	-0.0014	$-7.5752e^{-04}$
2	5	0.0019	0.0012	$8.0628e^{-04}$
3	19	0.0034	-0.0027	0.0071
4	23	0.0013	$1.3459e^{-04}$	$-3.3895e^{-04}$
5	29	0.0035	$2.1200e^{-04}$	$3.2024e^{-04}$
6	**31**	$\mathbf{1.0700e^{-04}}$	**0.0016**	**0.0045**
7	38	0.0012	$-4.1360e^{-04}$	-0.0013
8	43	0.0029	$-2.4555e^{-04}$	0.0017
9	**65**	**0.0183**	**0.0408**	**0.0037**
10	**66**	**-0.0323**	**0.0175**	**-0.0015**
11	**67**	**-0.0092**	**-0.0148**	$\mathbf{3.6e^{-05}}$
12	79	0.0056	0.0024	0.0099
13	**83**	**-0.0053**	$\mathbf{3.8240e^{-06}*}$	**-0.0030**
14	91	-0.0070	$3.7132e^{-04}$	-0.0024
15	96	-0.0016	$-6.9800e^{-04}$	-0.0105
16	103	0.0033	$6.9300e^{-04}$	-0.0056
17	113	0.0055	$4.2823e^{-04}$	-0.0026
19	131	0.0032	0.0051	0.0042

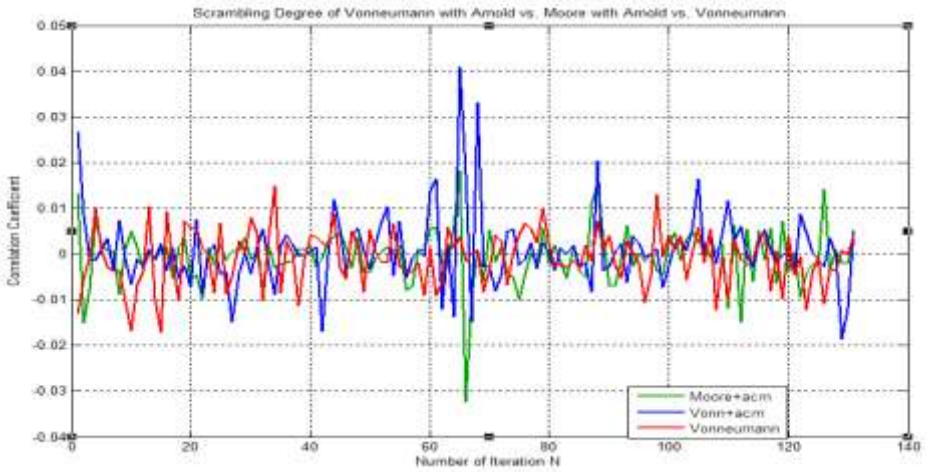


Figure 5.19: Correlation Coefficient of Moore with Arnold vs. Vonneumann with Arnold vs. Vonneumann

As among all three trivial methods taken Vonneumann performed better so a graph comparing Vonneumann and other two combined method's correlation is plotted. Here, all three Vonneumann combined with Arnold, Moore combined with Arnold and Vonneumann alone performs approximately similar to one another as far as numbers of iterations are concerned. Vonneumann with Arnold reaches its maximum closeness to ideality i.e. '0' at iteration 83 as 0.000003824 for correlation against 0.000036 of Vonneumann and 0.00003 of Arnold Cat Map which means it performs best for closeness to ideality compared to any methodology till now and reaches $3.824e^{-06}$ which is remarkable achievement. As far as deviation from ideality is concerned Vonneumann with Arnold is more deviated than Moore combined with Arnold as at iteration 65 correlation coefficient reaches 0.0408 against 0.0323 correlation coefficient at iteration 66 for Moore combined with Arnold. Although it is lesser than Arnold alone which reaches 0.18. Here, by combining Arnold with Vonneumann we get remarkable achievement of correlation as 0.000003824 and correlation gets better and closer to ideality.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

For secured transmission of images we need approaches that guarantee robustness. Encryption is among one of those approaches but, it can be easily invaded now a days, scrambling solves this issue and proven to be more robust than encrypting images. Arnold Cat Map is widely used scrambling technique and very popular for its simplicity but it possess some demerits as described in chapter1 as less secured because of its periodic nature and condition to work upon square images only, imposes a way to find out alternate technique of scrambling that overcomes these issues. 2D Cellular automata is an interesting and capable way of solving problems associated, unlike Arnold transform it doesn't possess periodic nature and can work upon rectangular images too. We prove by our experiment that 2D Cellular automata not only overcomes above problem associated with Arnold transform but performs better scrambling effect as parameters for measuring degree of scrambling like GDD(Gray difference and Degree) and Correlation Coefficient are better in case of 2D Cellular automata than Arnold transform. After comparing we succeeded in raising degree of scrambling for both parameters i.e. GDD and correlation coefficient remarkably by a combined effect of concatenating Arnold Cat Map and 2D cellular automata. This technique overcomes the periodic property of Arnold transform too and provides a more secured and robust way of scrambling images.

6.2 Future Scope

In our research work we have worked on a new technique for improving scrambling degree by applying a combined effect of Arnold transform and 2D cellular automata but many possibilities of improving it further is possible, as there is always a way for betterment.

- This research work can be extended further to improve scrambling degree by applying rules of Game of Life to scramble not only row wise but column wise too to make better chaos.
- Using a chaotic map, which performs better than Arnold transform for scrambling with 2D cellular automata may increase scrambling degree further.

- We may use the proposed combined scrambling technique to see what improvements are achieved as far as security and distortion are concerned by using it while watermarking the image.
- This technique can be used in combination with traditional Encryption scheme i.e. before encrypting image by traditional scheme we can scramble it with proposed scrambling scheme and see how security and noise measures are improved.

REFERENCES

[1] Abdel Latif Abu Dalhoum, Basel A. Mahafzah , Aiman Ayyal Awwad, Ibrahim Aldamari, "*Digital Image Scrambling Using 2D Cellular Automata*", 1070-986 X, IEEE CS Press, pp. 28-36, 2012.

[2] Aiman M. Ayyal Awwad, "*A Color Watermarking Scheme Based on Conway Game*", International Journal of Computer Science and Telecommunications, vol. 4, pp. 15-19, 2013.

[3] Congli Wang, Zhibin Chen, and Ting Li, "*Blind Evaluation of Image scrambling Degree based on the Correlation of Adjacent Pixels*", Indonesian Journal of Electrical Engineering, TELKOMNIKA, vol. 11, no. 11, pp. 6556-6562, 2013.

[4] Debasis Das, and Rajiv Misra, "*Programmable cellular automata based efficient parallel AES encryption algorithm* ", arXiv preprint arXiv: 1112.2021, vol.3, pp. 197-211, 2011.

[5] Deepak Ranjan Nayak, Sumit Kumar Sahu, and Jahangir Mohammed , " *A cellular automata based optimal edge detection technique using twenty-five neighborhood model* " , arXiv preprint arXiv*: 1402.1348,* 2014.

[6] Fasel Qadir, M. A. Peer, and K. A. Khan , " *Digital Image Scrambling Based on Two Dimensional Cellular Automata ",* International Journal of Computer Network and Information Security (IJCNIS), vol. 2, pp. 36-41, 2013.

[7] Gabriel Peterson , " *Arnold's Cat Map* ", *pages.physics.cornell.edu/~sethna/ teaching/562_S03/HW/.../**catmap**.pd,* 1997.

[8] Guodong Ye, Xiaoling Huang, and Changqing Zhu. "*Image encryption algorithm of double scrambling based on ASCII code of matrix element ",* International Conference on Computational Intelligence and Security, IEEE, pp. 843-847,2007.

[9] Jarkko Kari, "*Cellular Automata*", University of Turku, *cs.ioc.ee/~silvio/2013/ca kari-ca-notes-2011.pd ,* Spring 2011.

[10] Jianghong Bao, Qigui Yang, "*Period of the discrete Arnold cat map and general Cat map* ", Springer Science+Business Media, vol.70, pp. 1365–1375, 2012.

[11] J. L. Schiff, " *Introduction to Cellular Automata* ", 2005 .

[12] Lingling Wu, Jianwei Zhang , Weitao Deng , and Dongyan He , " *Arnold Transformation algorithm and anti-Arnold transformation algorithm ",* 1st International Conference on Information Science and Engineering (ICISE),

IEEE , pp. 1164-1167, 2009.

[13] Mao-Yu Huang, Yueh-Min Huang, " *Image Encryption Algorithm Based on Chaotic Maps* ", 978-1-4244-7640-4/10, IEEE Press , pp. 154-158 , 2010 .

[14] Md Moniruzzaman, Kayum Hawlader, Md Abul, and Md Faruque Hossain, "*Watermarking scheme based on game of life cellular automaton* ", International Conference on Informatics, Electronics & Vision (ICIEV), IEEE pp. 1-6, 2014.

[15] Minati Mishra, Ashanta Ranjan Routray, and Sunit Kumar , "*High Security Image Steganography with Modified Arnold cat map* ", arXiv preprint arXiv*: 1408.3838*, vol. 37, pp. 16-20, 2014.

[16] Min Li, Ting Liang, Yu-jie He, "*Arnold Transform Based Image Scrambling Method* ", International conference on Multimedia Technology (ICMT), pp. 1309-1316, 2013 .

[17] Niloy Ganguly, Biplab K Sikdar, Andreas Deutsch, Geo_rey Canright, P Pal Chaudhuri, " *A Survey on Cellular Automat* ", Centre for High Performance Computing , Dresden University of Technology , Dresden , Germany, http://www.cs.unibo.it/bison/publications/CAsurvey.pdf, 2003. .

[18] Omar Adwan, Aiman Ayyal Awwad, Azzam Sleit, and A. Abu Alhoum, "*A novel watermarking scheme based on two dimensional cellular automata*", Proceedings of the International Conference on Computers and Computing, World Scientific and Engineering Academy and Society (WSEAS), Canary Islands, Spain, pp. 88-94, 2011 .

[19] Pan Tian Gong, and Li Ta Yong. " *Image encryption algorithm based on 3D arnold cat and Logistic map* " , Advanced Materials Research , vol. 317, pp. 1537-1540 , 2011 .

[20] Pawan N Khade , and Manish Narnaware, " *Practical Approaches for Image Encryption/Scrambling Using 3D Arnolds Cat Map* ", Advances in Communication , Network and Computing , pp. 398-404 , Springer Berlin Heidelberg, 2012.

[21] Prashan Premaratne, "*Key based scrambling for secure image communication* ", Emerging Intelligent Computing Technology and Applications, Springer, pp. 259-263, 2012.

[22] Reema Rhine , Nikhila T Bhuvan , " *Image Scrambling Methods for Image Hiding: A Survey* ", International Journal of Computer Science and

Information Technologies (IJCSIT) , vol. 5 , pp. 751-755, 2014.

[23] Ruisong Ye, "*A Novel Image Scrambling and Watermarking Scheme Based on Orbits of Arnold Transform* ", Pacific-Asia Conference on Circuits, Communications and System , 978-0-7695-3614-9/09, IEEE CS, pp. 485-488, 2009.

[24] Ruisong Ye, and Huiliang Li, " *A novel image scrambling and watermarking scheme based on cellular automata* " , International Symposium on Electronic Commerce and Security, IEEE, pp. 938-941, 2008.

[25] Soumik Das, Pradosh Bandyopadhyay, Shauvik Paul, Arindam Sinha Ray, and Monalisa Banerjee , " *A New Introduction Towards Invisible Image Watermarking on Color Image* " , International *Advance* Computing Conference (IACC), IEEE , pp. 1224-1229 , 2009.

[26] Sourabh Chandra, Sk Safikul Alam, Debabrata Samanta, " *Data Hiding with Pixel Scrambling Techniques by Modified Shuffling* ", International Journal on Information Science and Intelligent System, vol.3 , pp. 9-14 , 2014.

[27] Tan Yongjie, and Zhou Wengang , " *Image scrambling degree evaluation algorithm based on grey relation analysis* " , International Conference on Computational and Information Sciences (ICCIS) , IEEE , pp. 511-514, 2010.

[28] Vidushi Sharma, Anurag Dev, Sachin Rai, "*A Comprehensive Study of Cellular Automata* ", International Journal on Advanced Research in Computer Science and Software Engineering , vol.2 , pp. 340-344 , 2012 .

[29] Wu Xue, " *Study on Digital Image Scrambling Algorithm"*, Journal of Networks , vol. 8 , pp. 1673-1679 , 2013.

[30] Xiaoqiang Zhang, Guiliang Zhu, Weiping Wang, Mengmeng Wang, and Shilong Ma, " *Period law of discrete two-dimensional Arnold transformation*" , Fifth International Conference on Frontier of Computer Science and Technology (FCST) , IEEE , pp. 565-569 , 2010 .

[31] Xiaoyan Zhang, Chao Wang, Sheng Zhong, and Qian Yao, "*Image encryption scheme based on balanced two-dimensional cellular automata* ", Mathematical Problems in Engineering, 2013.

[32] Xiongjun Li , "*A new measure of image scrambling degree based on grey level difference and information entropy* " , International Conference on Computational Intelligence and Security (CIS'08), IEEE, vol. 1, pp. 350-354, 2008.

[33] Zhenwei Shang, Honge Ren, and Jian Zhang, " *A block location scrambling algorithm of digital image based on Arnold transformation",* 9th International Conference for Young Computer Scientists (ICYCS), IEEE , pp. 2942-2947, 2008.

VIDEO PRESENTATION

The video presentation for the topic **"Image Encryption using 2D Cellular Automata"** is available on Youtube at following url:

- https://youtu.be/Tvl4yIJNseI

LIST OF PUBLICATIONS

- Communicated a paper "Comparative study of Image Scrambling Techniques Based on 2D Cellular Automata and Arnold cat map" in "Journal of Cellular Automata".
- Presented a paper "Introduction to Cellular Automata" in "National Conference on Smarter Approaches in Computing technologies & Application (SACTA-2014)" organized by Dept of IT, I.T.S, Mohan Nagar Gaziabad on 19th April 2014.