2D SUDOKU ASSOCIATED BIJECTIONS FOR IMAGE SCRAMBLING

A MINI PROJECT REPORT

submitted by

AASHIKA PREMKUMAR (119004002)
MONISHAA P (119004100)
VENNILA K (119004221)
VISHALI S (119004228)

towards partial fulfillment of the requirements for the award of the degree

of

Bachelor of Technology
in
Electronics & Communication Engineering

School of Electrical & Electronics Engineering

SASTRA DEEMED TO BE UNIVERSITY
(A University established under section 3 of the UGC Act, 1956)
Tirumalaisamudram
Thanjavur-613 401
MAY 2018

BONAFIDE CERTIFICATE

This is to certify that the project work entitled "**2D SUDOKU ASSOCIATED BIJECTIONS FOR IMAGE SCRAMBLING"** is a bonafide record of the work carried out by

AASHIKA PREMKUMAR(119004002)
MONISHAA P (119004100)
VENNILA K (119004221)
VISHALI S (119004228)

students of third year B.Tech., Electronics and Communication Engineering, in partial fulfillment of the requirements for the award of the degree of B.Tech in Electronics & Communication Engineering of the **SASTRA DEEMED TO BE UNIVERSITY, Thirumalaisamudram, Thanjavur - 613401,** during the year 2015-2019.

NAME OF THE INTERNAL GUIDE: Dr. V. Padma Priya
AP-III / ECE
School of ECE
SASTRA UNIVERSITY

SIGNATURE

Project Viva-Voice held on ______________________________

Examiner -I **Examiner-II**

ACKNOWLEDGEMENTS

First of all we express our gratitude to **Prof. R. Sethuraman**, Vice Chancellor, SASTRA University who provided all facilities & encouragement during the course of our study.We extend our sincere thanks to **Prof. K. Sridharan**, Registrar, SASTRA University for providing the opportunity to pursue this project.

We dedicate our whole hearted thanks to **Dr. K. Thenmozhi**, Associate Dean (ECE) and **Dr. R. John Bosco Balaguru**, Associate Dean(Research) who motivated us during the project work.

I heartily thank our project coordinators, **Dr. K. Narasimhan**, **N. Raju** for guiding us all along, till the completion of our project by providing all necessary information.

We owe a debt of deepest gratitude to our mentor **Dr. V. Padma Priya**, AP III, ECE, for her continuous support and guidance throughout the process viewing the pursuit of our project work. Her deep insight in the field and invaluable suggestions helped us in making progress through our project work.

We would like to dedicate this work with tremendous love to our **Parents** for their unlimited, ultra-supportive, encouragement, sacrifices and unconditional love throughout our entire life.

Above all, we thank the almighty for the divine grace we received throughout the research work, without which we could not have completed this work.

ABSTRACT

KEYWORDS: Sudoku , Bitwise , Block, Image Scrambling

Sudoku refers to a two-dimensional number placement puzzle with simple constraints that there are no repeated digits in each row, each column, or each block. Motivated by this Sudoku configuration, this project uses a number of Sudoku associated matrix element representation besides the conventional representation, using matrix row-column pair. This means that one can secretly represent matrix elements via a Sudoku matrix, and furthurmore develop new Sudoku associated 2D paramertic bijections.

Block scrambling is a technique to perform image scrambling which involves scrambling image blocks of the same size. However the image is still not sufficiently scrambled and shows some information in both the scrambled image and histogram. To counteract this, a technique called bit scrambing is used. In this process, bits of the image are taken and modified by performing the same puzzle pair scrambling process to obtain new pixel values in the image.

To demonstrate the effectiveness and randomness of bijections,a simple but effective Sudoku Associated Image Scrambler using 2D Sudoku associated bijections is used for image scrambling.Based on review of literature, this project introduces a simpler method for image scrambling.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 5 RESULTS AND DISCUSSION

CHAPTER 1

INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

Information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of image data is very important in many areas, such as copyright protection and privacy, security communication, and also in military applications.

Digital images, one typical type of 2D data, are considered to contain a huge amount of information, for example, a diagnosis CT image might tell a doctor whether the patient is healthy or not and if he/she is sick how bad he/she is; and a satellite photo might give information whether the interested region is under constructions and what these constructions could be. Because the information contained in a digital image might be inferred beyond requirement for unauthenticated usage , it is very important to protect these information.

Trust in digital data is characterized in terms of confidentiality, authenticity, and integrity. Confidentiality is 'the property that information is not made available or disclosed to unauthorized individuals, processes or entities.' Authenticity is defined as 'the corroboration that the source of data received is as claimed.' Integrity is the 'the property that data has not been altered or destroyed in an unauthorized manner.

One way of protecting digital images is called image scrambling, which disorders pixel relationship in the original image so that the scrambled image with rearranged pixels become unintelligent and unrecognizable.

There are various image scrambling techniques that that can be used to encrypt images efficiently by scrambling them. In general, the evaluation of data hiding performance depends mainly on the visual quality of stego-image and data hiding capacity.

Some of the methods used for image scrambling are discussed in the following section.

CHAPTER 2

REVIEW OF LITERATURE

There are various image scrambling techniques that that can be used to encrypt images efficiently by scrambling them. In general, the evaluation of data hiding performance depends mainly on the visual quality of the image and data hiding capacity.[1,3]

Several literary works and research papers were studied for the purpose of choosing an efficient methodology for image scrambling.

The techniques studied for the above mentioned purpose are as follows:

- Rubik's Cube Algorithm
- Arnold's Cat Method
- R-Prime Shuffle
- Sudoku Based Mapping

These methods are explained clearly in this section:

2.1 RUBIK'S CUBE ALGORITHM

Rubik's cubic was invented in 1974 as a famous wisdom game. It is nothing but a cubic model with 6 different colors on each face. It can be divided into 54 individual elements, as each face consists of 9 independent blocks.

In the beginning, the hidden data will be partitioned into different units of equal block sizes based on the number of pixels present. 3×3 pixels based. Then, 54 units will be selected sequentially and transformed into 6 faces according to the six faces of a Rubik's cubic by designating an index number.[7]

Therefore, an image can be partitioned into a 54 different units of blocks and thus giving rise to different combinational algorithms. To apply the Rubik's cube methodology for image scrambling, the basic process unit can be one pixel or a small block,

For example, an image can be partitioned pixel-wise and associated with each of the small elements of a Rubik's Cube. Therefore, 54 pixels can be fit into the Rubik's Cube and each pixel represents a small block. An image can also be partitioned based on 3×3, i.e. 9 pixels, thus converting it to a small block.

Using this method, 54 3×3 blocks can be fit into the Rubik's Cube and each 3×3 block represents a small block of the Rubik's Cube. Each Rubik's cube can be assigned a different random number for performing rotation to scramble the sequence of original 54 units.

2.2 ARNOLD'S CAT METHOD

Images are composed of discrete units called pixels. A pixel is the basic unit representing some color value, which when taken together forms the image. The image is a m×n matrix, where M represents the number of rows of pixels and N represents the number of columns of pixels, and each entry in the matrix being a numeric value, represents a given color.

Let X be the image matrix. From this, it is possible to examine selected entries in X. The numeric entries represents some color value. The mapping known as Arnolds Cat Map is named after the mathematician Vladimir I. Arnold, who first illustrated it using a diagram of a cat. It is a simple and elegant demonstration and illustration of some of the principles of chaos namely, underlying order to an apparently random evolution of a system.[9]

Arnold transformation has been very widely used in literature, so it is unsafe to use the same, Zhenwei Shang et al. proposed a novel image block location scrambling algorithm based on Arnold transformation. The method also makes use of logistic map to generate the sequence. This sequence is used on different blocks in the image after applying Arnold transformation over the blocks. Results show that the proposed method has a good encryption effect, has a large key space and also has key sensitivity.

The proposed data hiding scheme not only can achieve the benefits of reversible reconstruction of hidden data, but also it possesses good visual quality of the stego-image. Moreover, satisfactory data hiding capacity can be obtained simultaneously. Finally, the proposed data hiding scheme not only can be performed in spatial domain, but also can be performed in the frequency domain or even applied in hybrid domains.

2.3 R PRIME SHUFFLE

R-Prime shuffling technique is a simple yet powerful technique which can be used for image scrambling. The technique is robust as different relative prime numbers are used for row and column shuffling. From the experimental results it can be observed that there is a reduction of approximately 50% in the correlation between rows and columns of the encrypted image.

From time taken it can be concluded that the technique takes few seconds for the encryption process. It does not involve a high time complexity. As long as the relative prime number considered is kept secret it is not possible to decrypt the scrambled image. Hence this technique can be used to secure the image by storing the scrambled image and not the original image.[8]

One of the main goal of an image scrambling algorithm is that the correlation between any two rows and columns has to be minimum. Considering this aspect, firstly correlation is calculated between the first row and every subsequent prime row, the one having minimum correlation is brought next to the first row, this process is continued till all the rows are placed. Then same process is applied to columns. The method results in good amount of decrease in correlation among rows and columns of the scrambled image when compared to original image. The row prime and column prime would act as a key to descramble the image.[10]

2.4 SUDOKU BASED SCRAMBLING

Yang Zou et al. proposed an image scrambling algorithm based on Sudoku puzzle in [4]. The property of a sudoku puzzle is that in any row/column numbers 1 to N appears only once. This concept can be applied and a one to one relationship can be used between two Sudoku puzzles these puzzles can be used to map the original image to a scrambled image. The proposed method scrambles the image at both pixel level and also at bit level so as to provide more security.

This introduces a new way of constructing 2D bijections for digital image scrambling using Sudoku matrices. It demonstrates that an $N \times N$ Sudoku matrix can be used to define six new parametric matrix element representations for an $N \times N$ matrix. Consequently, it is possible to construct a 2D Sudoku associated bijection by mapping one matrix element representation to the other. Moreover, it demonstrates that 2D Sudoku associated bijections actually performs scrambling in a guarantee way.[2]

For example, the 2D Sudoku associated bijection mapping from the row-digit pair to the row-column pair is to scramble image pixels in such a way that two pixels originally lies in the same column will be in different columns after scrambling, while the 2D Sudoku associated bijection mapping from the digit-column pair to the row–column pair is to scramble image pixels in such a way that two pixels originally lies in the same row will be in different rows after scrambling.

From the above observations and research work it can be concluded that Sudoku associated 2D bijections provides a simple and unique solution for image scrambling. Simulation results on various image types and datasets demonstrate the effectiveness and robustness of the proposed method. Visual and Analytical comparisons to peer algorithms suggest that the Sudoku Associated Image Scrambler outperforms or reach state-of-the-art methods of image scrambling. Statistical testing results also support that Sudoku Associated Image Scrambler successfully decorrelates pixels in the original image to random-like.[5,6]

CHAPTER 3

SCOPE OF THE PRESENT WORK

Image processing is a newly emerging and a promising domain. It has vast applications in image analysis, pattern recognition, machine learning and computer vision and large scale automation. The challenges that exist in the automation industry and the need for artificial cognition are attracting the researchers towards image processing.

There is a lot of ongoing research in the domain and a tremendous rise in job opportunities pertaining to the present work carried out.

One of the most recent and mind blowing application of image processing is a pair of dark glasses and a vest which acts as an aid for the visually impaired. As the person moves the system creates a 3D map of the environment, while cameras in the dark glasses watch out for obstacles. The micro-motor sensors present in the vest indicate obstacles accordingly.

Another application of the same helps in monitoring traffic and environmental conditions in cities. This is done with the help of a drone which captures high resolution photographs and real time videos of earthquakes, fire or other disaster struck areas, to hunt out those trapped and help save lives. This involves high precision image processing.

Image processing also finds its significance in the medical industry. RCADIA, a start-up in Israel, uses a trademark image processing technique, to detect fatty heart plaques in arteries and helps doctors to determine the required diagnosis.

Another medical robot named daVinci system, allows doctors to perform delicate diagnosis and surgeries by seeing the high quality 3D images.

The most important feature of image processing is enhancement of image security.

This ensures safe transmission of sensitive data between end users and guarantees very high immunity to hacking and tampering of data. This is very useful for military and defence purposes.

CHAPTER 4

EXPERIMENTAL PROCEDURES

Fig 4.1 Original image

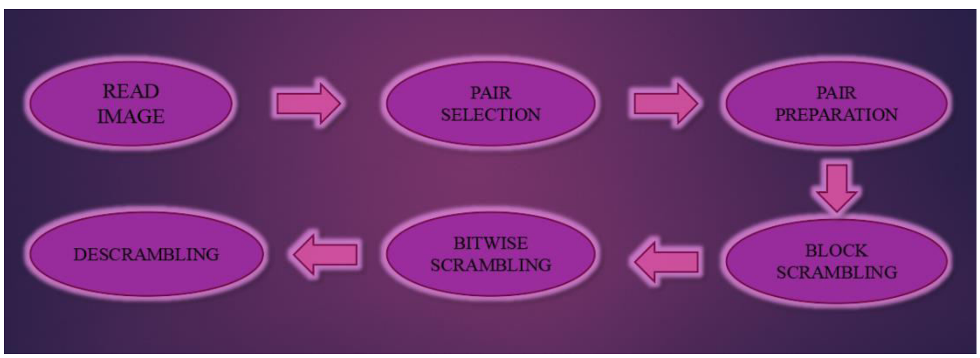

Fig 4.2 Flow graph

4.1 SUDOKU PAIR SELECTION AND PREPARATION

The original image is shown in Fig 4.1 and the flow graph is represented in Fig 4.2.

Pairs can be of any size and numbers. Different pairs can improve the security of the method.1-to-1 relationship should be present between each pair. Pair preparation is done by adding prefix to each of the digit entries in order to make them all unique. This way there is exactly one of each entry in first puzzle for each entry in the second puzzle as shown in Fig 4.5 .

ALGORITHM FOR PAIR PREPARATION

NEW_VALUE = OLD_VALUE + PARAMETER X POW(10, DIGITS)

where   PARAMETER can be either row, column or digit as shown in Fig 4.3 and Fig 4.4

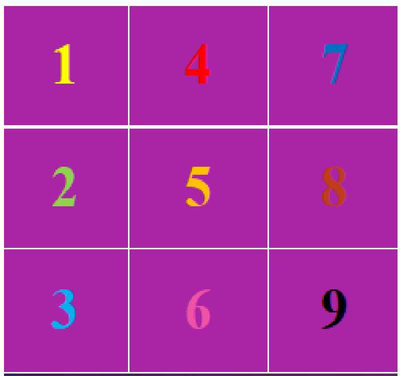

Fig 4.3 Block representation

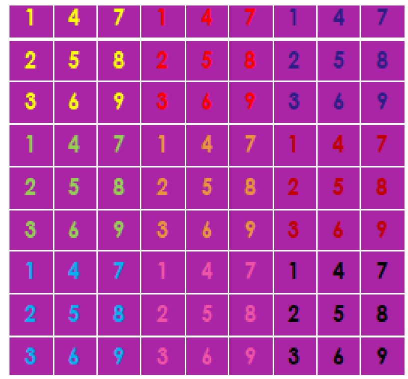

Fig 4.4 Grid representation

Fig 4.5 Original Sudoku puzzle

18	12	16	43	45	41	74	79	77
14	11	13	48	49	47	72	75	76
17	15	19	46	42	44	71	78	73
25	26	24	57	51	53	88	82	89
21	27	22	59	56	58	85	83	84
23	29	28	55	54	52	86	87	81
32	33	31	64	68	69	97	96	95
36	38	37	61	63	65	99	94	92
39	34	35	62	67	66	93	91	98

Fig 4.6 Block Digit Representation

11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99

Fig 4.7 Row Column Representation

4.2 BLOCKWISE SCRAMBLING

Sudoku pairs are used to scramble blocks of the same size in the original image. Sudoku puzzle is used to mark the pixel position. Then place that pixel in the equivalent entry.

BLOCK SCRAMBLING ALGORITHM

- Split the original image into red, green and blue channels
- Convert the image into blocks using mat2cell( ) & name it as CA_1as shown in Fig 4.8
- Extract a value from Parametric Array & Note its row & column as (R1,C1) as shown in Fig 4.6 and Fig 4.7
- Find that value in Fixed Array & Note its row & column as (R2,C2)
- Now place BLOCK (R1,C1) of CA_1 to (R2,C2) of CA_2 as shown in Fig 4.9
- Repeat the above process for 'N' times, N - no. of blocks
- The scrambled image is as shown in Fig 4.10

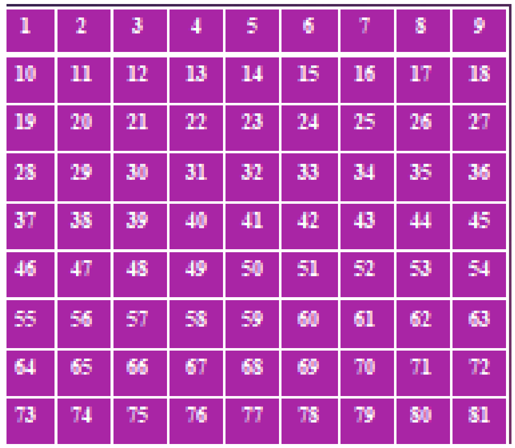

Fig 4.8 Original Image Representation

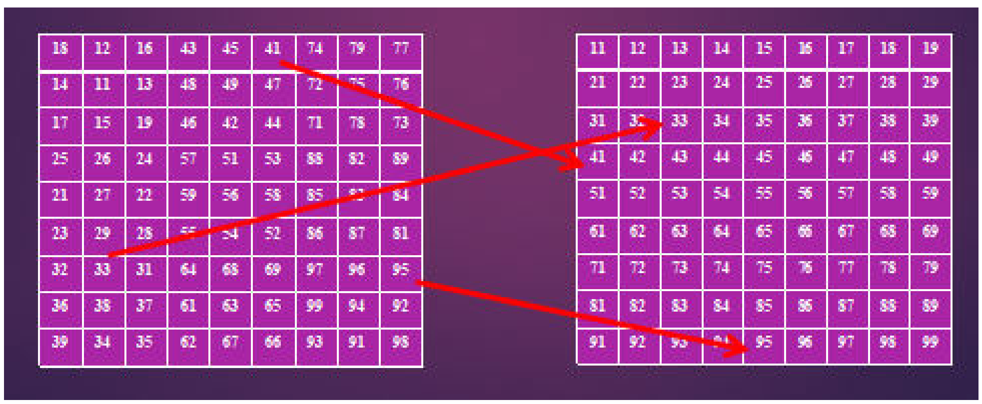

Fig 4.9 Scrambling Methodology

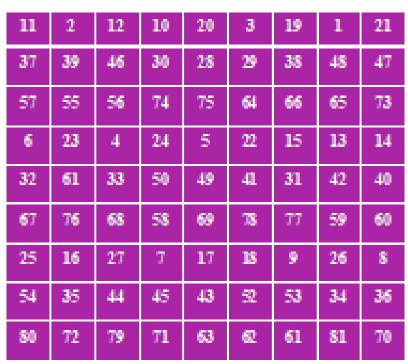

Fig 4.10 Scrambled Image Representation

4.3 BITWISE SCRAMBLING

Pixel values of the image are represented by its corresponding binary values. Every single bit of all pixel will form a bit plane.

ALGORITHM

- Flatten the scrambled image into a 1D array by connecting each row together - use horzcat( ) function.
- Array length will be P, where P - no of pixels.
- Create a column having its binary value - use de2bi( ) function.
- This gives a 2D array of size 8 X P as shown in Fig 4.11.
- Reshape it accordingly - use reshape( ) function.
- Perform the same puzzle pair scrambling to this 2D array.
- Reshape it into 8 X P - use reshape( ) function.
- Extract each column and convert this binary values to decimal - use num2str( ) & bin2dec( ) function.
- This decimal corresponds to new pixel values.
- This must be done for all 3 colors (Red, Green and Blue).
- Later join all 3 colors using cat( ) function.
- Display the image using imshow( ) function.
- This method won't show any information about the image.

67	72	81	18
10	51	84	93
95	93	25	36
Scrambled Image			

↓

56	76	90	67	72	81	18	10	51	84	93	95	93	25

↓

0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	0	0	0	1	1	1	1	0
1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	0	1	0	0	1	1	0	1	1	1	1	1	1
1	1	1	0	1	0	0	1	0	0	1	1	1	1
0	1	0	0	0	0	0	0	1	1	1	1	1	0
0	0	1	1	0	0	1	1	0	0	0	1	0	0
0	0	0	1	0	1	0	1	0	0	1	1	1	1

Fig 4.11 Bit Scrambling Matrix Generation

CHAPTER 5

RESULTS AND DISCUSSION

5.1 BLOCKWISE SCRAMBLING

In accordance with the above mentioned algorithm, we arrived with the following results. This result shows the blockwise scrambled images of 24 different mapping methodologies. Thus we infer from Fig 5.1 that the image is not sufficiently scrambled and still appears to show some information in it.

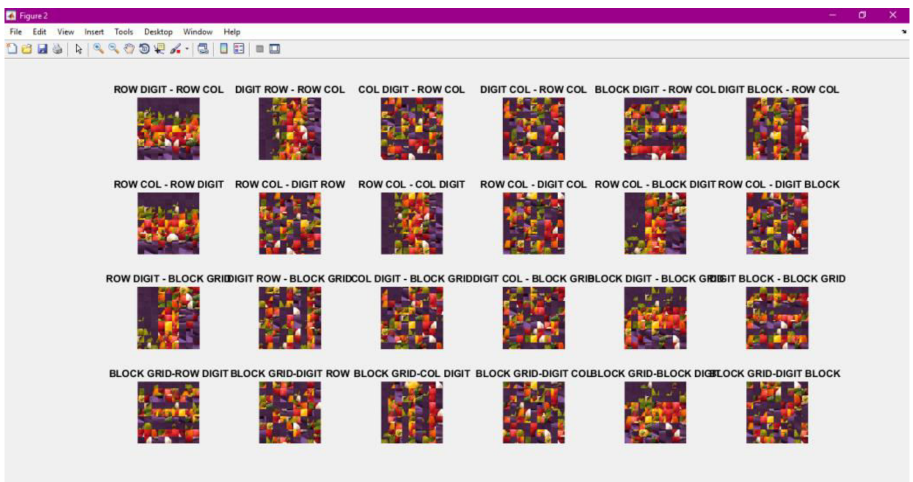

Fig 5.1 Blockwise scrambling

5.2 BITWISE SCRAMBLING

Results obtained from bitwise scrambling is shown in Fig 5.2. From this we infer that image is completely scrambled and it doesn’t reveal any information. Thus this methodology provides high robustness and improved security.

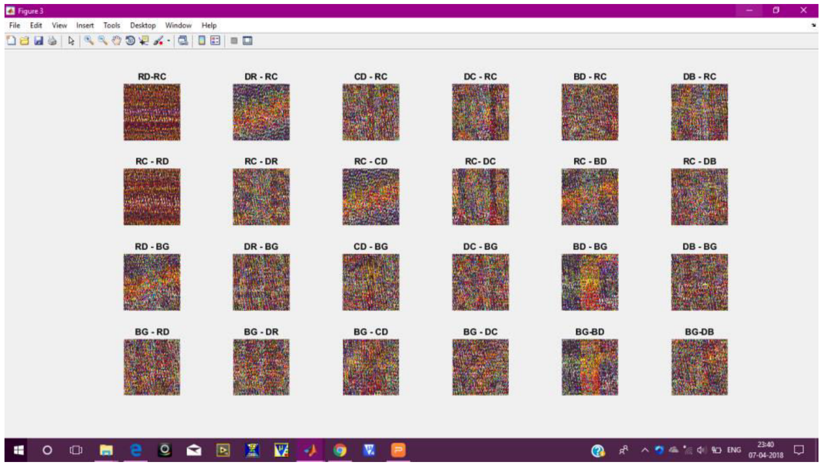

Fig 5.2 Bitwise scrambling

5.3 DESCRAMBLING

Using the above descrambling algorithm, we have efficiently restored the original image from the scrambled image as shown in Fig 5.3.

Fig 5.3 Descrambling

5.4 CORRELATION

It is the mutual relationship or connection between two or more images. Here we found the correlation between original image and scrambled image. The values shown in Table 5.1 reflects that how far both images are related. Here we observe scrambled image has less relation with original image.

Table 5.1 Correlation

COLOR	RED	GREEN	BLUE
ROW DIGIT - ROW COLUMN FORWARD MAPPING	0.0495	0.0246	0.0283

5.5 ENTROPY

It represents degree of disorder or randomness in an image. We found entropy of original image as 7.3737. From the Table 5.2, we infer that the degree of randomness for the scrambled image is increased for all the representation, comparatively more for block digit representation. Thus we would say that the image is well scrambled.

Table 5.2 Entropy

MAPPING	ROW COLUMN
ROW DIGIT	7.3873
DIGIT ROW	7.6278
COLUMN DIGIT	7.6254
DIGIT COLUMN	7.6285
BLOCK DIGIT	7.6294
DIGIT BLOCK	7.6280

5.6 HISTOGRAM

It is the graphical representation of the tonal distribution in an image. It plots the number of pixels for each intensity value. The following Fig 5.4 shows that there is a significant difference between the original and scrambled image.

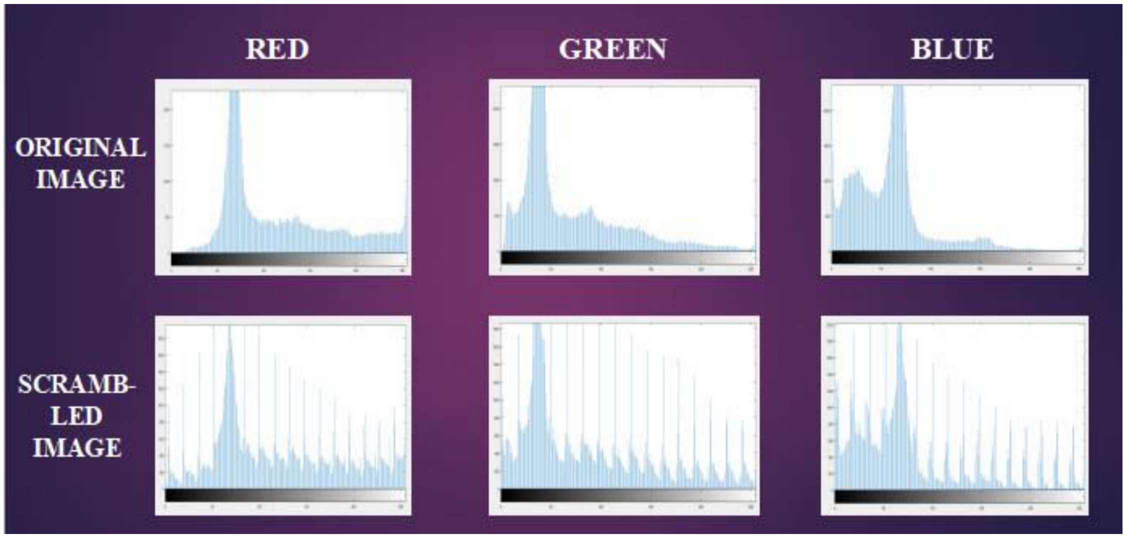

Fig 5.4 Histogram

5.7 COMPARISION WITH OTHER TECHNIQUES

From the above results we made certain conclusions as shown in Table 5.3.

Table 5.3 Comparison

PARAMETER	RUBIKS CUBE	ARNOLD'S CAT	SUDOKU PUZZLE
BASIC UNIT	PIXEL/BLOCK	PIXEL	BLOCK
SCRAMBLING TIMES	ANY NO OF TIMES	FIXED	ANY NO OF TIMES
AREA	ANY TYPE	SQUARE	SQUARE
REASSEMBLY	BY REVERSING	BY RE-SCRAMBLING	BY REVERSING

CHAPTER 6

CONCLUSIONS

In this Project we applied the Sudoku associated 2D bijections for image scrambling. It can be conclude that these bijections can be defined by Sudoku associated matrix element representations, which provide additional and parametric means to denote matrix elements besides the conventional way of using the row-column pair. Specifically, these new Sudoku associated matrix element representations are row-digit pair, digit-row pair, column-digit pair, digit-column pair, block-digit pair, and digit-block pair.

Since all these Sudoku associated matrix element representations are parametric with respect to a reference Sudoku matrix, it then allows us to denote matrix elements in secret ways and further provides Sudoku matrix dependent 2D bijections constructed by mapping from one representation to the other. We showed that many of these Sudoku associated 2D bijections have deterministic scrambling effect when we use them for image scrambling.

For example, the bijection mapping from row–column pair to row-digit pair is equivalent to scramble pixels within a row to different positions that none two pixels that originally lies in the same column is still in the same column after scrambling; the bijection mapping from block-grid pair to block-digit pair is equivalent to scramble pixels within each block and cause a mosaic-like effect.

Furthermore, the proposed Sudoku Associated Image Scrambler, is a simple but effect digital image scrambler of using these Sudoku associated 2D bijections, by using a scrambling key to control these bijections in a parametric way. Because a multi-round scrambler is mathematically equivalent to a new bijection composed of a series of bijections in each scrambler round, we showed that these fundamental Sudoku associated 2D bijections can be cascaded together to scramble image pixels in a deterministic way.

Simulation results of the proposed image scrambler and comparisons to recent peer algorithms indicate that Sudoku Associated Image Scrambler outperforms or atleast reaches state-of-the-art suggested by these peer algorithms with respect to a number of evaluation and analysis methods, including human visual inspections, gray degree of scrambling, and autocorrelation coefficient of adjacent pixels.

Moreover, our tests and results support that Sudoku Associated Image Scrambler converts the strong correlations between adjacent pixels to zero correlations after scrambling.

REFERENCE PAPERS

1. **Prarthana Madan Modak1, Dr. Vijaykumar Pawar -** A Comprehensive Survey on Image Scrambling Techniques.
2. **Yue Wua, Yicong Zhoub, Sos Agaianc, Joseph P. Noonana -** 2D Sudoku associated bijections for image scrambling, Vol. 327, 10 January 2016, Pages 91-109.
3. **Reema Rhine, Nikhila T Bhuvan -** Image Scrambling Methods for Image Hiding: A Survey.
4. **Yang Zou, Xiaolin Tian, Shaowei Xia, and Yali Song**. "A Novel Image Scrambling Algorithm Based on Sudoku Puzzle," Proceedings of the Fourth International Congress on Image and Signal Processing, Vol. 2, October 2011.
5. **Chin-Chen Chang, Yung-Chen Chou, and the Duc Kieu.** "An Information Hiding Scheme Using Sudoku," Proceedings of the Third International Conference on Innovative Computing Information and Control, Dalian China, June 2008.
6. **Yue Wu, Joseph P. Noonan, Sos Agaian**, "Image encryption using the rectangular Sudoku cipher", System Science and Engineering (ICSSE) 2011 International Conference on, pp. 704-709, 2011.
7. **Z. Hua, Y. Zhou, C.-M. Pun, C.L.P. Chen**, "Rubik's Cube method for image encryption", Inf. Sci. 297 (0) (2015) 80–94.
8. **H. fen Huang**," Perceptual image watermarking algorithm based on R-Prime Shuffle in DWT", in: Proceedings of the Fifth International Joint Con-ference on INC, IMS and IDC (NCM '09), 2009, pp. 1819–1822.

9. **K. Lin,** “Hybrid encoding method by assembling the Arnold’s Cat method and the binary encoding method in image hiding”, Opt. Commun. 284 (7) (2011) 1178–1784.

10. **Z. Zhu, W. Zhang, K. Wong, H. Yu**, “A R-Prime Shuffle method of symmetric image encryption scheme using a bit-level permutation”, Inf. Sci. 181 (6) (2011) 1171–1186.