International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 3; May 2018; Page No. 298-302

A survey on image scrambling encryption techniques

Swati Suryawanshi[1], Vaishali Kolhe[2]
[1] ME Scholar, D. Y. Patil College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India
[2] Assistant Professor, D. Y. Patil College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract

The ongoing development of organized network media frameworks has expanded the requirement for the security of advanced Media. Digital media incorporates content, advanced sound, pictures, video and programming. Digital image scrambling encryption technology is a method for securing digital image data. With the utilization of change strategies, it can change the original image into a disarranged one to the point of being unrecognizable, making it troublesome for individuals who get the in unapproved way to extricate data of the original image from the scrambled images. In this paper, the fundamental standards of digital image scrambling encryption are discussed. The different scrambling encryption techniques are studied. The literature overview and working of these scrambling techniques is introduced. The framework has many functions: information hiding mechanism, reversibility and good visual quality, better encryption.

Keywords: image scrambling, encryption, Rubik's cubic algorithm, Arnold's cat map, r-prime shuffle, Sudoku puzzle

1. Introduction

Data security turns into a critical and pressing issue for people as well as for business and governments. Security of image is very important in many areas, for example, protection and copyright insurance, security correspondence, and furthermore in military applications Trust in computerized information is described as far as privacy, legitimacy, and integrity [1]. Classification is the property that data isn't made accessible or unveiled to unapproved people, substances or procedures. Authenticity is characterized as the authentication that the wellspring of information got is as guaranteed. Integrity is the property that information has not been adjusted or destroyed in an unapproved way. Image Scrambling is a good strategy for giving security to picture information by making picture in unreadable format and furthermore hard to unscramble it for unapproved clients.

There are numerous image scrambling techniques that may be used to encrypt images with efficiency by scrambling them. In general, the analysis of information hiding performance depends principally on the visual quality of scrambled images and information hiding capacity.

2. Literature Survey

Chang-Lung Tsai, Chun Jung Chen, and Wei-Leih Hsu proposed a data hiding scheme based on the utilization of Rubik's cubic rotation [1]. They proposed a technique which can be joined with any sort of information hiding approaches and encipher framework to accomplish data assurance. The proposed information concealing plan not exclusively can accomplish the advantages of reversible recreation of shrouded information, yet additionally it has great visual nature of the stego -image. In addition, attractive information hiding capacity can be acquired all the while. At long last, the proposed information hiding scheme not only can be performed in spatial area, as well as can be performed in the recurrence space or even connected in hybrid domains.

Zhen wei Shang *et al.* proposed a novel image block location scrambling algorithm based on Arnold transformation [2]. Arnold transformation has been generally utilized as a part of writing, so it is risky to utilize the same. The technique additionally makes utilization of calculated guide to create the arrangement. This grouping is utilized on various blocks in the image after applying Arnold transformation over the blocks. Results demonstrate that the proposed technique has a good encryption impact, has a huge key space and furthermore has key affectability.

Kekre *et al.* proposed an image scrambling algorithm utilizing the idea of relative prime numbers in [3]. One of the primary objective of an image scrambling algorithm is that the connection between's any two lines and segments must be least. Then, firstly connection is calculated between the first row and every subsequent prime row, the one having minimum correlation is brought next to the first row, this procedure is proceeded till every one of the lines are set. At that point same process is connected to columns. The strategy brings about great measure of decrease in connection among rows and columns of the scrambled image when contrasted with original image. The row prime and column prime would act as a key to descramble the image.

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 technique scrambles the image at both pixel level and also at bit level so as to provide greater security.

3. Image Scrambling Techniques

A. Rubik's Cubic Algorithm

Rubik's cubic was invented in 1974 as a famous wisdom game. In the beginning, it is a cubic with different colors in each side (6 faces) as shown in Figure 1.

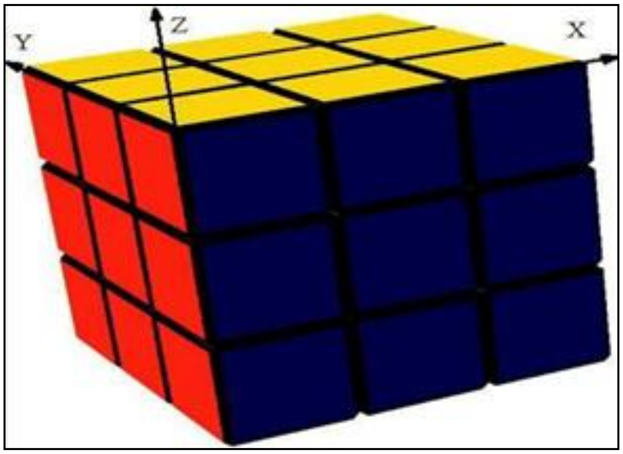


Fig 1: A Rubik's Cubic indexed with direction parameter [1].

Rubik's cubic has 6 faces and may be isolated into 54 (6 faces×3×3) components. In the beginning, the hidden information are going to be partitioned into completely different unit square size, for example, pixel based, 3×3 pixels based, or other n×n pixels based. At that point, 54 units are going to be chosen consecutively and changed into 6 faces as indicated by the six appearances of a Rubik's cubic by assigned a record number as appeared in Figure 2 and Figure 3. In this manner, an image can be divided into a variety of different 54 units of blocks and framed many Rubik's cubic. To apply the Rubik's cubic for image information hiding, the essential procedure unit can be one pixel, small block, or full scale cell is contrasted with the conventional Rubik's Cubic. For instance, an image can be partition by pixels to fit and connected with every one of the little cubic of a Rubik's Cubic. Subsequently, 54 pixels absolutely can be fit into the Rubik's Cubic and every pixel represents a small block. An image can also be partitioned based on 3×3, i.e. 9 pixels, as a small block. In this way, 54 3×3 pieces can be fit into the Rubik's Cubic and every 3×3 block represents a small block of the Rubik's Cubic. Each Rubik's cubic can be assigned alternate random number for performing rotation to scramble the arrangement of unique 54 units.

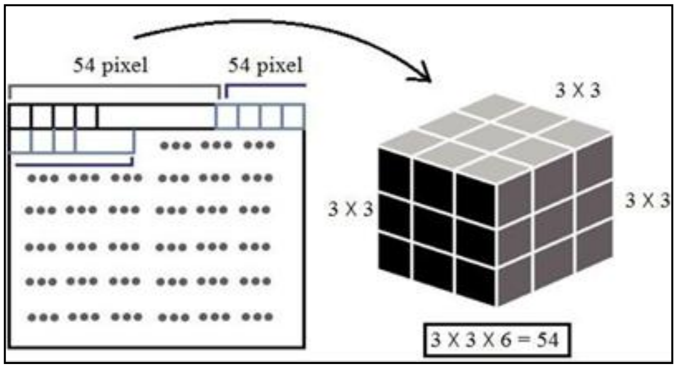


Fig 2: Mapping of Rubik's Cubic and image [1].

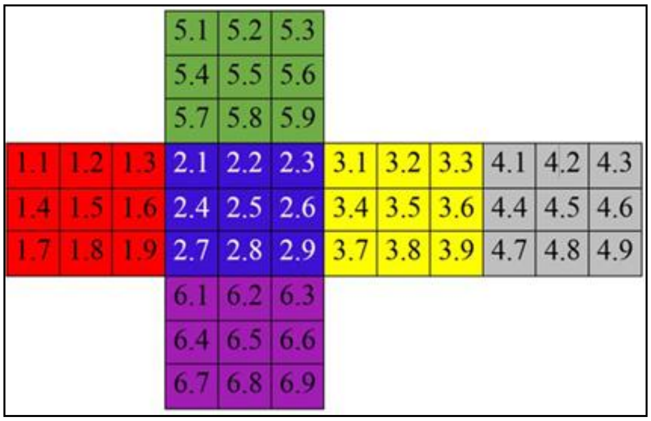


Fig 3: Corresponding index of Rubik's Cubic [1].

In the information hiding procedure is performed from left to right and after that top to bottom in the cover image, i.e., horizontally, with the covert data. In the proposed scheme, a few parameters are used for controlling the procedure of information scrambling and information installing as recorded below.

1. Macro cell parameter M*p:* It is utilized to indicate scrambling is either pixel or and block based.
2. Hiding technique parameter H*p*: Specify which data hiding is utilized.
3. Rotation parameter R*p*: Specifies number of rotation of Rubik's cubic block and its direction.
4. Rotation regulation parameter R*r*: Specifies all of the macro cells use the same or different rotation parameter for performing scrambling.

Proposed information hiding methodology is implemented by the following technique:

1. Define the required M*p*, H*p*, R*r* and R*p* parameters.
2. Hidden information is encrypted by the cipher system in order to strengthen the information security.
3. The encrypted information is scrambled by applying the Rubik's cubic rotation.

The scrambled data is embedded into the cover image to obtain the stego-image.

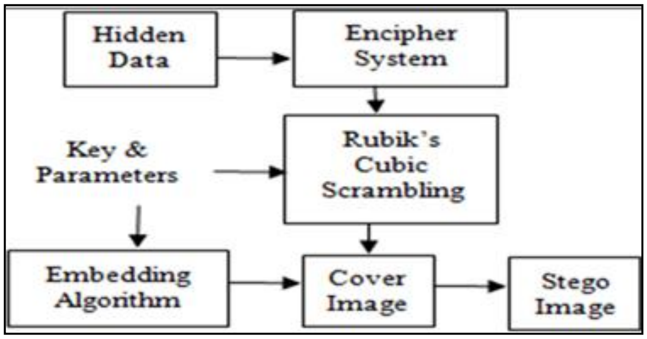


Fig 4: Data hiding scheme using Rubik's cubic scrambling [1].

B. Arnold's Cat Map

Images are made out of discrete units called pixels. A pixel is the fundamental unit representing some color value, which when taken together form the image. The image is an m×n matrix, where m represents the quantity of rows of pixels and n the quantity of columns of pixels, and every entry in the matrix being a numeric value that represents a given color. For example, consider the 175×175 image of a caffeine molecule below.

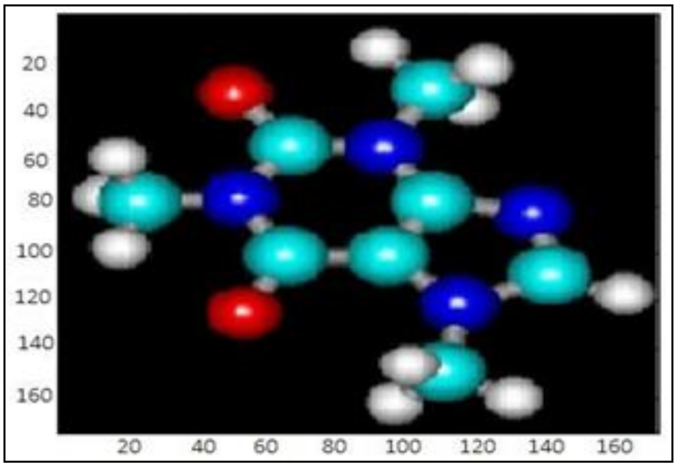


Fig 5: 175 × 175 image of a caffeine molecule.

Let X be the image matrix shown below, it is possible to examine selected entries in X. The numeric entries represent some colour 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.

$$X = \begin{bmatrix} 217 & 217 & 217 & 217 & \ldots & 217 & 217 & 217 & 217 \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \ldots & 251 & 251 & 251 & 251 \\ 217 & 217 & 217 & 217 & \ldots & 217 & 217 & 217 & 217 \end{bmatrix}$$

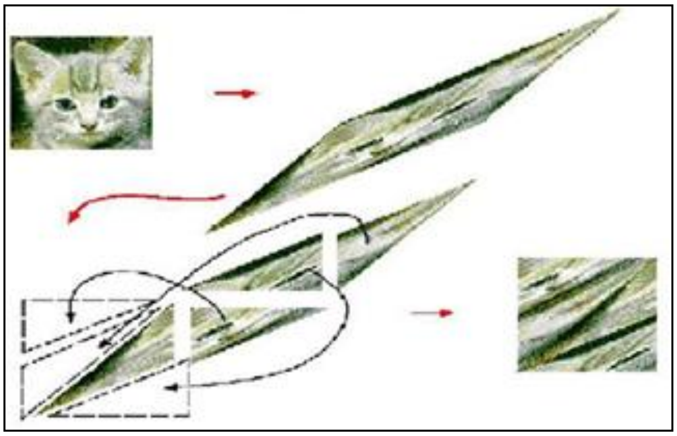


Fig 6: Visuals illustrating the steps

Arnold's cat map is the transformation

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \bmod n$$

Where mod is the modulo of the

$$\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$$

For understanding the mechanism of the transformation better, it can be decomposed into elemental pieces.

1. Shear in the x-diection by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix}$$

2. Shear in the y-direction by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix}$$

3. Evaluate the modulo.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

Figure 6 shows the shearing in the x and y directions, followed by modulo operation and then the reassembly of the image.

C. R-Prime Shuffle Technique

This technique is also known as Template Matching which is used to match the similarity between any two elements of the image. It also can be used to locate an object in a digital image. In this technique, Cross correlation using FFT is used as a measure of similarity between two Rows/Columns in a digital image. R-Prime known as Relative Prime Shuffling technique, two numbers are said to be relatively prime if they don't have any common factor except one. To choose a relative prime number for shuffling from the set, correlation concept is used. The Lowest correlation obtained between the different relative primes numbers (row/column positions) and 1st row/column is used as a key for carrying out the shuffling.

Encryption

This technique used for Encryption is as follows:

1. Read the image.
2. Convert it to gray scale.
3. Based on the size of the image (M×N), find out all the relative prime numbers and save them in a set S.
4. Find the correlation of the first row with remaining rows by using set S.
5. Take into consider the lowest correlation because the key

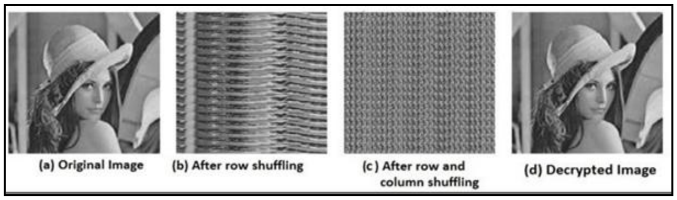
to shuffle the rows within the image.

6. Continue until all the positions within the image are considered.
7. Save the relative prime numbers as a key considered for row shuffling.
8. Repeat the similar procedure for column shuffling.

Decryption

1. Use the Saved key for Row and Column Shuffling to induce the initial image back.
2. Use the column Relative Prime and set up the columns, this may offer row shuffled image.
3. Using this row shuffled image and also the key for row relative prime set up the rows which is able to offer you original image back.
4. Continue until all the positions within the image are rearranged.

R-Prime shuffling technique could be a straightforward however powerful technique which may 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 will be determined that there will be discount of approximately 50 percent within the correlation between rows and columns of the encrypted image From time taken it will be all over that the technique takes few seconds for the encryption process. It doesn't involve a time quality.. 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.



(a) Original Image (b) After row shuffling (c) After row and column shuffling (d) Decrypted Image

Fig 7: R-Prime Shuffling [3].

D. Sudoku Puzzle

This method securely scrambles images making them appear to contain no information. The proposed method uses pairs of Sudoku puzzles to map original and scrambled images. The technique takes a combine of Sudoku puzzles and modifies it thus there's a 1- 1 relationship between the digits of the puzzles. It adds the digits corresponding to column number in front each of the digits for the puzzle corresponding to the original image. It does the same with row numbers to the puzzle for the scrambled image. It then scrambles the image by taking a pixel in the original image, locating the digit entry in the Sudoku puzzle in the same place as the pixel, and moving it to the corresponding digit in the other puzzle. The proposed method takes advantage of the Sudoku rule to create this 1- to-1 correspondence between puzzles. The methods also take benefits from the large number of Sudoku solutions to provide security against unscrambling attempts.

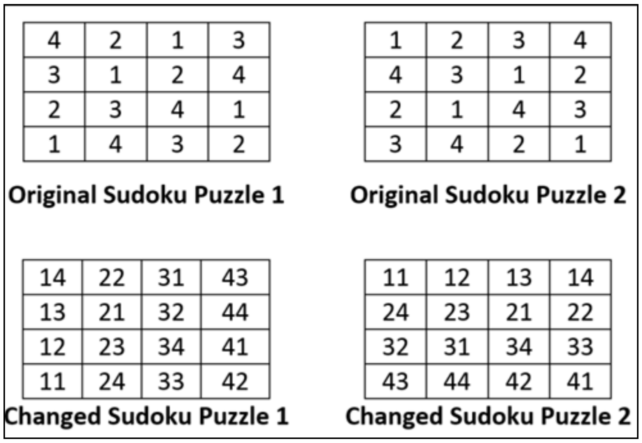
The scrambling algorithm for this method is divided into four parts: Sudoku pair selection, Sudoku pair preparation, image marking and mapping, and bit scrambling. This discussion also specified how to unscramble the image.

1. Sudoku Pair Selection

The first step is the Sudoku puzzle pair selection. In this step, one must simply make pairs of Sudoku puzzles. The pairs are often of any size and there is often any variety of pairs. Having many different pairs can be beneficial to improve the security of the method.

2. Sudoku Pair Preparation

In the second part, it need to establish 1-to-1 relations between the puzzles in each pair. This can be done by adding a prefix to each of the digit entries in order to make them all unique. This way there is exactly one of each entry in the first puzzle for each entry in the second. Then modify the entries in the first puzzle with the formula *NewValue* = *OldValue* + *Column* ×10*Digits*, Where digits is the number of digits in the puzzle. Note that this formula simply adds a row prefix to each entry. Below an image is given for exemplifying this process:



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

Original Sudoku Puzzle 1

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

Original Sudoku Puzzle 2

14	22	31	43
13	21	32	44
12	23	34	41
11	24	33	42

Changed Sudoku Puzzle 1

11	12	13	14
24	23	21	22
32	31	34	33
43	44	42	41

Changed Sudoku Puzzle 2

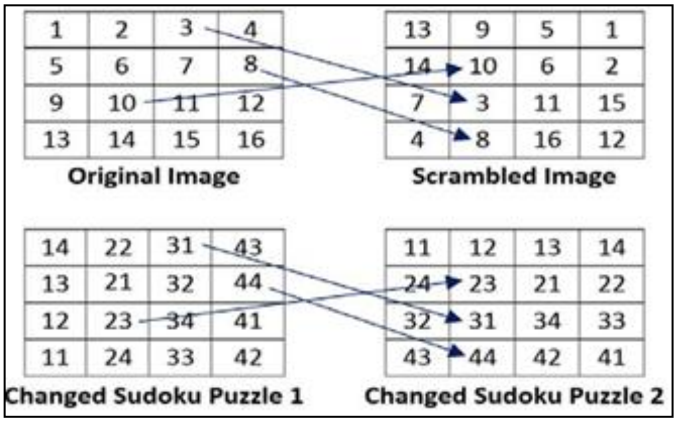
Fig 8: Sudoku Pair Preparation [4].

3. Image Marking and Mapping

The third part uses these prepared pairs of Sudoku puzzles to establish a relation between the original image and the scrambled one. This part is sub-divided into two sub-parts: block scrambling and sub-block scrambling.

i. **Block Scrambling:** In block scrambling, use the Sudoku pairs to scramble blocks of the same size in the original image. In this step the first Sudoku puzzle in a pair is used to mark the pixel positions of the original image. Then place that pixel in the equivalent entry for the second Sudoku puzzle. The following steps and figure explain the process in more detail:
   1. For the *ith* pixel in the original image block *pi*, take the *ith* entry in the first Sudoku puzzle *ai*.
   2. Find the entry within the second Sudoku puzzle such *bj* = *ai*.
   3. Set the *jth* pixel within the scrambled image to be *sj* = *pi*.
   4. Repeat these steps till all pixels within the block are processed.

ii. **Sub block Scrambling :** In sub-block scrambling, they take each scrambled block and break it up into smaller sub-blocks, then repeat the same process from block scrambling with these smaller blocks.



Original Image

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Scrambled Image

13	9	5	1
14	10	6	2
7	3	11	15
4	8	16	12

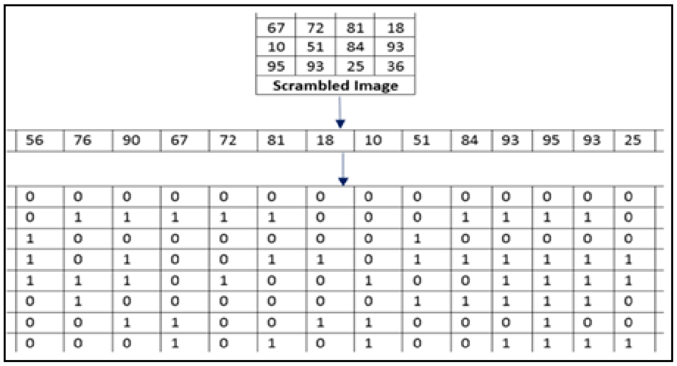
Changed Sudoku Puzzle 1

14	22	31	43
13	21	32	44
12	23	34	41
11	24	33	42

Changed Sudoku Puzzle 2

11	12	13	14
24	23	21	22
32	31	34	33
43	44	42	41

Fig 9: Block scrambling using Sudoku Pairs [4].



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 10: Bit scrambling matrix generation [4].

4. Bit Scrambling

After the third part, the image is not sufficiently scrambled and still appears to show some information in the scrambled image and in the histogram. For this reason, it need the fourth part: bit scrambling. In this part, take the bits of the image and modify them so it is possible to treat them like a 2-D grid. To do this first flatten the scrambled image into a 1-D grid by connecting rows to each other. The grids length is P, where P is the number of pixels. For each pixel in the grid, create a column containing its binary representation, giving us a 2-D grid of size 8×P. There are at most 8 rows because pixel values range between 0 and 255. Then reshape the grid into a square of size M×M, where M is the floor of square root of 8×P. This is performed by reshaping by going through entries row-by-row and adding them to the square grid. Then perform the same puzzle pair scrambling process to this grid and obtain new pixel values in the image.

5. Unscrambling

To restore the image to its pre-scrambled form, one must simply exchange roles of prepared Sudoku puzzles and repeat the scrambling steps with the same iteration numbers. This will successfully restore the image as long as the correct sets of puzzles and iteration numbers are used.

6. Conclusion

Now days, the security of images is very important because of the terrorist attacks. The different image scrambling techniques are discussed in the paper. All the techniques are very useful for real-time scrambling of images. Every technique is exclusive in its own means, which could be appropriate for various image encryption applications. These techniques can be used to encrypt image after or before embedding data into it. All scrambling techniques are good in its own way, which could be suitable for different scrambling applications for providing the security to images.

7. Reference

1. Chang-Lung Tsai, Chun-Jung Chen, Wei-Leih Hsu. Multi-morphological Image Data Hiding based on the Application of Rubik's Cubic Algorithm. IEEE International Conference, 2012.
2. Zhenwei Shang, Honge Ren, Jian Zhang. A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. The 9th International Conference for Young Computer Scientists. 2008; 978-0-7695- 3398-8/08/$25.00 © IEEE.
3. Kekre HB, Tanuja Sarode, Pallavi Halarnkar. Image Scrambling using R-Prime Shuffle. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2013.
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. 2011; 2.
5. Chin-Chen Chang, Yung-Chen Chou, The Duc Kieu. An Information Hiding Scheme Using Sudoku. Proceedings of the Third International Conference on Innovative Computing Information and Control, Dalian China, 2008.
6. Qi Dongxu, Zou Jianchun, Han Xiaoyou. A New Class of Scrambling Transformation and Its Application In The Image Information Covering. J Science in China Scrics, 2000.