International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Comprehensive Survey on Image Scrambling Techniques

Prarthana Madan Modak[1], Dr. Vijaykumar Pawar[2]

[1]PG student, A. C. Patil College of Engineering, Mumbai University, Mumbai, India

[2]Professor, A. C. Patil College of Engineering, Mumbai University, Mumbai, India

Abstract: ***Digital image scrambling is the technique which transforms a meaningful image into a meaningless or disordered image in order to enhance the ability to confront attack and in turn improve the security. Various image scrambling techniques are designed to make the image content unintelligible. This discussion focuses on the different kinds of image scrambling techniques. In general, the better an image is scrambled, the better the information is hidden. Image scrambling technology is basically used in image encryption method by which the original image information can be hidden, so that the information will not be easily intercepted.***

Keywords: Scrambling, Rubik's cubic algorithm, Arnold's Cat Map, R-Prime Shuffle, Sudoku Puzzle.

1. Introduction

Image scrambling (one of the kind of encryption) is a good method for providing security to image data by making image visually unreadable and also difficult to decrypt it for unauthorized users.

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.

Chang-Lung Tsai, Chun Jung Chen, and Wei-Leih Hsu proposed a data hiding scheme based on the application of Rubik's cubic rotation [1]. They proposed a method which can be combined with any kind of data hiding approaches and encipher system to achieve information protection. 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.

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 [2]. 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.

Kekre et al. proposed an image scrambling algorithm using the concept of relative prime numbers in [3]. 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.

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.

2. Literature survey

2.1 Rubik's Cubic Algorithm

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

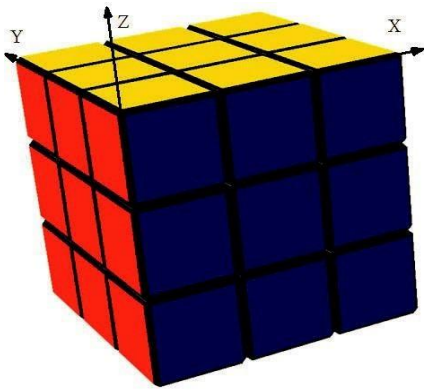

Figure 1: A Rubik's Cubic indexed with direction parameter

Rubik's cubic possesses 6 faces and can be divided into 54 (6 faces×3×3) elements. In the beginning, the hidden data

(treated similar as an image) will be partitioned into different unit block size such as pixel based, 3×3 pixels based, or other n×n 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 designated an index number as shown in Figure 2 and Figure 3. Therefore, an image can be partitioned into a lot of different 54 units of blocks and formed a lot of different Rubik's cubic. To apply the Rubik's cubic for image data hiding, the basic process unit can be one pixel, small block, or macrocell (large block) is compared to the traditional Rubik's Cubic. For example, an image can be partition by pixels to fit and associated with each of the small cubic of a Rubik's Cubic. Therefore, 54 pixels totally can be fit into the Rubik's Cubic and each pixel represents a small block. An image can also be partitioned based on 3×3, i.e. 9 pixels, as a small block. Thus, 54 3×3 blocks can be fit into the Rubik's Cubic and each 3×3 block represents a small block of the Rubik's Cubic. Each Rubik's cubic can be assigned a different random number for performing rotation to scramble the sequence of original 54 units.

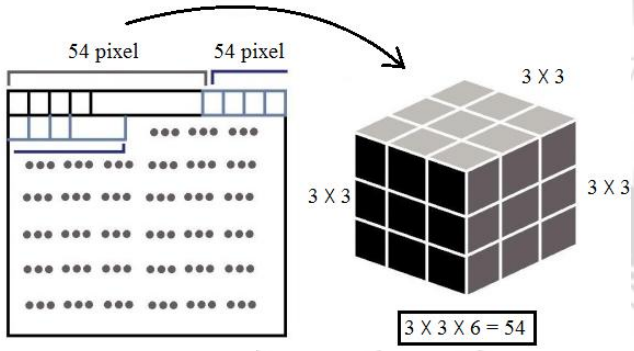

Figure 2: Mapping of Rubik's Cubic and image

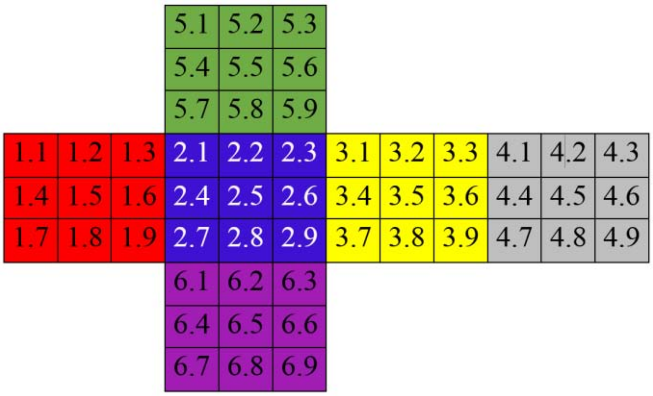

Figure 3: Corresponding index of Rubik's Cubic

In the proposed data hiding, the data hiding process is performed from left to right and then top to bottom in the cover image, i.e., horizontally, with the covert information. In the proposed scheme, some parameters are utilized for controlling the process of data scrambling and data embedding as listed below.

- Macrocell parameter M_p: It is used to specify scrambling is either pixel or and block based.
- Hiding method parameter H_p: Specify which data hiding is used.
- Rotation parameter R_p: Specifies number of rotation of Rubik's cubic block and its direction.
- Rotation regulation parameter R_r: Specifies all of the macrocells use the same or different rotation parameter for performing scrambling.

Proposed data hiding approach is implemented by the following procedure:

1) Define the required M_p, H_p, R_r and R_p parameters.
2) Hidden data is encrypted by the cipher system in order to strengthen the data security.
3) The encrypted data is scrambled by applying the Rubik's cubic rotation.
4) The scrambled data is embedded into the cover image to obtain the stego-image.

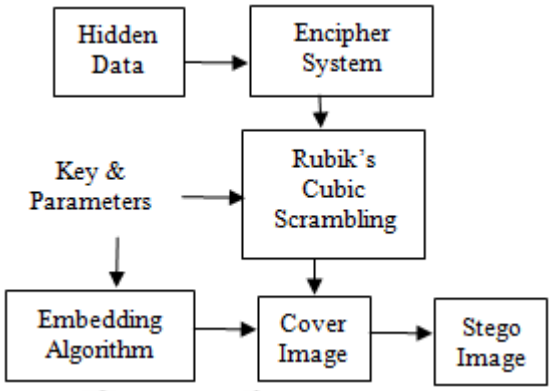

Figure 4: Data hiding scheme using Rubik's cubic scrambling

The hidden data can be extracted by performing the above steps reversely.

2.2 Arnold Transformation

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

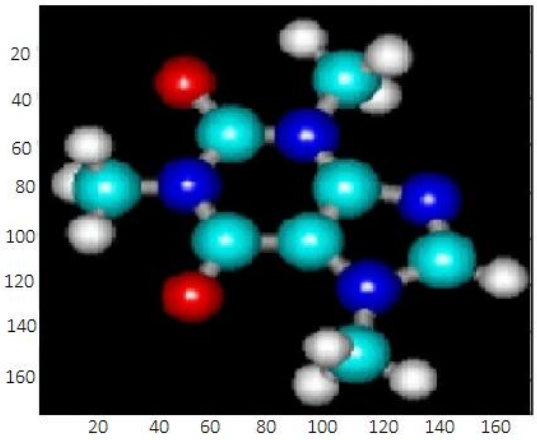

Figure 5: 175 × 175 image of a caffeine molecule

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

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

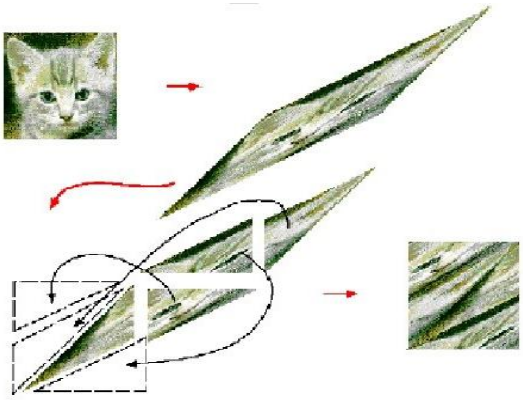

Figure 6: Visuals illustrating the steps

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*-direction 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 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.

2.3 R-Prime Shuffle Technique

This technique is also called as Template Matching which is used to match the similarity between any two parts of the image. It can also 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 called 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 the method used for Encryption is as follows:

1. Read the image.
2. Convert it to grayscale.
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. Using set S to find the correlation of the first row with remaining rows (positions w.r.t elements present in the set).
5. Consider the lowest correlation as the key to shuffle the rows in the image.
6. Continue till all the positions in the image are considered.
7. Save the relative prime numbers as a key considered for row shuffling
8. Repeat the same procedure for column shuffling ...

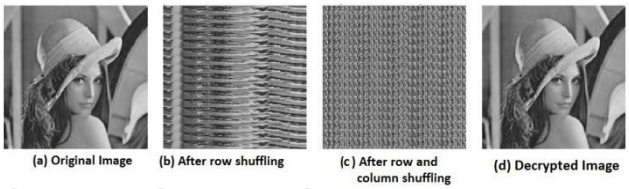

Figure 7: R-Prime Shuffling.

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.

2.4 Using Sudoku Puzzle

In 2011, Zou, Tian, Xia, and Song [4] introduced an image scrambling method using 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 method takes a pair of Sudoku puzzles and modifies it so there is 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 method 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.

2.4.1 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 can be of any size and there can be any number of pairs. Having many different pairs can be beneficial to improve the security of the method.

2.4.2 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 $NewValue = OldValue + Column \times 10^{Digits}$, 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

Figure 8: Sudoku Pair Preparation.

2.4.3 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.

2.4.3.1 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 i^{th} pixel in the original image block p_i, take the i^{th} entry in the first Sudoku puzzle a_i.
2. Locate the entry in the second Sudoku puzzle such that $b_j = a_i$.
3. Set the j^{th} pixel in the scrambled image to be $s_j = p_i$.
4. Repeat these steps until all pixels in the block have been processed.

2.4.3.2 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.

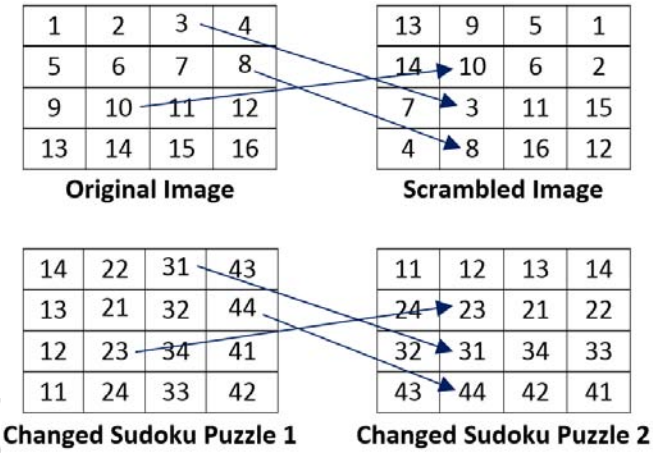

Figure 9: Block scrambling using Sudoku Pairs.

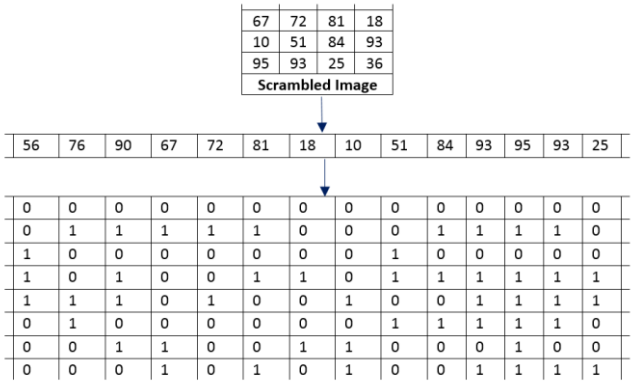

Figure 10: Bit scrambling matrix generation.

2.4.4 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.

2.4.5 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.

3. Conclusion

Nowadays, the security of images become very important. In this paper we have surveyed different image scrambling techniques. All the techniques we discussed here are very useful for real-time scrambling of images. Each technique is unique in its own way, which might be suitable for different image encryption applications. These techniques can be used to encrypt image after or before embedding data into it. The characteristic of above mechanisms are that these possesses the advantages of reversibility and good visual quality.

References

[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. 2008. A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. *The 9th International Conference for Young Computer Scientists, 978-0-7695-3398-8/08/$25.00 © IEEE*

[3] H B Kekre, Tanuja Sarode, Pallavi Halarnkar, "Image Scrambling using R-Prime Shuffle," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, August 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, 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] 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.