A Study on various Image Scrambling Techniques

Seesa Paul
PG Student
Department of Computer Science & Engineering
CKC, Kuzhoor, Kerala, India

Abstract— Image scrambling is an encryption method that transforms an image which is ordered into an image which is disordered or meaningless. This method provides security to the image data that is, it cannot be visually readable. This solves the problem of decryption of image data by unauthorized users. Studies on some image scrambling techniques are done here like Rubik's cubic, Arnold transform, Improved Arnold transform etc. If the image is scrambled well then better information hiding can be done.
Key words: Scrambling, Rubik's Cubic, R-Prime Shuffle, Arnold Transform, Improved Arnold Transform

I. INTRODUCTION

Image scrambling is a method that is proposed with the rapid development of IoT (Internet of Things). The method scrambling is used for privacy protection. Because of the computing efficiency of scrambling over encryption it is much simpler than the complicated encryption techniques. The scrambling methods are of various kinds that will encrypt the image in an efficient manner i.e., by scrambling those images. The capacity of data hiding and visual quality of stego-image are the main factors in which the performance of the data hiding depends on.

In this paper the section II contains the survey of various scrambling techniques. The method Rubik's Cubic rotation is proposed by Chang-Lung Tsai, Chun Jung Chen, and Wei-Leih Hsu and it is a data hiding scheme [1]. By using this method the benefits of reversible reconstruction of the data which are hidden can be perform and also it poses a good rate of visual quality of the stego- image. This scheme can be performed in spatial, frequency or in the hybrid domains.

Using the relative prime numbers concept another image scrambling method is proposed by Kekre et al [2]. It considers the aspect that the minimum correlation between any two rows and columns, which is a goal of the algorithm in scrambling of image. In this method same operations are performed for rows and columns. Firstly, the first row and every subsequent prime row are considered and the correlation between them is calculated. Next, the row which has the minimum correlation is taken and placed next to the first row. Until the placing of all the rows the procedure continues. This method achieves the decrease of the correlation among columns and rows in a good amount when compared to the image before scrambling and the key which is used to descramble the image will be the row prime and column prime.

Arnold transform is also known as cat mapping which is proposed by V I Arnold in the ergodic theory [5]. It is then applied to the digital images. It is the process of changing pixel from one point to another point. It contains number of iterations. After performing the Arnold transform the Arnold transform a new image is produces which is entirely different from the original image with no loss in the information. Being cyclic and reversible are also the properties of this method. Sometimes the Arnold transform is not safe because it is widely used because it is simple. So, based on Arnold transform a novel image block location scrambling is proposed by Zhenwei Shang et al [3]. This method will generate sequence using logistic map and it is applied on different blocks after the Arnold transform on the blocks.

Arnold transform is a scrambling method which is widely used and it is periodic in nature. It is an encryption and decryption tool. The disadvantage of the traditional Arnold transform is that it can't be applied to the non-squared images. To overcome this limitation another algorithm which is a multi-region algorithm i.e. IAT (Improved Arnold Transform) is proposed by MA Ding & Fan Jing [4], in which the non-square image is splits into multiple squared regions and after that the scrambling is applied to each regions. This improved method will effectively improves the security of the image to avoid the decipher process. By this method the image which is same as the original image can be restored.

II. LITERATURE SURVEY

A. *Rubik's Cubic Algorithm*

Rubik's cubic is a famous wisdom game which is invented in 1974 by Erno Rubik. Rubik's Cubic is a cube of 6 faces and have 6 different colors in each face and it can be divided into 54 elements. The Rubik's Cubic is shown in the Figure 1. Firstly in the process, the data which is hidden i.e. similar as an image will partitioned into various unit block size like pixel based or any n x n pixels based. After that the 54 units will sequentially selected and according to the six sides (faces) of the Rubik's Cubic it will transformed into six faces by designated an index number which is shown in Figure 2 and Figure 3. So, an image can be partitioned into various 54 unit blocks and thus can form lot of Rubik's Cubic which are different. In the case of applying the Rubik's method for image hiding when compared to traditional Rubik's Cubic method the basic process unit can be a pixel, small or large block. Below figure shows the Rubik's Cubic indexing.

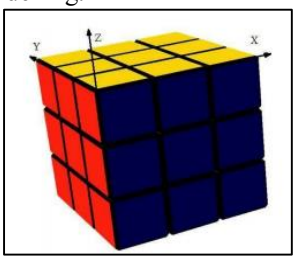

Fig. 1: Rubik's Cubic which is indexed with direction parameter

Considering an example, if an image is taken and it is represented by pixel. This pixels are fits and associated each of small Cubic of the Rubik's Cubic and also the image can be partitioned as n×n, for example n=3, i.e. 3×3 which means 9 pixels, represented as a small block of Rubik's Cubic. For the scrambling original 54 units sequence the rotation will performed and for this rotation a random number is assigned to each Rubik's Cubic.

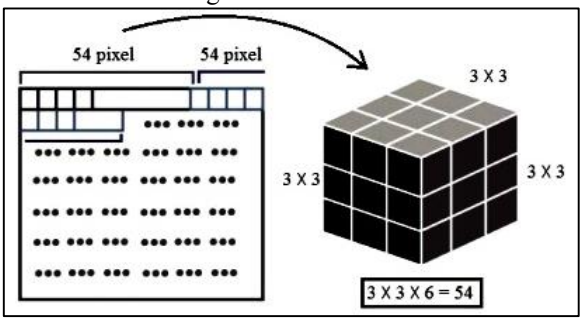

Fig. 2: The mapping of Rubik's cubic and the image

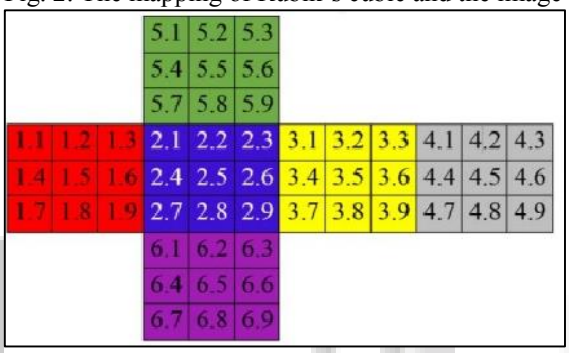

Fig. 3: The Corresponding index of Rubik's Cubic

For controlling scrambling and embedding of the data, some parameters are utilized which are listed below:

- Macrocell parameter (M_p): Pixel based or block based scrambling is specified using this parameter.
- Rotation parameter (R_p): The number of rotation of Rubik's Cubic and its rotation is specified by this parameter.
- Rotation regulation parameter (R_r): This specifies all macrocells used for performing scrambling.
- Hiding method parameter (H_p): This parameter specifies which data hiding is used.

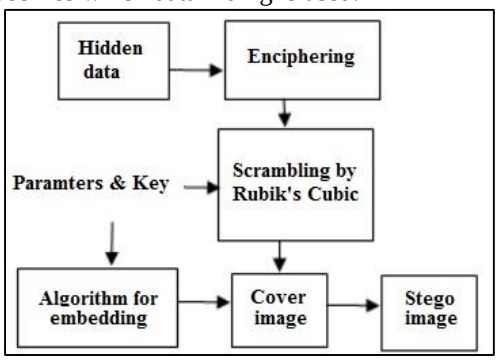

Fig. 4: The scheme data hiding using Rubik's Cubic scrambling

By the following procedure the proposed data hiding is implemented:

1) The parameters $M_p,\ H_p, R_r, R_p$ required are defined.
2) In order to strengthen the security of data the hidden data is encrypted using the cipher system
3) The scrambling of encrypted data is done by using Rubik's Cubic rotation.
4) To obtain the stego image, the data which is scrambled is embedded into the cover image.

By performing the above steps reversely, the hidden data can be extracted.

B. R-Prime Shuffle Technique

The R- Prime is the Relative Prime. If two numbers don't have any common factor except one then, those numbers are said to be relatively prime. The similarity matching between any two parts of the image can be found using the R- Prime shuffle technique. This method is also known as Template Matching. The measure which is used to find the similarity between the two rows or column in a digital image is the Cross correlation using FFT (Fast Fourier Transform). The correlation concept is used to choose an R- Prime number for the shuffling from the set. Between relative prime numbers and the first row or column the correlation is obtained and for the shuffling the lowest correlation is used as a key.

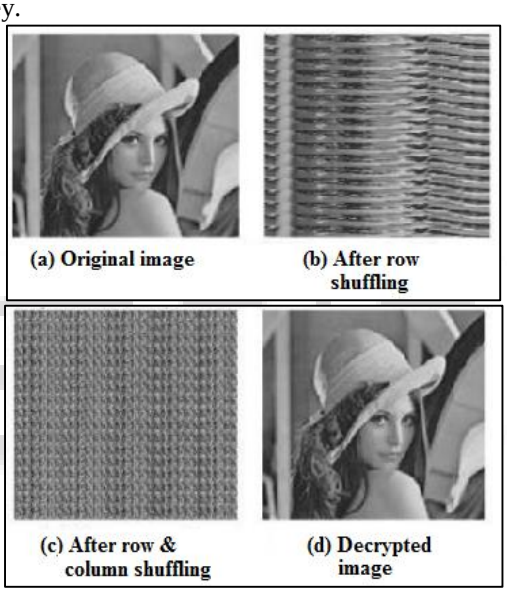

Fig. 5: R-Prime shuffling

For the encryption firstly, read the image. In the second step the image that has read is converted into gray-scale. Then all the relative prime numbers are found which is based on the image size and it is saved in the set S. After that the correlation is found between first row and remaining rows using the set S. Then to shuffle the rows in the image the lowest correlation is considered as the key. Until all the image positions are considered the process continues. The relative prime numbers are saved as a key which considered for the shuffling of row. Then for the shuffling of the column the same procedure is repeated.

For column and row shuffling different relative prime numbers are used therefore the technique is robust. And also the technique is simple but powerful for scrambling the image. But the techniques sometimes have a few seconds of delay for the encryption, but not involve a high complexity in case of time. If the relative prime number is kept as secret the decryption of the scrambled image is not possible.

C. Arnold Transform (Arnold cat map)

Arnold transform is also known as Cat mapping and simplicity is one the main feature of this method and it is cyclic and reversible. The Arnold cat map (Arnold transform) is given by:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \quad (1.1)$$

Here x, y represents the co-ordinates of the original image and x', y' represents the co-ordinates of the transformed image after performing this Arnold transform. Figure 6 shows an example of Arnold transform.

Fig. 6: The face is scrambled using Arnold transform

Arnold transform is a widely used scrambling technique. So, sometimes it is not efficient because it has a demerit. The demerit is that the four transform coefficients which are used in the method are fixed in nature. So, one can easily perform descrambling of the image by identifying that Arnold transform is performed for scramble the image by using the fixed value of those parameters (coefficients).

To overcome this problem, based on the Arnold transform a Block location scrambling algorithm of digital image is proposed. Its operations are similar to that of Arnold transform the exception from the traditional is that its matrix coefficients are different. As per the proposed method the traditional Arnold algorithm is transformed into:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ mod N} \quad (1.2)$$

For a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ when elements which satisfies the criteria, ad-bc = 1 is proved by QI DAONG-XU [6]. The coefficients of the transformation can be used as scrambling transformation. By this method we have only limited choice for choosing different matrix coefficients which is a demerit. Another demerit is that the first coefficient of the matrix is fixed to unity.

D. Improved Arnold Transform (IAT)

The traditional Arnold transform will not support scrambling of non- squared images. To overcome this limitation an improved method based on Arnold transform is proposed which converts the non- squared image into squared images and then the Arnold transform is applied to each squared images. During the recovering of original image from the scrambled image the IAT (Improved Arnold Transform) performs better than traditional version. The equation for IAT is given, which is the matrix for IAT:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} \text{ mod N} \quad (1.3)$$

A= $\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ is the transform matrix coefficient. This can be any matrix. The advantages of the IAT are in the case of conventional Arnold matrix it only uses a fixed set of matrix coefficients but in the case of improved Arnold transform it can use various sets of matrix coefficients. Another advantage is that in the case of conventional block location scrambling the first parameter is fixed as unity, so there are only two choices to select the rest of three coefficients but in IAT all the four matrix coefficients are different and therefore a lot of choices are there to choose the matrix coefficients. To calculate the difference between original image and transformed image there should be a scrambling factor. For the security of image the scrambling factor should be as high as possible, this results in the difficulty to attack the image which is done in the IAT.

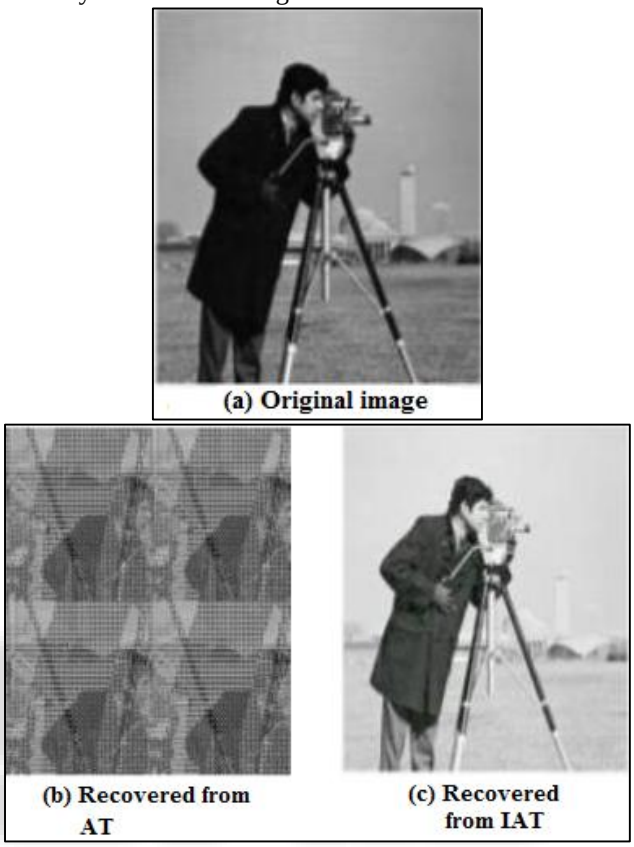

Fig. 7: Image recovered from AT and IAT

By dividing an image into four or sixteen sub-images the scrambling ratio can be improved. Then, on each image the Arnold transform is applied. By this the original image size can be changed. By knowing the transform coefficients which are exact ones and the size of image the true image can be restored at the destination side. Without knowing this the image cannot be restored so the image security is high by using this method.

III. Analysis of Image Scrambling Techniques

The various scrambling techniques that has be analyzed are Rubik's Cubic, R- Prime shuffling, Arnold transform and Improved Arnold transform. In the R- Prime shuffling the relative prime numbers are used as key therefore the technique is robust and also the technique is simple and powerful. But one of the disadvantages is the encryption process take some delay but not a high time complexity. At the same time as long as the R- Prime is kept as secret the decryption of the scrambled image is not possible. When comparing the Rubik's Cubic and Arnold transform, in the case of Arnold transform the basic processing unit can be only pixel but in the case of Rubik's cube it can be pixel, small blocks or macrocells. When taking other criteria such as scrambling times, In Rubik's Cubic scrambling can be done any times but in Arnold transform it is based on the

number of pixel. In the Rubik's Cubic the security is higher than Arnold cat map. The improved version of the Arnold transform is IAT (Improved Arnold Transform) in which the disadvantage of the traditional Arnold method such as it will works on squared image can be overcome. The recovery image from IAT is better than AT (Arnold Transform).

IV. CONCLUSION

Nowadays the security of the image is a major issue. For the security purpose various image scrambling techniques are proposed. In this paper some scrambling techniques are surveyed, which are useful for real- time image scrambling. Each of them is suitable for applications of image encryption. These scrambling techniques can be used before or after embedding data into the image. The surveyed techniques have the characteristics such as 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] 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
[3] 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
[4] G.Artist, M.Porwa " Dual Layer Image Scrambling Method Using Improved Arnold Transform"American International Journal of Research in Science, Technology, Engineering & Mathematics, vol .3, pp. 258-264 , February. 2015.
[5] Richard Jiang, Somaya Al-Maadeed "Face Recognition in the Scrambled Domain via Salience-Aware Ensembles of Many Kernels "IEEE Transactions on information forensics and security, vol 11, no.8, August
[6] 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 IEEE. pp. 2942-2947.

