iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Digital Image Scrambling Encryption Techniques

Dhananjay Santosh Waghulde[1], Dr. P. M. Mahajan[2]
[1,2] Department of Electronics & Telecommunication, North Maharashtra University, Jalgaon

Abstract*: Digital image scrambling encryption technology is a way of securing digital image information. With the use of transformation techniques, it can change the original image into a disordered one beyond recognition, making it difficult for those who get the image in unauthorized manner to extract information of the original image from the scrambled images. In this paper, we have discussed basic principles of digital image scrambling encryption. We have reviewed the transformation techniques of the scrambling encryption. The literature survey and working of these scrambling transformation techniques is presented. The system has many functions: data hiding mechanism, reversibility and good visual quality, better encryption.

Keywords— Digital Image, Image Scrambling Encryption, Arnold Transformation, R-prime shuffle, Random Number Generation

I. INTRODUCTION

A. DIGITAL IMAGE

The digital image composed of many image points. This image points also namely pixels, are of spatial coordinates that indicate the position in the image, and intensity (gray level value). An image as described above refers to a grayscale image (2 D image). A colored image accompanies high dimension information than gray image (3D, 4D), as red, green and blue values are typically used in different combination (color systems) to reproduce the colors of an image in the real world. An image defines as two dimensional functions, where x and y are coordinates and f is amplitude, or gray level value at the point. When x, y and f are all discrete finite values, we call the image a digital image [1].

B. Digital image scrambling encryption

Scrambling a digital signal in the spatial or the frequency domain corresponds to modify that signal in such a way that the original semantic media loses its meaning and become hard to be viewed (the inverse of scrambling is descrambling). Refer to transforming the digital image into another completely different digital image. The users only know the algorithm and keys; this allows them to restore the original image. Also image scrambling can be seen as encryption. The plain text is the original image and the cipher text is meaningless noises for unauthorized users [2].

Compared with traditional cryptography, digital image has a large amount of data, thus it has a lot of clear space, and also has a great cipher text space, and the most important is the autocorrelation of the digital image visually manifested direction of perpendicular and direction of various tilt angles. Therefore, when considering the scrambling encryption algorithm we should fully consider the impact of algorithm on the image autocorrelation, the worse the autocorrelation the better the scrambling, the poorer the intelligibility of the image after scrambling. Therefore, the conventional cryptography encryption algorithm has a strong security, but the effect of encrypting image is not necessarily the best [4].

C. Generalized Scrambling Encryption Process

Image scrambling encryption disarrange pixel position or pixel color in order to make it unrecognizable and finding the algorithm to rebuild the original image. With the use of transformation techniques, it can change the original image into a disordered one beyond recognition, making it hard for those who get the image in unauthorized manner to extract information of the original image from the scrambled images [3].

The scrambling encryption process of digital image is essentially a process of coding and decoding of a class of image. When the third capture confusing image, since the parameters of scrambling algorithm are confidential, even in the case that the algorithm is known it is also difficult to decipher. The image scrambling requires that the image has a lower intelligibility after scrambling; the scrambling image should have a certain degree of security after scrambling, and can withstand a certain degree of attack. Digital

image scrambling cannot change the resolution of images; the images that remove the scrambling have undifferentiated or little difference with original image, and can be able to accurately express the content or meaning of the original image. Figure 1.1 shows generalized block diagram of image scrambling [4].

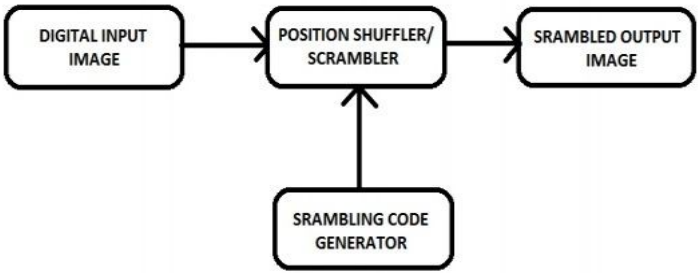


Fig. 1.1: Block Diagram of Image Scrambling

In image scrambling and descrambling encryption, it is imperative to have simple algorithm to 'shuffle' the pixel values fast and reorder it to reveal the original. It builds a pseudorandom sequence using the user defined long positive integer value sequence. Since these values are used for image pixel row and column shuffling, the values usually have a lower and an upper limit. This provided sequence is used to generate a longer sequence that is as long as the maximum dimension of the image (length or width). We have few options to generate the longer sequence from the user provided sequence. One option would be to periodically insert the user provided sequence in order to generate the longer sequence. In order to shuffle the image well, we can increment each value of the shorter sequence whenever it is repeated in the longer sequence [5].

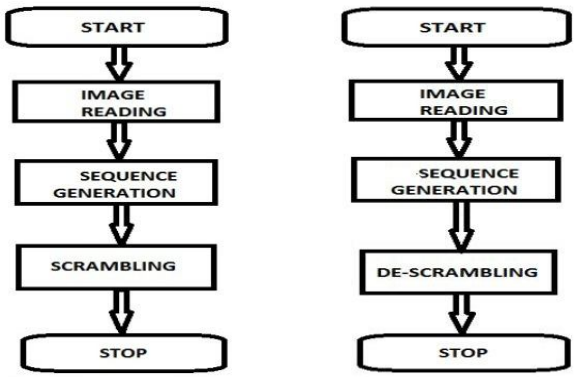


Fig. 1.2: Flow cart for image scrambling encryption

Once the shuffling order sequence is generated, which is the 'key' in this process, sequence values are read and the rows are switched. Once all rows are switched according to the key sequence, columns are switched using the same sequence. At this stage the amount of scrambling achieved is visually not acceptable. Thus this process is now followed by circular shifting of rows and then the columns using the key sequence [5].

II. LITERATURE REVIEW

Zhenwei Shang et al. [6] proposed an image block location scrambling encryption algorithm based on Arnold transformation which has been very widely used in literature. In this work 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 good encryption effect and has the lager key space.

Shiva Shankar et al. [7] introduced the data hiding in encryption images using Arnold transform. This work is based on Arnold

transform applied on blocks of the image. This work presents a method which replaces the LSB of the image blocks by the secret message and then applying Arnold transform followed by random diffusion a certain number of times according to the secret message digit. The number of times the transform is applied depends on a secret message expressed in a higher base. In order to identify the correct number of times the transform is applied, check bits are added to the LSBs. The security aspects of the system are analyzed.

Vineeta Singh, Vipin dubey [8] introduced two level image security based on Arnold transform and logistic mapping. In this work the hybrid Arnold transform scheme based on DWT is used, a double layer of security is provided by utilizing the multi-resolution property of wavelet using Arnold transform and chaotic logistic mapping. Scheme provides high security as even after the extraction of first layer, without knowing the extraction algorithm, original image cannot be recovered in its entirety.

H. B. Kekre et al. [9] proposed an image scrambling algorithm using the concept of relative prime numbers. One of the main goals of an image scrambling algorithm is that the correlation between any two rows and columns has to be minimum. Considering this aspect in this work 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 work shows 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.

H. B. Kekre, Tanuja Sarode, Pallavi Halarnkar [10] Perfect shuffle for image scrambling is introduced. The numbers of patterns are used to generate the prefect shuffle. Effects of perfect shuffles with different factors of the image size are discussed in this work. Lena grayscale image of size 1024 X 1024 was used for analysis of experimental work. This work shows number of iterations required to get back the original image are related to the power of 2.

H. B. Kekre, Tanuja Sarode, Pallavi Halarnkar [11] introduced an image scrambling algorithm using R- prime shuffle technique for digital images and extended over the blocks of digital image. In this work the method is applied to different block sizes in image. For the experimental purpose five images of Lena, Mountain, Forest, Lotus and fruits of 256x256 were used. Method used in this work is R- prime shuffling on the blocks of the digital image, to increase the security of image data, different relative prime numbers are used for row and column shuffling for every block. Work shows combination of all the R-primes from each block with respect to rows and columns can be used as key and from experimental results it concludes the technique takes few seconds for encryption process.

Jiancheng Zou , Rabab K. Ward , Dongxu Qi [12] presented a method for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real-time situations. The scrambling effect is very sensible, the data of the image is re- distributed randomly across the whole image. The method can endure common image attacks, such as compression, noise and loss of data packet .They developed a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

Shao. Z. Qin et al. [13] a new scrambling algorithm based on random shuffling strategy is discussed, which can scramble non equilateral image and has a low cost to build coordinate shifting path. The algorithm has a good one time scrambling performance. It can be used to scramble or recover image in real time and can also resist the JPEG compression attacks. Experiments show the scrambling method validity in scrambling or recovering non equilateral image and robustness in enduring erasing, cropping and JPEG compressing attacks.

Makera M. aziz et al. [14] discussed the simple algorithm to encrypt and decrypt the grey level image base on the random number generation. The image encrypt by changing the position of each pixel in the original image without changing the value of grey level. The original image reads row by row pixel by pixel each pixel will take a new position in encrypt image. The new position chose based on random number generation from the random number generators. The key will generate during the encryption process. Three grey level images with different size and type were used in this work. Experimental results show the decrypt image is clear without noise.

Shuqun Zhang and Mohammad A. Karim [15] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green- Blue) formats. The proposed single-channel color image encryption method is more compact and robust

than the multichannel methods.

III.IMAGE SCRAMBLING TECHNIQUES

A. Arnold Transformation Based Image Scrambling Encryption

The Arnold transform is an image scrambling technique that can be used to encrypt and decrypt image data. The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image [16].

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.

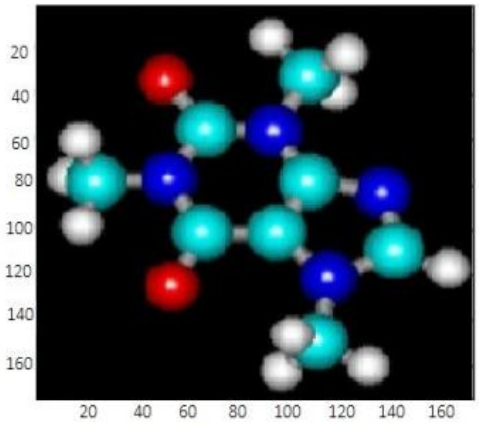


Fig. 3.1: 175 × 175 iage of a caffeine molecule

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

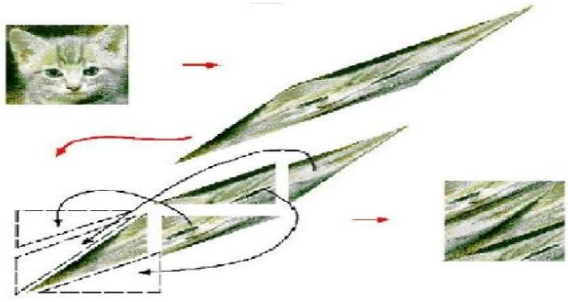


Fig. 3.2: Visual illustrating the steps

Figure 3.2 shows the shearing in the x and y directions, followed by modulo operation and then the reassembly of the image.

Arnold's cat map is the transformation

$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} mod\ n \qquad \text{.....(1)}$$

Where mod is the modulo of the

For $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ understanding ..... (2) of the transformation better, it can be decomposed into elemental pieces.

1. Shear in the *x*-direction by a factor of 1.
$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix} \quad \text{.....(3)}$$
2. Shear in the *y*-direction by a factor of 1.
$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix} \quad \text{.....(4)}$$
3. Evaluate modulo.
$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} mod\ n \quad \text{.....(5)}$$

Arnold transform is an efficient technique for position swapping, and widely applied to image encryption. But, Conventional Arnold transform based schemes have a common weakness that image height must equal image width. The two dimensional Arnold transforms only scrambles the positions and leaves the grayscale values intact. This allows Eve to confirm whether the image was a particular one in her possession. This makes brute force attacks likely to deduce the original image by randomly applying inverse Arnold transform several times and checking against a standard natural image model.

IV. IMAGE SCRAMBLING ENCRYPTION USING 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.

A. 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.

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 as shown in figure 3.3, it can be observed that there is a reduction of approximately 50% in the correlation between rows and columns of the encrypted image.

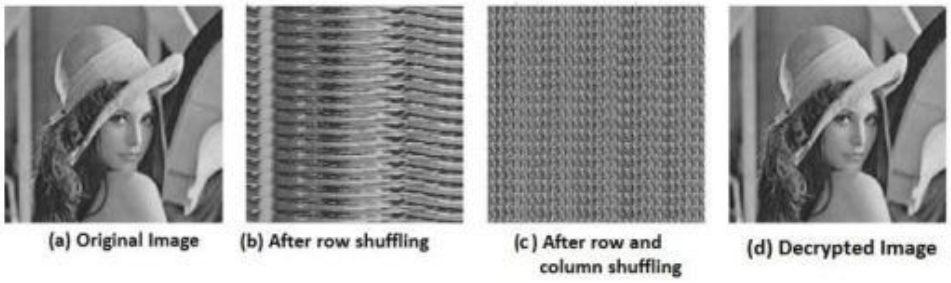


Fig. 3.3 Image Scrambling Encryption using R-Prime Shuffling.

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.

V. SCRAMBLING ENCRYPTION BASED ON RANDOM NUMBER GENERATION

The methodology of this algorithm will create, encrypt image with a secret key in encrypt process and create decrypt image in decrypting process. The original image will read. The encrypted image will build randomly and the decrypt image will rebuild. Two algorithms are used one for the encrypt original image, second is for decrypt image. In encrypt processing two random number generates for each pixel one for the row the range of this number starts from 1 to the total number of rows and the following equation to generate the number from a two b. a=1 and b= total number of rows. n1=round ((b-a). *rand+a);The second number of the columns in the range of these numbers start from 1 to total numbers of columns and the same equation use to generate numbers from 1 to see when c equals the total amount of columns.

A. The encryption algorithm includes following steps

1) Input original image.
2) Find the size of the original image (the total number of rows and column).
3) Point to the first pixel in the original image.
4) Let counter equal to 1.
5) Generate new position of the current pixel in the encrypt image by generating two random (n1, n2) numbers, one for row the other for the column.
6) While the new position of encrypt image is generated before go to step 4 otherwise go to step6.
7) Save the value of n1 in the array k1 (counter).
8) Save the value of n2 in the array k2 (counter).
9) The current pixel of the original image will take the position (n1, n2) in encrypt image.
10) While all the pixels of original image finished, go to step13 otherwise go to step10.
11) Point the next pixel in the original image.
12) Increment counter by 1.
13) Go to step 5.
14) End.

B. The decryption algorithm includes following steps

1) Input the encrypt image.
2) Input the key k1 and k2.
3) Set counter equal to 1.
4) Point to the first pixel of the decrypt image.
5) n1=k (counter).
6) n2=k2 (counter).
7) Get the value of the position (n1, n2) from the encrypt image and put it in the current position of decrypt image.
8) While the counter is not the last position of k1 and k2 go to 9 otherwise go to 13.
9) begin.
10) Increase counter by one.
11) Point to the next pixel of encrypt image.
12) Go to 5.
13) End.
14) End.

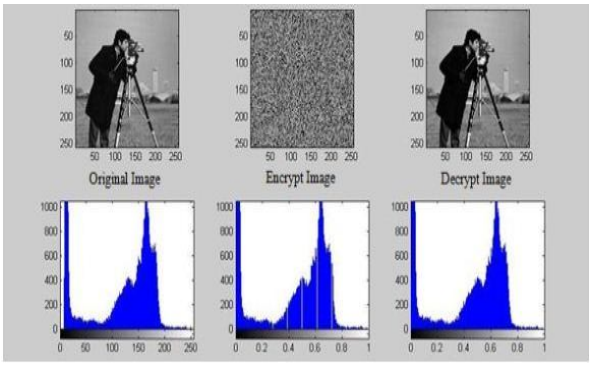


Fig. 3.4: Random Number Generation Scrambling Encryption

The original image will read row by row. The first pixel in the original image will use to build the first pixel in encrypt image by changing the position. The new position of the pixel will chose randomly by generating two random numbers (n1, n2), when n1 represent the row number for a new position and n2 represent the column number of new positions. The same procedure will do for all pixels.

The new position chose based on random number generation from the random number generators. The key will generate during the encryption process. The key that will used to decrypt image, it will generate as a matrix. The key saves the position of each pixel in encrypt image. The encrypted image will decrypt by using the key. Each pixel in encrypt image return back to its first position in decrypt image position that saved in key then the decrypt image builds as shown in figure3.4.

From the histogram of image in three case (original image, encrypt the image and decrypt image) are showing that there is no change of the grey value only the change in position only. We get the decrypt image without any noise or damage.

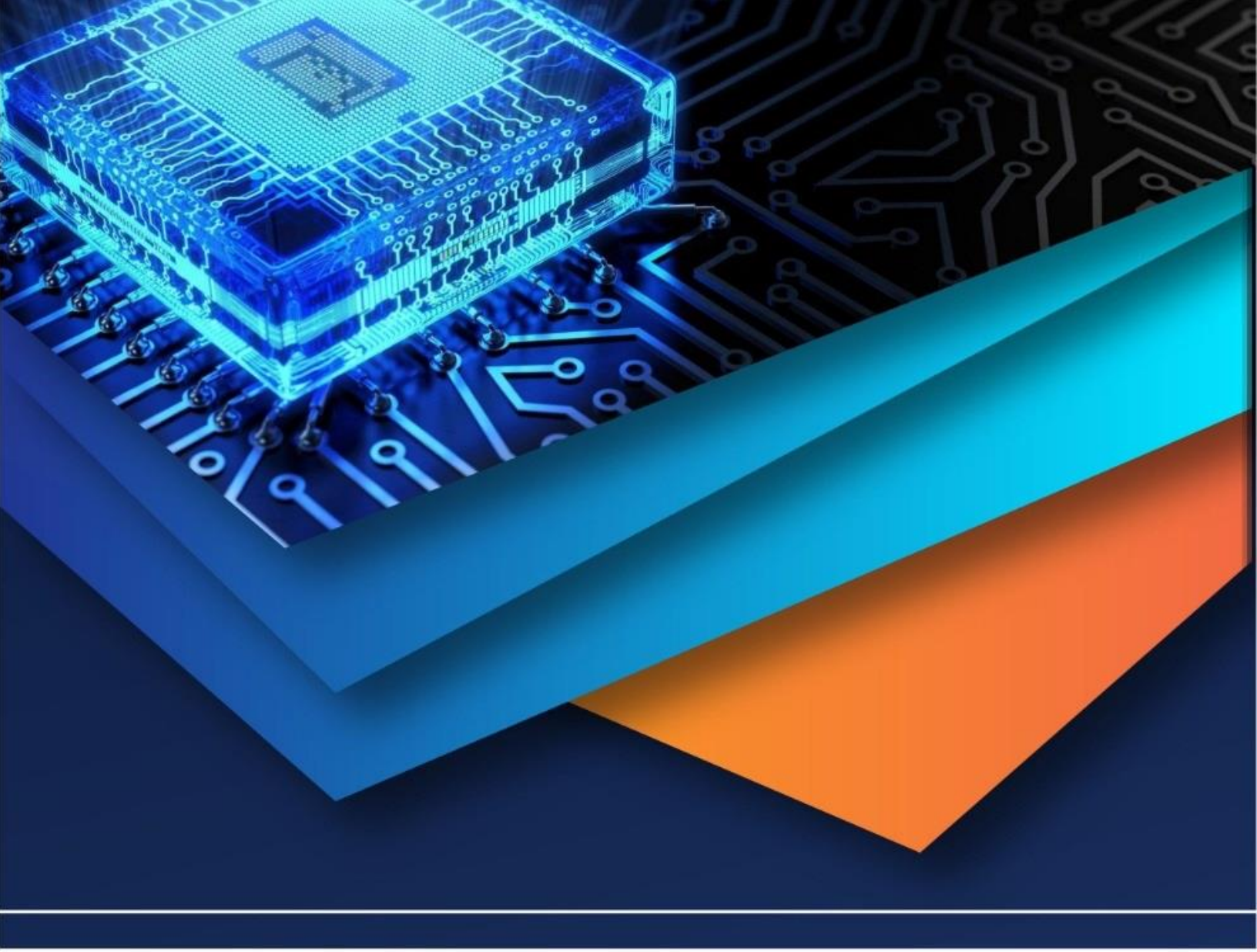
VI. CONCLUSIONS

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

REFERENCES

[1] Gonzalviz Woods " Digital Image processing book".
[2] Yan, WeiQi, and Jonathan Weir, Fundamentals of Media Security. Bookboon, 2010.
[3] Zhao Xue-feng, "Digital image scrambling based on the baker's transformation". Journal of Northwest Normal University (Natural Science),vol.39, pp26-29, February .2003.
[4] Wenquing Chen, Tao wang and Bailing Wang, "Design of Digital Encryption Algorithm Based on chaotic Sequences" International Journal on smart Sensing and Intelligient Systems Vol. 7, no. 4,December 2014.
[5] P. Premaratne and M. Premaratne, "Key-based scrambling for secure image communication," in Emerging Intelligent Computing Technology and Applications, P. Gupta, D. Huang, P. Premaratne and X. Zhang, Ed. Berlin: Springer, 2012, pp.259-263.
[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.
[7] Shiva Shankar S., A Rengarajan, "Data Hiding In Encrypted Images Using Arnold Transform," ICTACT Journal On Image And Video Processing, Volume: 07, Issue: 01, August 2016.
[8] Vineeta Singh, Vipin Dubey, "A Two Level Image Security based on Arnold Transform and Chaotic Logistic Mapping," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015.
[9] H B Kekre, Tanuja Sarode, Pallavi Halarnkar, "Image Scrambling using R-Prime Shuffle," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, volume:2, Issue:8, August 2013.
[10] H B Kekre, Tanuja Sarode, Pallavi Halarnkar, "Study of Perfect Shuffle for Image scrambling" International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.
[11] H B Kekre, Tanuja Sarode, Pallavi Halarnkar, "Image Scrambling Using R-Prime Shuffle on Image and Image Blocks" Internationational journal of Advanced Research in Computer and Communication Engineering, Volume 3, Issue 2, February 2014.
[12] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number," Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.
[13] Shao Z. Qin, B. Liu J. Qin and H Li., "Image Scrambling Algorithm Based on Random Shuffling Strategy", in ICIEA 2008, pp. 2278-2283.

[14] Makera M Aziz, Dena Rafa Ahemad "Simple Image Srambling Algorithm Based on Random Number Generation" IJARCSSE, volume 5, issue 9,September 2015.
[15] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.
[16] W.Chen, C.Quan and C.J.Tay. "Optical Color Image Encryption based on Arnold Transform and Interference Method", Optics Communications, Vol. 282, No. 18, pp. 3680-3685, 2009.
[17] S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan," Image Scrambling Algorithm Based on Random Shuffling Strategy" 3rd IEEE Conference on Industrial Electronics and Applications, 2008,pp. 2278 – 2283.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY