A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern

Monisha Sharma, PhD,Sr. Associate professor ,Faculty of Engineering,
Shri Shankarcharya Group of Institution, Bhilai, India

Chandrashekhar Kamargaonkar, Associate Professor, Faculty of Engineering,
Shri Shankarcharya Group of Institution, Bhilai, India

Amit Gupta,Master of Engineering Scholar,
Shri Shankarcharya Group of Institution, Bhilai, India

***Abstract*-This is new image encryption method where image is incrypted by simple specific rule that is rearrangement of pixles. In this paper, we present Image encryption and decryption by using partition and scanning pattern which is related to scan methodology. SCAN language is based on spatial accessing methodology that can generate a wide range of scanning paths. This paper presents a brief over view of encryption and decryption algorithm, implemented in MATLAB environment and tested on various images.**

Index Terms- Image Encryption, Decyption, Scanning, Partition

1. Introduction

Security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption has a wide range of applications in inter-net communication, multimedia systems, medical imaging, tele medicine, and military communication. There already exist several image encryption methods like SCAN-based methods, chaos-based methods, tree structure-based methods, and other miscellaneous methods. However, each of them has got their own strengths and weakness in terms of security level, speed, and stream size metrics. Hence, we now propose a new encryption method that would make an attempt to address the above mentioned problems.

The proposed image encryption method is based on rearrangement of the pixels of the image. The rearrangement is done by scan patterns that generated by the SCAN methodology. The scanning path of the image is a random code form, and by specifying the pixels sequence along the scanning path. Note that scanning path of an image is simply an order in which each pixel of the image is accessed exactly once. Such an encryption also involves the specification of set secret scanning paths. Therefore, the encryption needs a methodology to specify and generate a larger number of wide varieties of scanning paths effectively.

2. About scan language

The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths. The SCAN is a family of formal languages such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. Each SCAN language is defined by a set of basic scan patterns, a set of partition patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns and transformations with scanning or partitioning.

A scanning of a two dimensional array A = {a(I, j): $1 \le i \le m$, $1 \le j \le n$} is a bijective function from A to the set{1,2,…,pq-1,pq}. In other world, a scanning of a two dimensional array is an order in which each element of the array is accessed exactly once. In this paper the terms scanning, scanning paths, scan pattern, and scan words are used interchangeably. Note that an p×q array has (p×*q*)! scannings.

2.1 Basic partition pattern

There are three basic partition patterns that include

- B type partition patterns
- Z type partition patterns
- X type partition patterns

These are clearly shown in the figure 2.1.1.

Figure 2.1.1 Basic partition patterns

Each basic partition pattern has eight different transformations which depends on initial point and the final point which are as shown in the figure 2.1.2 .

B type partition pattern can be defined as B0, B1, B2, B3, B4, B5, B6, B7 as in fig. 2.1.2 (a)

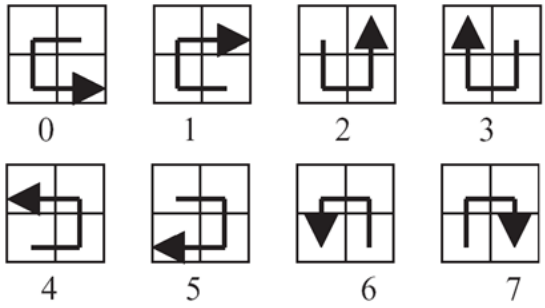

Figure 2.1.2 (a) Transformation of partition B

Similarly, Z type partition patterns can be defined as Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7 as seen in fig. 2.1.2 (b)

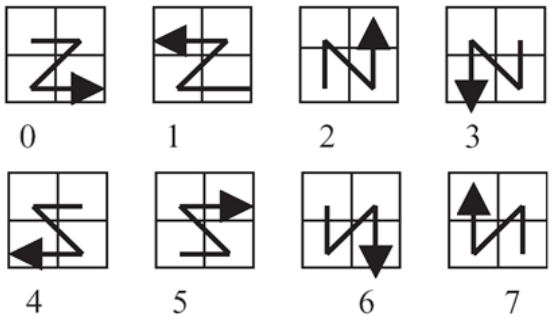

Figure 2.1.2 (b) Transformation of partition Z

And X type partition patterns can be defined as X0, X1, X2, X3, X4, X5, X6, and X7 which is shown in fig 2.1.2 (c)

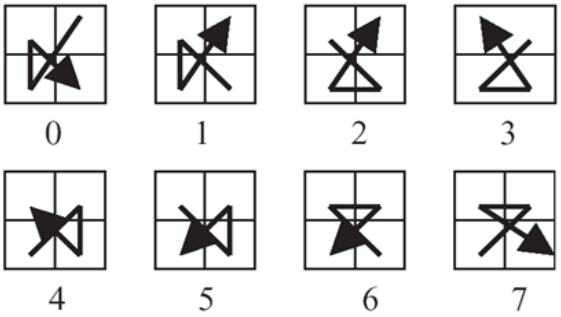

Figure 2.1.2 (c) Transformation of partition X

2.2 Basic Scanning Pattern

We have four basic scanning patterns namely,

- Continuous Raster C
- Continuous Diagonal D
- Continuous Orthogonal O
- Spiral S

All the above mentioned scanning patterns are clearly shown in figure 2.2.1

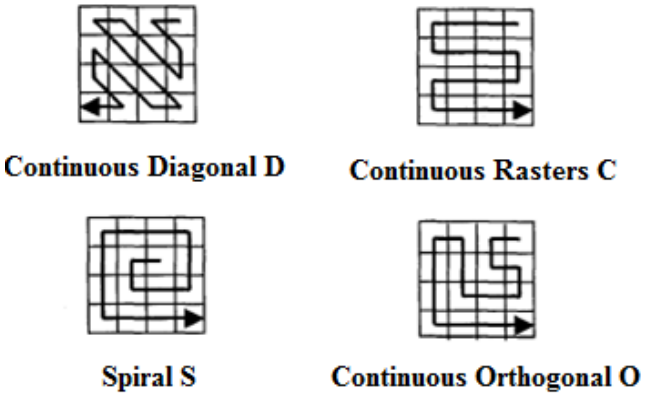

Figure 2.2.1 Basic scanning pattern

Each scanning pattern can be rotated through an angle of 0^0, 90^0, 180^0 and 270^0 which can be represented as C0, C2, C4, C6.

When the same pattern reverses, it takes the order of C1, C3, C5, C7

These are again shown in the following figure 2.2.2

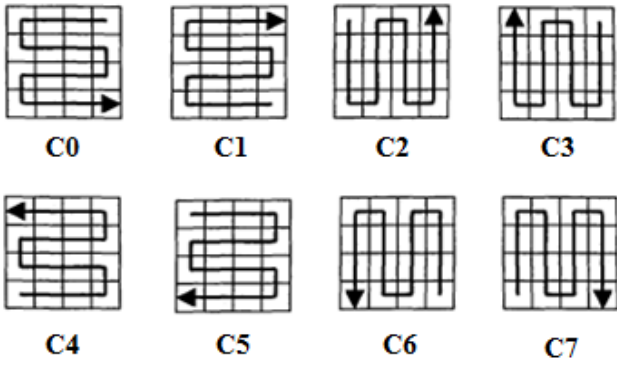

Figure 2.2.2 Eight Transformations of continuous Rasters C

Similar rotation of the continuous diagonal pattern yields the following set of figures shown, with the order of D0, D1, D2, D3, D4, D5, D6, D7 which is applied in the same fashion for the Continuous orthogonal and the spiral patterns with the respective orders of O0, O1, O2, O3, O4, O5, O6, O7 and S1, S2, S3, S4, S5, S6, S7 upon rotation through the angles of 0^0, 90^0, 180^0 and 270^0.

These are similarly represented in the following set of figures namely 2.2.3, 2.2.4 and 2.2.5

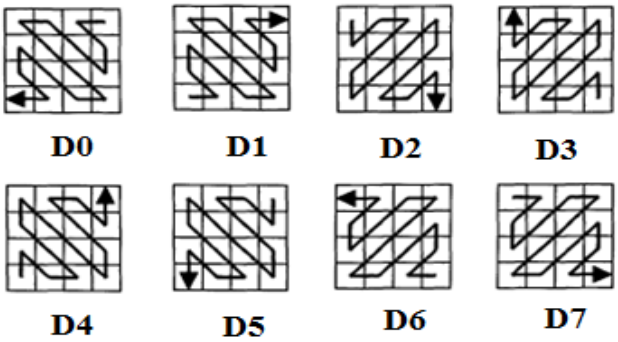

Figure 2.2.3 Eight Transformations of continuous Diagonal D

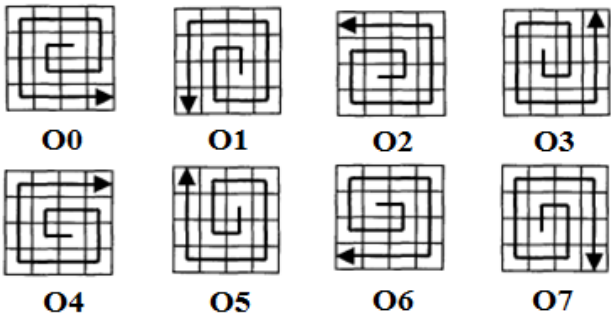

Figure 2.2.4 Eight Transformations of continuous Diagonal O

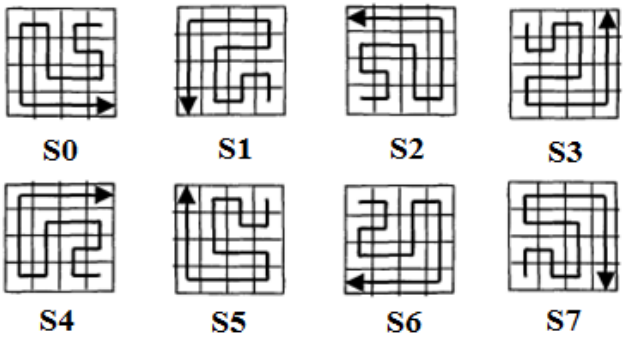

Figure 2.2.5 Eight Transformations of continuous Diagonal S

3. Methodology

Since most images require different scanning in different subregions, the encryption specific SCAN language allows an image region to be recursively partitioned into four subregions, and each subregion to be scanned independently. When an image region is partitioned, the order in which the four subregions are scanned is specified by a partition pattern.

The partition patterns are represented by letter B, letter Z, and letter X, each of which has eight transformations as previous mention.

Following by basic scan patterns and partition patterns to produce concept, we use a random code generating produce the SCAN word and to define encryption key. The SCAN word contain scan and partition patterns.

The scan partition word has c0~c7, d0~d7, O0~O7 and s0~s7. The partition word has B0~B7, Z0~Z7 and X0~X7. This word separately has been done using special scanning paths and partition. Because the SCAN word has large variation, so we can attain encryption technology.

A given image is encrypted by rearranging the pixel of the image using a set of scanning paths.

This paper proposed encryption key rules assume that maximum image size is 512× 512. The partition institution least is 4 × 4 image size, then the least size done scan patterns. However the scan patterns institution when the image not done partition.

Consider the 16× 16 size image and the scanning path shown in Figure 1. The scanning path is corresponding to the SCAN word constructed as follows. The SCAN word defines encryption key can achieve encryption objective.

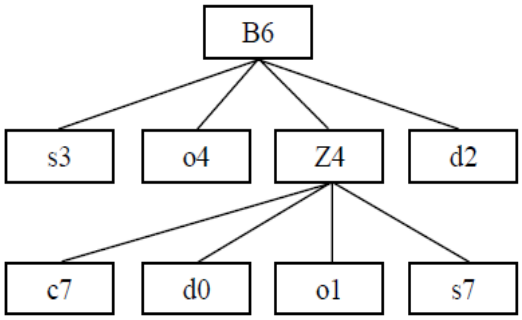

Figure 3.1 (a) SCAN word diagram

Encryption key B6(s3 o4 Z4(c7 d0 o1 s7) d2)

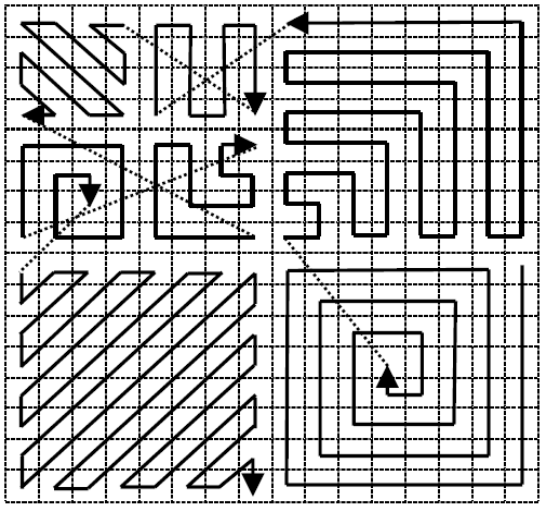

Figure 3.1 (b) The scanning path by 16× 16 size image

4. Encryption/Decryption algorithm

For a given 2D, $2^k \times 2^k$, $2 \geq k \geq 9$ image, the encryption algorithm transforms it into one dimensional strings of length 22k firstly. Then each arrangement strings of length are encrypted using random generating encryption keys. Additionally the encryption keys have 32 possible groups

Figure 4.1 illustrates how we encrypt a 4 ×4 image. Transform one-dimensional string of length 16 using an encryption key. Then wide string data according filled the new 4×4 encryption image. The encryption is done by the Encrypt ( ) function. Under describe Scan( ), Partition ( ), Random code ( ), Encrypt ( ) and Decrypt ( ) algorithm. Note the Scan ( ),n Partition ( ) algorithm is symmetry, so only description encryption part.

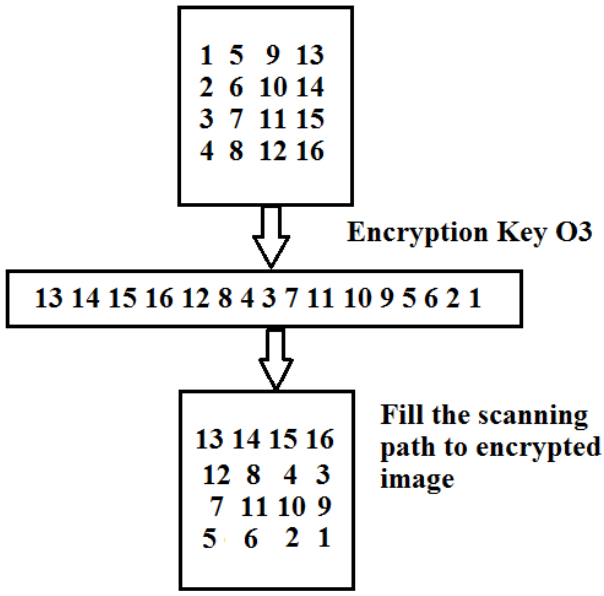

Figure 4.1 Illustration of encryption

5. Result

The proposed encryption methodology was implemented in software using MATLAB 7.1 Figure 5.1 shows the 256 × 256 gray-scale Lena and air fighter image. The process encryption image is compliance the encryption key. It is clear that the SCAN methodology image encryption and decryption achieves an excellent encryption.

From previous mention, it is clearly known that we have 3 × 8 possible partition and 4 × 8 possible scan patterns. Due to us randomly select the partition and/or scan pattern. We hence have encryption key have

$$32, k = 2; (3\times 8)\sum_{i=0}^{k-3} 4^i \times (4\times 8)^{4^{k-2}}, 3 \geq k \geq 9$$

Possible groups of encryption keys.

When execute partition has 3× 8 possible or scan pattern has 4× 8 possible. Select execute partition or scan pattern is random decision.

Figure 5. 2. illustrates a 16 × 16 example, which calculates how the possible encryption keys may exist. That is,

$$(3\times 8)\sum_{i=0}^{1} 4^i \times (4\times 8)^{4^2} = (3\times 8)^5 \times (4\times 8)^{16}$$

possible groups.

Figure 5.1 **Car Encryption Image diagram**

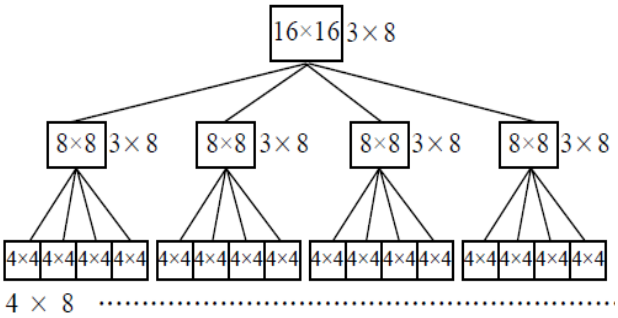

Figure 5.2 16*16 Image Possible groups diagram

6. Conclusions

The method proposed in this paper has got a lossless encryption of image. This also gives access to variable lengths of the encryption keys.

Another main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible.

This Encryption uses only integer arithmetic and it can be easily implemented in the hardware.

7. References

[1] Tzung Her Chen,Kai HsiangTsao,and Kuo Chen "Image Encryption by Random Grids" in Proceeding of IEEE Internationl Conference

[2] Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins " Digital Image Processing", Pearson Education

[3] J N.Bourbakis, A Language for Sequential Access of Two Dimensional Array Elements, *IEEE* Workshop on *LFA*, Singapore, 1986, pp 52-58.

[41 N-Bourbakis, C.Alexopoulos, A Fractal Based Image Processing Language – Formal Modeling, *Pattern Recognition Journal*, vol 32, no 2, 1999, pp 317-338.

[5] C.Alexopoulos, N.Bourbakis, N.Ioannou, Image Encryption Method Using a Class of Fractals, *Journal* of *Electronic Imaging*, July 1995, pp 251-259.

[6] N.Bourbakis, Image Data Compression Encryption Using G-SCAN Patterns, *IEEE Conf* on *SMC*, Oct 1997, pp 11 17-1 120

[7] W.Pennebaker, J.Mitchel1, *JPEG Still Image Data Compression Standard*, Van Nostrand Reinhold, 1993.

[8] JBIG Progressive Bilevel Image Compression, ISO/IEC International Standard 11544, 1993 498

[9] P.Howard, J.Vitter, Fast and Efficient Lossless Image Compression, *Proc. Data Compression Conf*, 1993, pp 351-360.

[10] X.Wu, N.Memon, CALIC - Context Based Adaptive Lossless Image Codec, *IEEE Int. Con$ on Acoustics, Speech and Signal Processing*, vol 4, May 1996, pp 1890-1893.

[11] M. Weinberger, J.Rissanen, R.Arps, Applications of Universal Context Modeling to Lossless Compression of Gray Scale Images, *IEEE Trans. on Image Processing*, vol 5, no 4, 1996, pp 575-586.

[12] M.Weinberger, G.Seroussi, G.Sapiro, LOCO-1: Low Complexity Context Based Lossless Image Compression Algorithm., *Proc. Data Compression Conf*, 1996, pp 140-149.

Author Profile

Dr. Monisha Sharma is an Sr. associated professor in the department of Electronic & CommunicationEngineering at Shri Shankarcharya Group of Institution, Bhilai,India. She was awarded Ph.D.(Electronics)degree on "Development of Highly Secured Image Encryption algorithm using multi chaotic sequences" from C.SV.T.U., Bhilai on 2010. She has published more than 46 papers in national/ international journals/conferences. She Awarded as Chhattisgarh Young Scientist Award in 2008 for "Generation of secured image for Telemetry using Adaptive Genetic Algorithm" by C.G Council of Science and Technology . Her research interests include Digital Image Processing, Secure communication, Cryptography, Stenography, Stegnanalysis, Cryptanalysis, Error Codes

Chandrashekhar Kamargaonkar is an associated professor in the department of Electronic & Communication Engineering at Shri Shankarcharya Group of Institution,.Bhilai India. He is M.E. Coordinator in the Department of Electronic &Communication Engineering at S.S.G.I. Bhilai India.He has more than 9 year experience in teaching. He has received Master Degree(M.E.) in digital electronics from S.S.G.M. College of Engineering, Shegaon India. His current area of research include Image Processing, Digital Communication, Microcontroller & Embeded System.

Amit gupta is a scholar of master of engineering in the department of Electronic & Communication Engineering at Shri Shankarcharya Group of Institution,.Bhilai India. He has received bacholer Degree(B.E.) in electronics and telecommunication from SSCET. Bhilai. His current area of research include Image encryption and decryption