A Novel Image ENCRYTION Algorithm for Enhanced Security

Miss.Amrita Singh,
Asst. Professor
Dr.C.V.Raman University
Bilaspur (C.G.)

Miss.Laxmi Goswami
Asst. Professor
Dr.C.V.Raman University
Bilaspur (C.G.)

Aijaz Ur Rahman Khan
Asst.Professor
M.M.College of Technology
Raipur(C.G.)

*Abstract-**The main aim of this paper is to develop a novel encryption algorithm for increasing the security of encryption so that only the intended person is able to decrypt the image. In this algorithm, original image is first encrypted using SCAN based encryption operation followed by ElGamel based encryption method. Various analysis has been done to test the performance of proposed algorithm.***

Keywords : Image encryption, SCAN , Spiral, Orthogonal, Diagonal, Raster, MSE.

I. INTRODUCTION

The advancement in communication and internet technology has given a quick and fast mode of communication using world wide web. Though this mode of information interchange is very fast but at the same it also creates security problem. Encryption is one way of ensuring the security in text, image, audio and video data. Image encryption play very important role in telemedicine, medical imaging, military communication,multimedia system. Various image encryption method has been proposed by different researcher in the past which include chaos-based image encryption method[1],SCAN-language based encryption method[2-5],tree structure-based encryption method[6] and some other method[7-9].Some methods provides better security while other method are very efficient in term of speed. In any kind of public key crypto system, security depends on the difficulty of factoring. In 1985 [10],[11] ElGamel proposed an encryption method whose security depends on the difficulty of computing the discrete algorithms. His method of encryption require a large prime number p and its primitive root r.High level of security is ensured by using big key size[12] because big size key require a very extensive computation and hence more difficult to decrypt[13].In this paper an effort has been made to design a novel and more secure method of encryption by combining two different methods.

The proposed encryption method starts by rearranging the image pixel. In this method pixel rearrangement is carried out by different scan pattern using SCAN methodology. Scanning pattern of an image is simply a arrangement order of a pixel. Since different scan pattern has different arrangement order therefore it can be used for encryption by

generating a large number of scan pattern .Once the image is encrypted using SCAN based methodology then it is again encrypted using elgamel encryption method to enhance the security of encryption. Since ElGamel encryption method provides good security and least complexity therefore it is chosen along with the SCAN based methodology.

II. SCANNING METHOD

SCAN [2-5] is a formal language based method of accessing or arranging the position of pixels in an image.Using SCAN language,large number of scanning path can be generated. SCAN is actually a group of formal language and can be termed as Simple SCAN, Generalized SCAN, Extended SCAN. Each SCAN language follows some basic rules and grammer. There are some basic pattern of scanning and rule in each SCAN language which are used to generate some simple scanning pattern which later on can be used to generate complex scan pattern. In this proposed method four basic scan pattern has been used which are known as continuous diagonal(D),continuous raster(C),continuous orthogonal(O), spiral(S).Each of these basic pattern can have eight different transformations which can be numbered from 0 to 7.Transformation 0,2,4,6 are the reverse transformation of 1,3,5,7.Different types of basic scanning pattern[16] is shown in figure

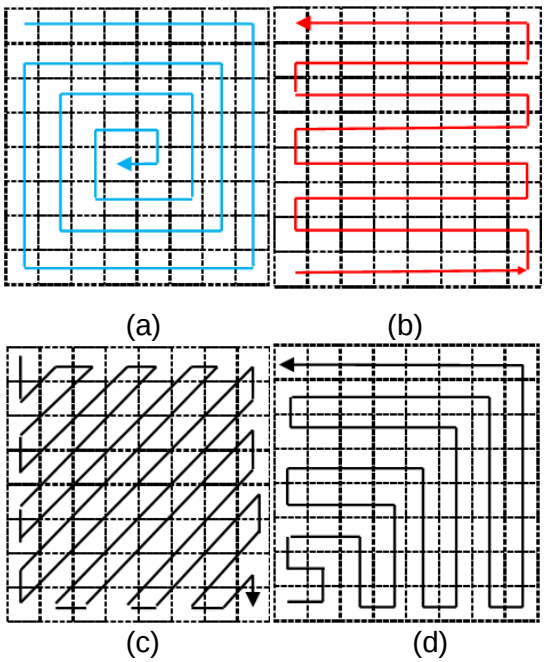

Figure 2 (a) Spiral (b) Raster
(c) Diagonal (d) Orthogonal

We can apply each of these basic pattern individually in single image or alternatively divide the image into different parts and apply these basic pattern in different parts.

A. Partition Pattern

Partition pattern define the order by which each sub-regions of the image are scanned and these partition order are denoted by letter A,B, C and E. Each partition order can also have six different transformations or pattern.

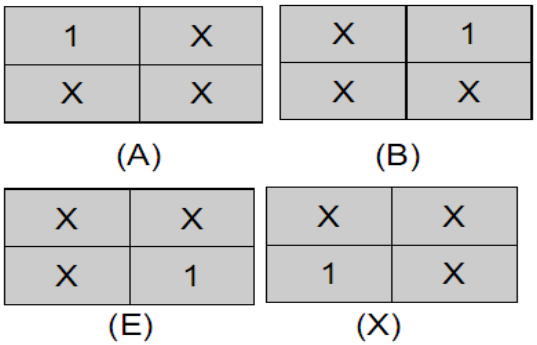

Figure 3 Partition order for different letter

Here letter A represent the partition order which starts from left upper (denoted by 1). And goes to the rest of the three part in 6 different ways or in other words has 6 different transformation.

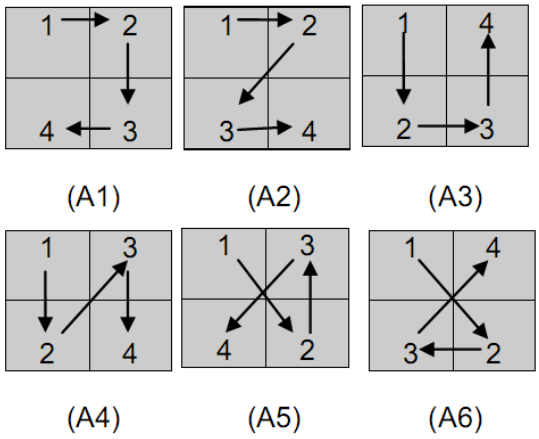

Figure 4 Partition pattern for 'A'

B. Key Generation

In order to generate a key for this encryption and decryption we encode all the scanning pattern and its eight-transformation as C1-C8(for continuous raster), D1-D8(for Diagonal),O1-O8(for orthogonal),S1-S8(for Spiral).

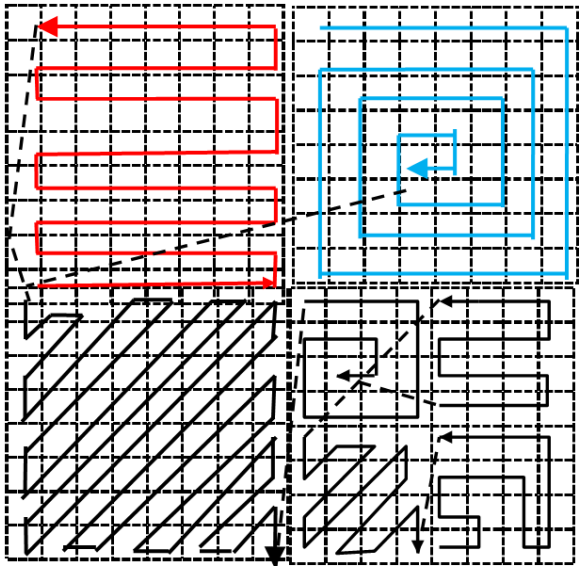

Figure 5 SCAN Pattern Diagram

In a similar way in this method,4- different partition order (A,B,E,X) and its six transformation are being used therefore it can be encoded as A1-A6,B1-B6,E1-E6,X1-X6.

For example the key for following figure is shown below

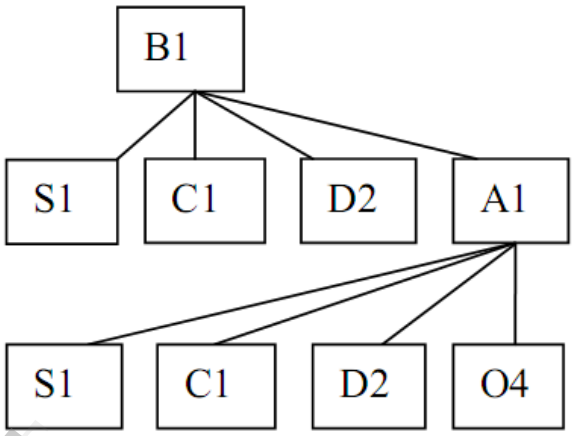

Figure 6 Encryption Key Generation

III. ELGAMEL ENCRYPTION

This method is based on the facts that if p is a large prime number then the primitive root of this number p is a number r which satisfy the following property

$$R \pmod p \neq r^2 \pmod p \neq r^2 \pmod p \neq \ldots \neq r^{p-1} \pmod p \neq 0 \quad \ldots(1)$$

i.e. mod of p taken over the power of number r yield distinct and non-zero number and all are also relative prime to p. For example consider a prime number 7.The primitive root can be any integer number from 1 to 6 which satisfy the equation (1).From the table it is clear that only number 3 and 5 satisfy the equation (1) and hence these number are primitive root of prime number 7.

r1	r2	r3	r4	r5	r6
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	3	1	5
6	1	6	1	6	1

Figure 7

IV. PROCEDURE FOR ELGAMEL METHOD

In this method a user has to choose the private key on the basis of which, a public key is calculated. Let p be a prime number of large value and α be the primitive root of p.Suppose the selected private key is represented by r then the public key β is computed by

$$\beta = \alpha^r \pmod p \quad \ldots.(2)$$

Choose any random integer and compute b by

$$b = \alpha^k \pmod p \quad \ldots..(3)$$

If the plain text is T then compute cipher text by

$$C = \beta^k T \pmod p \quad \ldots..(4)$$

Now, for decryption at the receiver side can be computed by

$$T = C b^{-r} \pmod p \quad \ldots..(5)$$

This is due to the fact that

$$\begin{aligned} C\, b^{-r} &= \beta^k T\, (\alpha^k)^{-r} \\ &= (\alpha^r)^k T\, (\alpha^k)^{-r} \\ &= \alpha^{rk} T\, \alpha^{-rk} \\ &= T \end{aligned} \quad \ldots(6)$$

Algorithm steps for ELGamel method are as follows-

A. *Encrytion Process*

Step 1 First of all choose any large prime number p

Step 2 Compute the primitive root of p and choose any one primitive root α.

Step 3 Select a private key ‘a’ and compute the corresponding public key using equation 2.

Step 4 Take the first pixel of the Red channel and encrypt it using equation 4 for a selected random number ‘k’

Step 5 Repeat step 4 for the pixel of Green channel.

Step 6 Repeat step 4 for the pixel of blue channel.

Step 7 Repeat step 3 to 6 till all the pixel gets encrypted.

Step 8 Merge all encrypted Red, Green and Blue pixel to get the encrypted image.

A. *Decrytion Process*

Step 1 Get the encrypted image and separate the Red, Green and Blue channel.

Step 2 Compute the value of ‘b’ using equation 3.

Step 3Take the first encrypted pixel of Red channel and decrypt it using equation 5.

Step 4 Repeat step 4 for Green and Blue channel.

Step 5 Merge all the decrypted Red, Green and Blue pixel to get back the decrypted image.

V. PROPOSED METHOD

Proposed encryption process consists of two part.The first part encrypt the original image using scanning technique as describe in the part II.Scanning technique works by changing the pixel position only. The value of each pixel remain intact. In the second part the encrypted image obtained by the first part is again encrypted using Elgamel method as described in part IV.

A. Encrytion Process

Encryption process is summarized as-

1. Get the Original Image.
2. Encrypt the Image by applying SCAN method as describe in part II and generate the key1.
3. The encrypted image obtained after step 2 is again encrypted by applying ELgamel method as described in part IV and using key2.

The whole process of encryption is shown in Figure 8

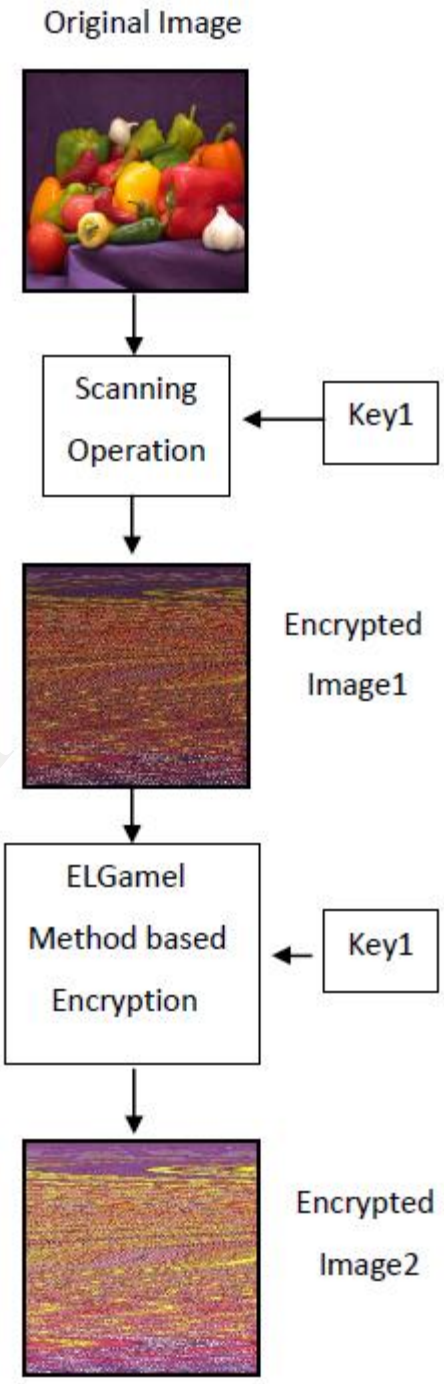

Figure 8 Encryption Process

B. Decrytion Process

Since in this method two key are used one for scanning based method of image encryption and

another is for ELGamel method ,therefore the security of this method gets enhanced manifold.In order to decrypt the image, person must know both the keys which is difficult in this algorithm.

The decrytion process is summarized as -

1. Get the Encrypted image
2. Perform the Elgamel decryption operation using key2.
3. Perform the SCAN based decryption operation using key1 to get back the original image.

The decryption process is shown in figure 9

VI. EXPERIMENTAL RESULT

Proposed method is implemented in the computer having dual core processor and 2GB RAM.In order to evaluate the performance of proposed method, Mean square error has been computed for testing the distortion between original image and decrypted image. Execution time for this algorithm is also computed and tabulated in Table 1From the Table 1 and figure 10 it is clear that the proposed method is fast and produce no distortion in decrypted image and at the same it also give enhanced security because of using two different keys for decryption.

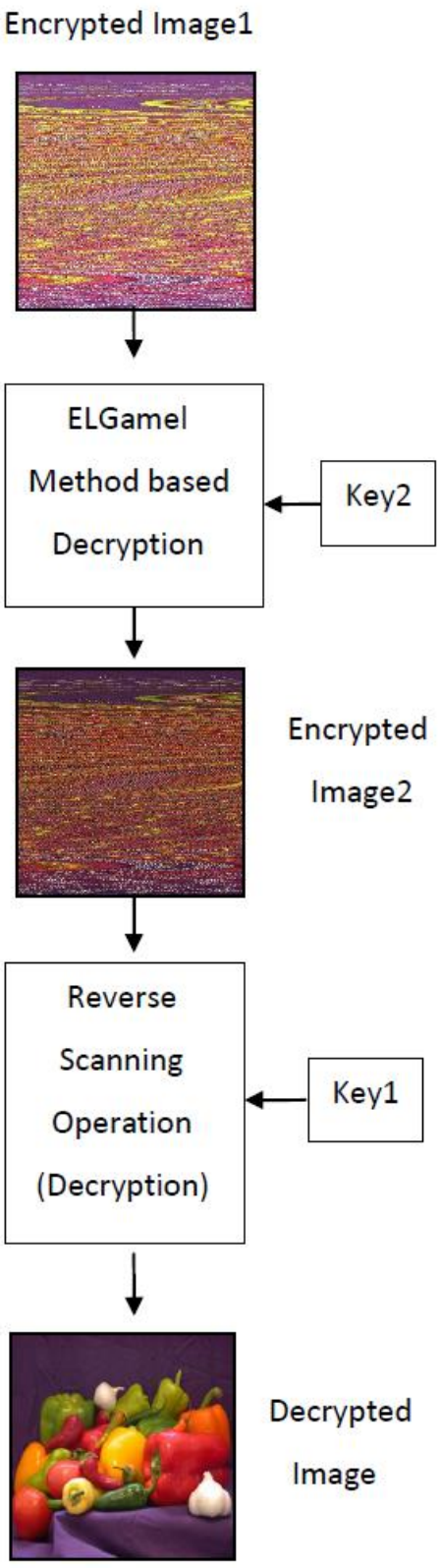

Figure 9 Decryption Process

TABLE 1:Execution time,MSE Between Original and Decrypted Image

Image	Image size	MSE between Original and Decrypted Image (For Lenna Image)	Execution Time (in second)
Peppers.png	256x256	0.00	0.30
Peppers.png	512x512	0.00	0.35
Football.jpg	256x256	0.00	0.29
Football.jpg	512x512	0.00	0.33
Kids.jpg	256x256	0.00	0.30
Kids.jpg	512x512	0.00	0.34

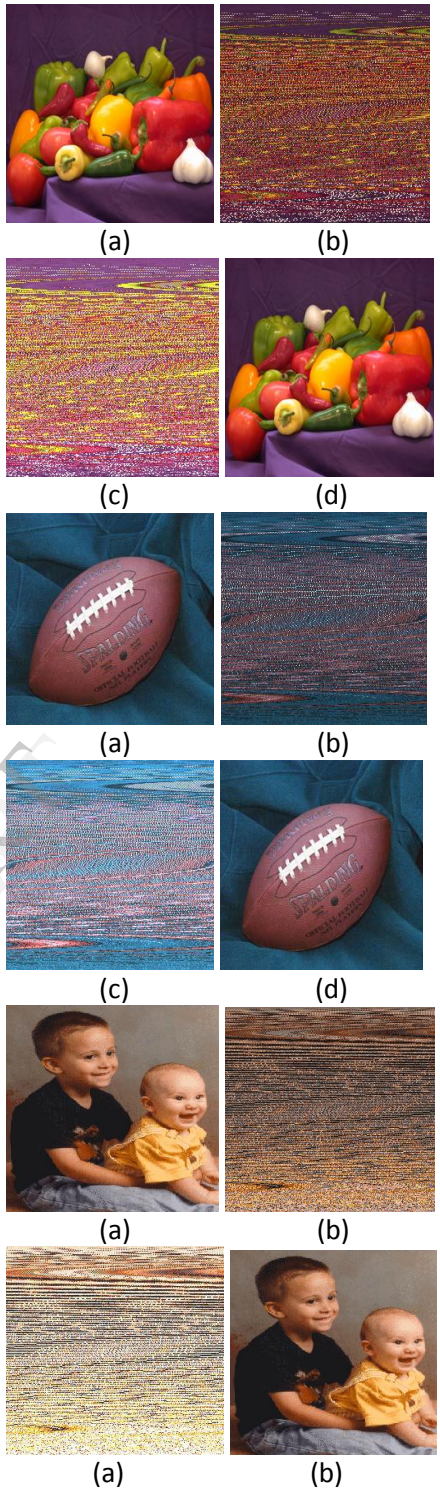

Figure 10 (a) original image (b)Image encrypted using SCAN method (c)Image Encrypted using ELGmel method (d) Dcrypted Image

References

[1] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows," Electronic Imaging, vol. 17, no.2, pp. 318-325, 1998.
[2] N. Bourbakis, C. Alexopoulos, "Picture data encryption using SCAN patterns," Pattern Recognition, vol. 25, no. 6, pp. 567-581, 1992.
[3] C. Alexopoulos, N. Bourbakis, and N. Ioannou, "Image encryption method using a class of fractals," Electronic Imaging, no. 4, pp. 251-259, 1995.
[4] N. Bourbakis, "Image data compression encryption using G-SCAN pattern," in proceedings of IEEE Conference on SMC, pp. 1117-1120, Orlando, Florida, USA, October 1997.
[5] S. S. Maniccam, N. G. Bourbakis, "Image and video encryption using SCAN patterns," Pattern Recognition, no. 37, pp. 725-737, 2004.
[6] X. Li, "Image compression and encryption using tree structure," Pattern Recognition, no. 18 no. 11, pp. 1253-1259, 1997.
[7] T. Chuang, J. Lin, "New approach to image encryption,"Electronic Imaging, no. 4, pp. 350-356, 1998.
[8] T. Chuang, J. Lin, "A new multiresolutional approach to still image encryption, "Pattern Recognition Image Anal", vol. 9, no. 3, pp. 431-436, 1999.
[9] X. Wu, P. moo, "Joint image/video compression and encryption via high order conditional entropy coding of wavelet coefficients", in Proceedings of IEEE InternationalConference.

[10] William Stallings, "Cryptography and Network Security", Pearson Education, 5th edition, 2011.
[11] Trappe, Washington, "Introduction to Cryptography with coding Theory", Pearson Education, 2nd edition, 2011.