Encryption And Decryption Techniques: A Review

Swati Kumari,

M.Tech. Student, Department of Electrical And Electronics, NITTTR Bhopal, M.P., India

---***---

Abstract - *Image encryption is the process of hiding the important data from the unauthorized users. In present time, the security of multimedia has become necessary. One of the methods to protect data is encryption. In this paper, different techniques for the encryption and decryption of digital colored image has been reviewed.*

Key words: Encryption and decryption, cryptography, symmetric key, asymmetric key.

1. INTRODUCTION

The use of internet has grown rapidly for transmission of valuable information. The information may be in the form of multimedia (text, image, video). In our daily life, we share our valuable images with friends and family. With the rapid growth in the technology, security is primary need for multimedia data transmission. The multimedia data is required to be protected from unauthorized users .To protect data from unauthorized users data protection techniques are required. Encryption of data is one of the important techniques used for data protection.
This paper has been organized as follows-
In section 1, some general guidelines about cryptography has been provided. In section 2, survey on already existing research papers has been done. Finally, in section 3, survey has been concluded.
There are two main types of cryptography:

(i) Symmetric key Cryptography (Secret Key)
(ii) Asymmetric key Cryptography (Public Key)

In symmetric key cryptography, both sender and receiver use the same key to encrypt and decrypt the data respectively.
In asymmetric key cryptography, sender and receiver use different key to encrypt and decrypt the data.
This encryption and decryption technique is used when secret messages are transmitted from one end to another end. Usually, very sensitive information has been stored in computer and transmitted over the internet. Thus, to ensure the security of data has become key issue. There are number of algorithms available to encrypt and decrypt image which is described in next section.

2. LITERATURE SURVEY

2.1 Partial Encryption of Images Using RSA, 2005

M. B. I. Reaz, F. Mohd-Yasin, S. L. Tan, H. Y. Tan [1] have proposed partial encryption of compressed images. They have used a secure encryption algorithm to encrypt only the crucial parts, which are considerably smaller than the original image. This will result in significant reduction in processing time and computational requirement for encryption and decryption. Rivert-Shamir-Adleman (RSA) algorithm has been used for the encryption. Equation (1) and (2) has been used to encrypt and decrypt images respectively.
To encrypt plaintext M,

$$C = M^e mod\ n \qquad (1)$$

To decrypt C,

$$M = C^d mod\ n \qquad (2)$$

Here,
M- 32-bits block which is to be encrypted.
C- 32-bits encrypted block.
(e,n)- 32-bits public key which has been used for encryption.
(d,n)- 32-bits private key which has been used for decryption.
e, n and d- Modular exponentiation.
RSA encryption algorithm gives PSNR=27.17 and MSE=3.45, when this algorithm is applied on image dimension of 256*256.

2.2 A highly Adaptive Novel Symmetric Encryption Using The Sylvester Equation, 2005

Min-sung Koh and Esteban Rodriguez-Marek [2] have proposed a symmetric encryption technique based on the Sylvester equation. In this, data has been encrypted by Hankel matrix that is made up of a symmetric key sequence and the decrypted information is obtained by solving the Sylvester equation. There are three theorems that show that the Sylvester equation is a valid method for encryption. It generates the huge amount of possible keys that makes the algorithm an exhaustive search for the best approach towards breaking the algorithm. Figure 1 shows the block diagram of encryptor and decryptor. Here, an image matrix

P has been given to serial to parallel converter V/M. Then, this converted image has been given to m*m Hankel matrix F and A which gives FP and PA respectively. Now, after FP has been xor with PA which gives Sylvester equation –C. At receiver side, this Sylvester equation has been solved using keys and parallel to serial converter M/V has been used after this to get back the original image.

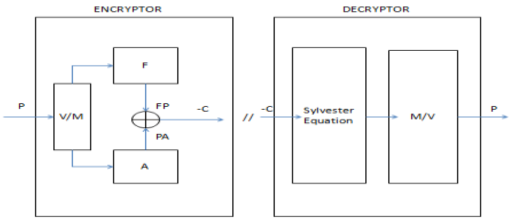


Fig 1: encryption and decryption technique using Sylvester equation and Hankel matrix

Here,
P- m*m Image matrix which is to be encrypted.
V/M- Serial to Parallel converter.
M/V- Parallel to Serial converter
F and A- m*m Hankel matrix to generate Key.
C- m*m Encrypted Image matrix. Sylvester equation is,

$$FP + PA = -C \qquad (3)$$

Equation (3) shows the Sylvester equation which is used for the decryption of the encrypted image matrix.
The Sylvester equation algorithm provides PSNR=30.56 and MSE=3.02, when this algorithm is applied on image dimension of 256*256.

2.3 Image Encryption Using Binary Key images, 2009

Yicong Zhou, Karen Panetta and Sos Agaian [3] have proposed a new concept for image encryption using a binary "key-image". In this, the key-image is of the same size as the original image which is to be encrypted. The performance of algorithm is shown against common attacks such as the brute force attack, ciphertext attacks and plaintext attacks. The proposed algorithms can encrypt all types of image. This algorithm has the potential to be used to secure communications. Figure 2 shows the procedure for encryption of 2D or 3D image using binary key images. Here, original image has been decomposed into binary bit planes and another image of same size has been taken as key image. Now, XOR operation has been operated between both images to get 1st level encrypted image. After this, order of bit planes has been inverted. Now, all bit planes has been combined to get final encrypted image.
To decrypt the encrypted image using its security keys the encrypted image is decomposed into bit planes. Now each bit plane and the key-image is applied to XOR operation. Then the order of bit planes is reverted. Now all bit planes has been combined to get original image.

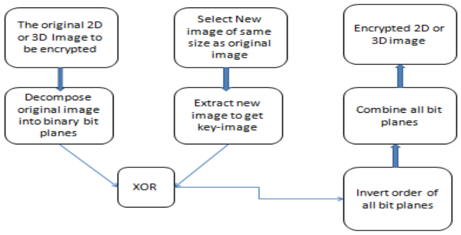

The original 2D or 3D Image to be encrypted
Select New image of same size as original image
Encrypted 2D or 3D image
Decompose original image into binary bit planes
Extract new image to get key-image
Combine all bit planes
XOR
Invert order of all bit planes

Fig 2: encryption of 2D or 3D image using binary key image algorithm

The binary key image algorithm provides PSNR=57.91 and MSE=1.25, when this algorithm is applied on image dimension of 256*256.

2.4 A Novel Symmetric Image Encryption Approach Based on an Invertible Two-dimensional Map, 2009

Yong Feng, Xinghuo Yu [4] has proposed a new invertible Line map, for image encryption and decryption. It converts image into an array of pixels and then converts it back from the array to a same sized image. This paper presents a novel image encryption approach based on the Line maps, which can perform two processes permutation and substitution simultaneously, using the left and right map of line map. The proposed algorithm does not have information loss. It is fast and there is no restriction on the length of security key that is desirable for different security requirements. Figure 3 shows the principle of line map which has been used to encrypt image. The left Line map projects an $N \times M$ image, A, to an array of $N \times M$ pixels, I, from the upper left corner to the lower right corner along the diagonal. Then the array of N.M pixels is further mapped to a same sized image B.

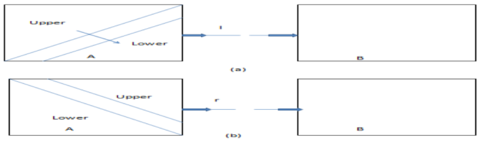
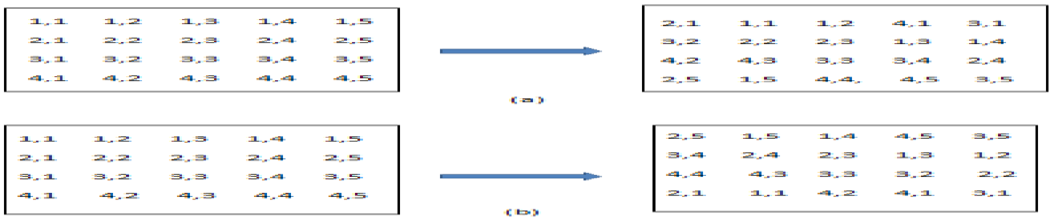


Fig 3: the principle of line map. (a) the left line map; (b) the right line map.



1,1	1,2	1,3	1,4	1,5
2,1	2,2	2,3	2,4	2,5
3,1	3,2	3,3	3,4	3,5
4,1	4,2	4,3	4,4	4,5

2,1	1,1	1,2	4,1	3,1
3,2	2,2	2,3	1,3	1,4
4,2	4,3	3,3	3,4	2,4
2,5	1,5	4,4,	4,5	3,5

1,1	1,2	1,3	1,4	1,5
2,1	2,2	2,3	2,4	2,5
3,1	3,2	3,3	3,4	3,5
4,1	4,2	4,3	4,4	4,5

2,5	1,5	1,4	4,5	3,5
3,4	2,4	2,3	1,3	1,2
4,4	4,3	3,3	3,2	2,2
2,1	1,1	4,2	4,1	3,1

Fig 4: encryption using the line mapping algorithm with 4*5 image (a) the left line map; (b) the right line map.

Figure 4 shows the encryption technique using line map algorithm which is combination of left line map 4(a) and right line map 4(b). In the left line map as shown in Fig 4(a), each pixel from a super diagonal has been inserted between adjacent two pixel of the lower level neighboring super diagonal. Similarly, in the right line map as shown in Fig 4(b), each pixel from sper skew diagonal is inserted between the adjacent two pixels of the lower level super skew diagonal along the direction from the upper right corner to the lower left corner. The invertible two dimensional map algorithm provides PSNR=46.94 and MSE=2.28, when this algorithm is applied on image dimension of 256*256.

2.5 Logical Transform based Encryption for Multimedia Systems, 2010

Sos.S.Agaian, Raja.G.R.Rudraraju and Ravindranath.C.Cherukuri [6] have proposed an encryption technique based on Logical Transforms. In this technique, a secret key which is based on the logical transforms that satisfies proposed boolean matrix, is used to encrypt the images. This is novel encryption technique for the images of arbitrary size and format. This method can also be implemented on hardware. Figure 5 shows image encryption using logical transform. Firstly, the size of the input image is obtained, if the image is a square matrix with the order of 2^n , various keys required are generated from their basic matrix form to the size of the image 2^n .If there is a limitation for the size of the key matrices, the image is made into blocks P_1, P_2, P_3....... P_k, where all the 'k' blocks of the image 'P' are square matrices of size 'n'. The keys to be generated should be the size of the image block 'P'.

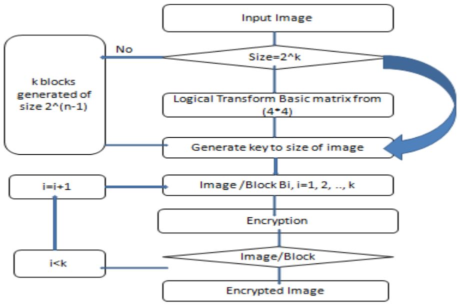

Input Image
Size=2^k
No
Yes
k blocks generated of size 2^(n-1)
Logical Transform Basic matrix from (4*4)
Generate key to size of image
i=i+1
Image /Block Bi, i=1, 2, .., k
Encryption
i<k
Image/Block
Encrypted Image

Fig 5: image encryption using logical transform

(i) Each data block P_i is encrypted as follows:

$$C_1 = [S.(P_1 \oplus V).S]K \oplus V \qquad (4)$$

Here,
C_1 is ciphered image w.r.t. block P_1,
S is key matrix
K is number of blocks
V is initial image matrix

(ii) Each encrypted block C_k is decrypted into original image blocks using received keys as follows: $P_1 = S^{-1}.[(C_1 \oplus V).K].S^{-1} \oplus V$

$$= S^1.[(C_1 \oplus V).K].S^1 \oplus V \qquad (5)$$

Here,
S^{-1} is inverse of key matrix.

Equation (4) shows encryption of each data block P_i and equation (5) shows decryption of each encrypted block C_k.

Image encryption using logical transform provides PSNR=67.24 and MSE=.472, when this algorithm is applied on image dimension of 256*256.

2.6 Discrete Chaotic Exclusive OR Encryption of Digital Image, 2010

Zhang Dinghui, Zhang Jianwei, Wang Yuping, Xu Saisai and Li You [7] have proposed an encryption technique which produces binary chaotic sequence and then a binary exclusive OR operation has been done between the binary chaotic sequence and the digital image to encrypt the digital image. This algorithm has both a good encrypting effect and stronger security, and it is a symmetric and lossless encryption system.

Equation (6) and (7) shows the binary chaotic sequence.

$$x_{n+1} = \mu x_n(1 - x_n) \qquad (6)$$

Here, $0 < \mu \leq 4$

$x_n \in (0,1), n = 0, 1, 2, \ldots.$

$$y_n = \begin{cases} 1, & 0.5 < x_n < 1 \\ 0, & 0 < x \leq 0.5 \end{cases} \qquad (7)$$

Here,

y_n is binary chaotic sequence.

X_n is state variable.

μ is logistic map parameter.

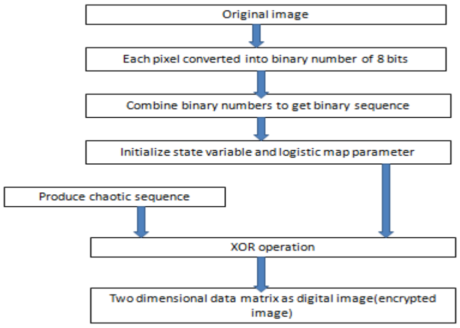

Original image
Each pixel converted into binary number of 8 bits
Combine binary numbers to get binary sequence
Initialize state variable and logistic map parameter
Produce chaotic sequence
XOR operation
Two dimensional data matrix as digital image(encrypted image)

Fig 6: encryption using two dimensional chaotic sequence algorithm

Figure 6 shows encryption technique using two dimensional chaotic sequence algorithm. Here, each pixel of original image is converted into binary number of 8 bits. Then, all binary numbers are combined to get binary sequence. Now, XOR operation has been done between chaotic sequence of image and binary sequence of image to get encrypted image. Image encryption using chaotic sequence algorithm provides PSNR=65.58 and MSE=.678, when this algorithm is applied on image dimension of 256*256.

2.7 A Novel Image Encryption Method based on Invertible 3D Maps and its Security Analysis, 2011

Yong Feng, Juan Li, Fengling Han and Tohari Ahmad [8] have proposed a novel invertible 3D maps based image encryption method. In this paper, invertible 3D maps are utilized for image encryption. Now to provide extra security, 2D positions of image pixels are permuted and 1D grey level value of the pixels are also substituted, using the invertible 3D maps. Figure 7 shows the principle of line map which has been used to encrypt image. The left Line map projects an $N \times M$ image, A, to an array of $N \times M$ pixels, l, from the upper left corner to the lower right corner along the diagonal. Then the array of N.M pixels is further mapped to a same sized image B.

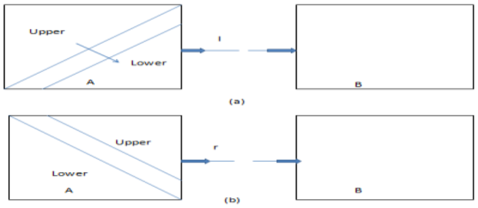


Fig 7: principle of invertible 3D line map (a) left line map; (b) right line map.

Figure 8 shows the encryption technique using line map algorithm which is combination of left line map 8(a) and right line map 8(b). In the left line map as shown in Fig 8(a), each pixel from a super diagonal has been inserted between adjacent two pixels of the lower level neighboring super diagonal. Similarly, in the right line map as shown in Fig 8(b), each pixel from super skew diagonal is inserted between the adjacent two pixels of the lower level super skew diagonal along the direction from the upper right corner to the lower left corner.

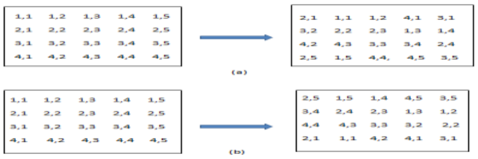


Fig 8: image encryption using invertible 3D map algorithm

Image decryption is the inverse process of image encryption. It means converting encrypted image to original image. Image encryption using invertible 3D map algorithm provides PSNR=50.04 and MSE=1.89 when this algorithm is applied on image dimension of 256*256.

2.8 A New Image Stream Encryption Technique, 2014

Firas Hassan, Michael Limbird, Vishwanath Ullagaddi and Vijay Devabhaktuni [9] have proposed a technique which uses the parity bit plane of a public image to encrypt the image. The information leakage in the proposed encryption process is negligible. The proposed algorithm can be used in real time multimedia and wireless applications.

(i) To encrypt image, Figure 9 shows the image encryption technique using image steam technique. Here, shift register (SR) is initialized first. Then the Automatic Key Generator (AKG) produces a single key bit from the different output bits of the SR that are accessed simultaneously. The input message bit and the key bit are fetched into XOR gate to obtain the encrypted image bit. Then this output is used to update the content of the shift register. This process is repeated until all the message bits have been streamed into the SR.

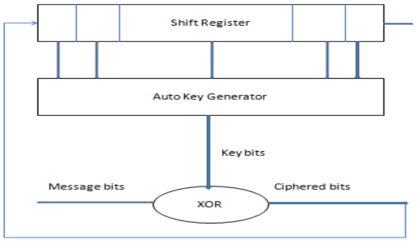


Fig 9: to encrypt image using image stream algorithm

(ii) To decrypt image, Figure 10 shows decryption technique using image stream algorithm. The shift register is initialized. Then the cipher bit is given to shift register and XOR gate. Now the AKG produces a single key bit. Now the message bit is obtained by doing XOR operation on key bits and cipher bits. This process is repeated until all the ciphered bits have been streamed.

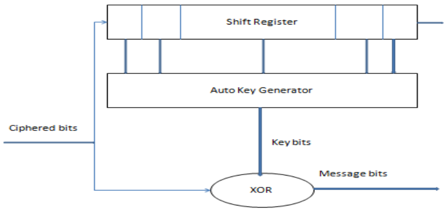


Fig 10: to decrypt image using image stream algorithm

Image encryption using image stream algorithm provides PSNR=68.06 and MSE= .426, when this algorithm is applied on image dimension of 256*256.

2.9 A New Quaternion-Based Encryption, 2015

Mariusz Dzwonkowski, Michal Papaj and Roman Rykaczewski [10] have proposed a new quaternion-based encryption technique for digital image to get negligible loss. This algorithm is slightly modified to point out the best location for the proposed encryption scheme, which significantly improves speed of images encryption. The proposed algorithm decomposes image into two 8-bit images in order to perform encryption. This algorithm uses special properties of quaternion to perform shuffle the data sequences in 3D space for each of the cipher rounds.

Quaternion formula

$$q = w + xi + yj + zk \quad (8)$$

Quaternion rotation

$$P_{rot} = q.P.q^{-1} \quad (9)$$

Equation (8) and (9) show the quaternion formula and quaternion rotation to encrypt digital image.
Here,
w, x, y, z are real coefficients of quaternion q.

i, j, k are imaginary units with following properties:
$i^2 = j^2 = k^2 = ijk = -ji = k,$
$jk = -kj = i$
$ki = -ik = j$
Image encryption using Quaternion based algorithm provides PSNR=70.29 and MSE=.221, when this algorithm is applied on image dimension of 256*256.

3. CONCLUSION

Transmitting digital data oven open network have become very frequent. Thus, securing of digital data has become very important requirement. In this paper, we studied and reviewed about the work on image encryption which has been done earlier.

Table 1: PSNR value of different encryption technique

Technique Name	PSNR	MSE
RSA Algorithm	27.17	3.45
The Sylvester Equation Algorithm	30.56	3.02
Binary key Algorithm	57.91	1.25
2D Line Map Algorithm	46.9425	2.28
Logical Transform Algorithm	67.24	.472
Chaotic Sequence Algorithm	65.58	.678
3D line Map Algorithm	50.0454	1.89
Image Stream Algorithm	68.06	.426
Quaternion Based Algorithm	70.29	.221

Table 1 shows the PSNR value of different encryption algorithm.

$$PSNR= \log (2^{n} -1)/ MSE \qquad (10)$$

Here,
n is number of pixels of image.
PSNR is Peak Signal to Noise Ratio of image.
MSE is Mean Square Error of image.

Equation (10) shows the formula for peak signal to noise ratio. Thus, after reviewing these papers it can be concluded that with improvement in encryption technique the PSNR value of image is improving and MSE value is decreasing.

4. REFERENCES

[1] M.B.I. Reaz, F. Mohd-Yasin, S. L. Tan, H. Y. Tan and M. I. Ibrahimy, "Partial Encryption of Compressed Images Employing FPGA", IEEE 2005, page no. 2385-2388.

[2] Min-sung Koh and Esteban Rodriguez-Marek, "A highly Novel Symmetric Encryption Method Using Sylvester Equation", IEEE 2005, page no. 1-7.

[3] Yicong Zhou, Karen Panetta and Sos Agaian, "Image Encryption Using Binary Key-images", 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009, page no. 4569-4574.

[4] Yong Feng, Xinghuo Yu, "A Novel Symmetric Image Encryption Approach based on an Invertible Two-dimensional Map", IEEE 2009, page no. 1973-1978.

[5] Sos.S.Agaian, Raja.G .R.Rudraraju, Ravindranath.C.Cherukuri, "Logical Transform based Encryption for Multimedia Systems", IEEE 2010, page no. 1953-1957.

[6] Zhang Dinghui, Zhang Jianwei, Wang Yuping, Xu Saisai, Li You, "Discrete Chaotic Exclusive OR Encryption of Digital Image", 2010 International Conference on Web Information Systems and Mining, page no. 71-73.

[7] Yong Feng, *Member,* Juan Li, Fengling Han, and Tohari Ahmad, "A novel Image Encryption Method based on Invertible 3D Maps and its Security Analysis", IEEE 2011, page no. 2186-2191.

[8] Firas Hassan, Michael Limbird, Vishwanath Ullagaddi, Vijay Devabhaktuni, "A New Image Stream Encryption Technique", IEEE 2014.

[9] Mariusz Dzwonkowski, Michal Papaj, and Roman Rykaczewski, "A New Quaternion-Based Encryption Method for DICOM Images", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 11, NOVEMBER 2015, page no. 4614-4622.

BIOGRAPHY

Swati Kumari, M.Tech Student, NITTTR, Bhopal, M.P., India.