ISSN:0975-9646

Aman Jain et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2886-2889

Image Based Encryption Techniques: A Review

Aman Jain[1], Namita Tiwari[2], Madhu Shandilya[3]

[1]*Department of Computer Science and Engineering and* [3]*ECE,*
Maulana Azad National Institute of Technology
Bhopal, Madhya Pradesh, India

[2] *Department of Computer Science and Engineering,*
Maulana Azad National Institute of Technology
Bhopal, Madhya Pradesh, India

***Abstract*— Now a day's rapid increasing growth of internet and multimedia data, security is main problem in storage and communication of images. The solution of this multimedia data can be solved by using encryption. There are various techniques available to protect the image data from unauthorized access. In this paper, authors reviewed different existing techniques of image encryption and also discussed the basic knowledge of Cryptography.**

***Keywords*— Chaotic Map, Cryptography, Decryption, Encryption, SCAN pattern, Security.**

I. INTRODUCTION

Confidential communication has long been a common practice in the social life. However, as information can be communicated electronically, it is exposed in public domain and unavoidably resulted in interceptions. A scientific approach to respond to the demands of achieving the sense of security is termed as cryptography. The term cryptosystem, also called cipher, is often used in cryptography. The main theme of encryption is to change the message in which its original message can only be identified by an authorized recipient. So we can say that a message in its original form is known as plaintext P and the information concealed in an incoherent form is known as cipher text C. The encryption process consists of an algorithm and a key. A key may be private key or public key. So it is generally defined as:

$$C = E(P, K_e) \quad (1)$$

Here K_e is the encryption key of an image.

So, the cipher text C can be transmitted over public channels without leaking the information it represents. In the same way, decryption process is the reverse of encryption process that is based on the cipher text C and decryption key for the reform of the original plaintext.

$$P = D(C, K_d) \quad (2)$$

Here K_d is decryption key of an image.

D ( ) = E^{-1}( ) and the principle of encryption process is shown in Fig. 1.

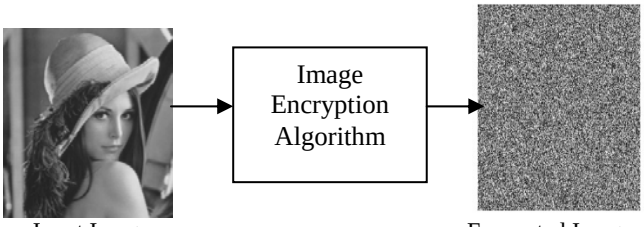

Fig. 1. Image Encryption Process

Cryptanalysis is used for the study of methods in obtaining the meaning of encrypted information without access to the key so we can say that it is the study of how to know encryption algorithms or their implementations. Cryptography systems may be divided into two parts first is Secret key cryptography also known as symmetric key cryptography which uses a secret key for encryption and decryption. Second is Public key cryptography also known asymmetric key cryptography which uses two keys for encryption and decryption.

Image encryption algorithm is different from the Data encryption algorithm because of the large size of digital images and data redundancy. Image encryption technique converts an image to another image that is not easy to understand.

In this paper we presented literature survey on existing research techniques. In the next section, security analysis and parameter of the existing image encryption techniques will be discussed like statistical analysis, Key sensitivity analysis etc. These parameters are essential to prove the security against the most common attacks. Finally, in the last section we describe the conclusion of this paper.

II. LITERATURE SURVEY

An easy way to comply in 2006, Pareek et al. [1] introduced an image encryption method using chaotic logistic map. In this paper, Image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for both the logistic maps are derived using the external secret key by providing different weightage to all its bits. Further, in the encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map.

In 2006, Chao-Shen Chen [2] described the image encryption by rearrangement of the pixels of the image. Rearrangement was performed by SCAN patterns that generated by the SCAN methodology. There are various types of SCAN pattern that are used for the rearrangement of the pixels of an image like Raster C, Diagonal D, Orthogonal O, Spiral S. SCAN is a two dimensional spatial accessing methodology which can efficiently generate a wide range of scanning paths. So a scanning of a two dimensional array that is define as.

$$P_{m*n} = \{P(i, j) : 1 \le i \le m, 1 \le j \le n\} \quad (3)$$

Where P (i, j) is a bijective function and P_{m*n} is the set of {1, 2…....mn-1, mn}.

So the scanning path is techniques that traverse the each pixel of the image exactly once. The main advantage of this existing SCAN methodology image encryption and decryption is security that can be increased using several encryption loops.

In 2008, TiegangGao, Zengqiang Chen [3] presented an image encryption technique based on hyper chaos. This technique performs into two parts. In the first part, total shuffling of the pixels of the image is done by using the rows transformation that is based on logistic map. Then column transformation takes place that is also dependent on the logistic map. After shuffling the image, in the second part apply the hyper chaos to encrypt the shuffled image. Use of hyper chaos changes the gray level of the pixels of the shuffled image. This method has the advantage of large key space but reusing the key again and again makes it weak against chosen cipher text, chosen plaintext attacks.

In 2009, Vinod Patidar et al. [4] defined the image encryption scheme using two chaotic logistic maps and an external key of 80-bit. The initial conditions for both logistic maps were derived from the external secret key. The first logistic map was used to generate numbers in the range between 1 and 24 and the initial condition of the second logistic map was modified by the numbers generated by the first logistic map. The authors showed that by modifying the initial condition of the second logistic map in this way, its dynamics became more random.

In 2009, Bibhudendra Acharya et al. [5] proposed an advanced Hill (AdvHill) cipher algorithm which is based on involuntary key matrix for encryption. In this method they used different types of images and encrypted those using original Hill Cipher algorithm and it is clearly defined that original Hill Cipher can't encrypt the images in efficient way if the image consists of large area covered with same color or gray level. But their existing algorithm works for any images with different gray scale as well as color images.

De Wang, Yuan-Biao Zhang [6] proposed an image encryption technique based on S-box Substitution and Chaos theory. The purpose of this technique is to enhance the security. This method consists of two steps, in the first step S-boxes are used for the substitution of each byte and this S-box included multiple rounds of S-boxes substitution. After that we apply the algorithm that is based on chaos theory, random sequence. So we can say that the new improved image encryption algorithms could efficiently increase the efficiency and the anti-errors-proliferation character of image encryption algorithm and be easily implemented.

In 2010, Mao-Yu Huang, Yueh-Min Huang [7] proposed a new image encryption algorithm, which is based on Arnold cat map and logistic chaotic system to improve the security of the image transmission. Firstly, by using Arnold cat map they shuffled the original image. After that applies the logistic chaotic map to encrypt the shuffled pixels value of the image.

Arnold cat map can shuffle the image, but after applying several iterations, it returns to the original image and only using the Arnold cat map cannot provide the security level. So they applied the logistic map algorithm to increase the security of this technique.

Sesha Pallavi Indrakanti and P.S.Avadhani [8] proposed a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involved three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provides confidentiality to color image with less computations permutation process is much quick and effective. The key generation process is unique and a different process.

Amitava Nag, Jyoti Prakash Singh, Sraban Khan, Saswati Ghosh [9] presented that image encryption was an important method to secure image data. We know that the neighboring pixel of original images is highly correlated to their neighbor pixels. Due to this strong correlation any pixel can be naturally predicted from the values of its neighbor's pixels. So in this paper, proposed a symmetric key image encryption technique that is based on location transformation. We scramble the pixel values to different location using affine transform technique with four 8-bit keys. The transformed image then breaks into 2 x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size used in this algorithm is 64 bit. The experimental results proved that after apply the affine transform the correlation between pixel values was significantly reduced.

G.Nagaraju and T. V. Hyma Lakshmi [10] proposed an idea for image encryption using secret-key images and SCAN patterns. The key image is created by the secret alphanumeric keyword and each alphanumeric key has a different 8 bit ASCII code. After creating a key image, it is added with the original and then applies the SCAN pattern which is generated by the SCAN methodology at the original image or key image. This technique provides the better security because encryption is performed by two methods.

In 2013, Xuan Li [11] proposed a novel image encryption scheme based on even-symmetric chaotic maps and skew

tent chaotic map. First, permutation phase, the iteration time of even-symmetric chaotic map to avoid transient effect is not fixed but relevant to the plaintext so the P-box shuffles the position of all the pixels of the image. Then in the diffusion phase, both even-symmetric chaotic maps and skew tent map are used to generate the key stream. The performance and security of this proposed technique are checked thoroughly using key space analysis, statistical analysis and sensitivity analysis and so on. So we can say that the scheme is reliable to be adopted for the secure image communication application.

Sunil Kumar et al. [12] described the image encryption using 4 out of 8 codes and apply chaotic map. Firstly, original image is applied to permutation block. Original image is permuted using chaotic map to produce permuted image. After generating a carrier image the permuted image and Carrier image generated from 4 out of 8 codes perform Ex-or operation to produce the encrypted image. Image encryption using 4 out of 8 code and chaotic map is simple and effective.

Narendra K. Pareek et al. [13] proposed an efficient and secure algorithm for gray level image encryption that is based on a new approach of substitution and diffusion. The algorithm is based on sixteen rounds of iterations. The diffusion process follows the zigzag path to rearrange the pixels of the image. The substitution process in which, the pixels of the image changed with one of their adjacent pixels. The chosen adjacent pixel to the current pixel is one of the pixels located at the eight possible adjacent locations and is XORed with the current pixel. The chosen of pixel depends on the key used in the algorithm. So this proposed method is simple, easy to implement on both hardware and software, efficient and has high level of security. The scheme can be used in real practice.

III. Security Analysis Parameter

A good encryption method should stable via all kinds of cryptanalytic such as statistical and brute force attacks [14]. In this section we define the proposed method with statistical analysis, key sensitivity analysis and information entropy analysis to prove the existing method is secure against the most common attacks. First we define the histogram and the correlation of the two adjacent pixels in the image to prove the stability against statistical attacks. Second we define the key sensitivity analysis in the image to make brute force attacks infeasible. Third we define the information entropy analysis in the image to protect the information in the encryption process. Then there is no unauthorized access of information in the encryption process.

A. Histogram and Correlation Analysis

The image histogram show the distribution of pixels is an image by plotting the number of pixels at each gray scale level. From Fig. 3 and Fig. 5 we can say that histograms of the plain image and encrypted image are different to each other. The histogram of encrypted image is uniform. Thus, this histogram analysis is robust against statistical attacks.

Fig. 2.Plane Image

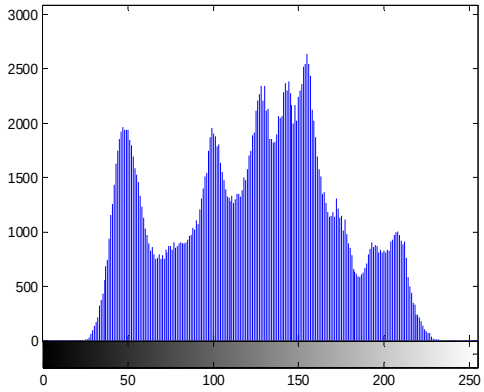

Fig. 3.Histogram of Plain Image

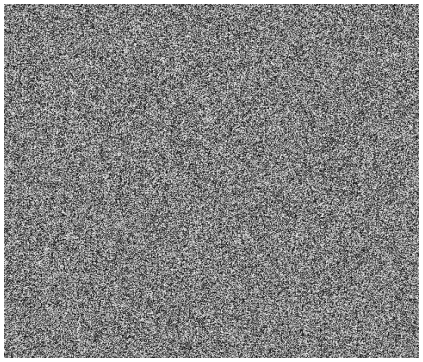

Fig. 4.Encrypted Image

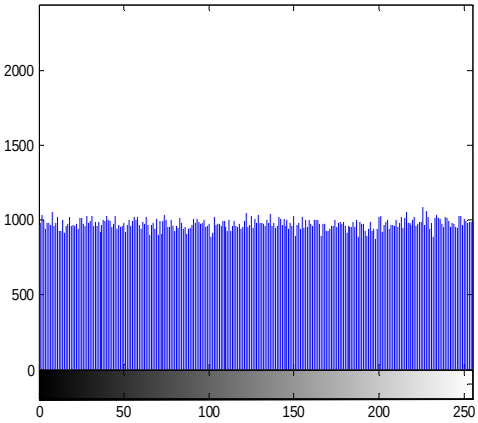

Fig. 5.Histogram of Encrypted Image

Correlation [14] is defined as the relation of adjacent pixels in an image. Each pixel is highly correlated with its adjacent pixels either in horizontally, vertically or diagonally. In a plain image correlation value is very close to 1, while in encrypted image its value should be as low as possible. For calculation of correlation, we have to take random number of pairs of pixels that is defines as.

$$r = \frac{m\sum(ab) - \sum a \sum b}{\sqrt{[m\sum(a^2) - (\sum(a)^2][m\sum(b^2) - (\sum(b)^2]}} \quad (4)$$

Where m is the number of pixels in an image, a and b are the values of adjacent pixels vertically, horizontally and diagonally.

B. Key Sensitivity analysis

A key sensitivity [15] define as a little change in the plain image, a different encrypted image is obtained. NPCR is the pixel rate change at the encrypted image for changing a pixel at the plain image and UACI is the mean of these changes for secure image cryptosystems high key sensitivity is required which means that the encrypted image cannot be decrypted correctly although there is only a slightly difference between encryption or decryption keys. This guaranty that the security of the proposed technique against brute-force attacks to some extent. NPCR and UACI are defining as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \quad (6)$$

Where NPCR is Number Pixel Change Rate and UACI is Unified Average Changing Intensity. H and W are the height and width of the image.

C1 and C2 are two encrypted images obtained from two plain images with just one different pixel and D is:

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) = C_2(i,j) \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

C. Information Entropy analysis

Information entropy [15] is a common way to shows the randomness of the data, i.e. more entropy means data will be more disordered and hence, prediction of information becomes difficult. So the value of information entropy should not be more than 8. If entropy is less than 8, there is possibility certain degree of predictability [15]. The basic formula of information entropy is defines as.

$$H(S) = \sum_{i=0}^{2N-1} P(s_i) \log\left(\frac{1}{P(s_i)}\right) \quad (8)$$

Here $P(s_i)$ is the probability of the ith gray level and n is the number of gray level in the image (256 for 8 bit images).

IV. CONCLUSIONS

In the digital world, the security of images has become more important as the communication has increased rapidly. In this paper, we have reviewed existing techniques on image encryption. We also gave general guide line about cryptography. We can say that all techniques are useful for real-time image encryption. Many of the existing techniques could only find a low level of security. To achieve the substantial security, we can use existing image encryption techniques but only few existing image encryption techniques fulfill this requirement. The security analysis parameter shown that the existing image encryption techniques are resistive against the different attacks like statistical attacks, key sensitivity analysis attack etc.

REFERENCES

[1] K. Pareek, VinodPatidar, "*Image encryption using chaotic logistic map*", Elsevier, Image and Vision Computing 24 (2006) 926-934.

[2] Chao-Shen Chen, and Rong-JianChen, "*Image encryption and decryption using scan methodology*", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006 IEEE.

[3] TiegangGao, Zengqiang Chen, "*A new image encryption algorithmbased on hyper-chaos*", Physics Letters a 372 (2008) 394–400

[4] Vinod Patidar ,N.K. Pareek , K.K. Sud, "*A new substitution–diffusion based image cipher using chaotic standard and logistic maps"*, ELSEVIER , Communications in Nonlinear Science and Numerical Simulations 14 (2009) 3056–3075.

[5] BibhudendraAcharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and GanapatiPanda,"*Image encryption using advanced hill cipher algorithm*", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[6] DeWang, Yuan-Biao Zhang, "image *encryption algorithm based on s-boxes substitution and chaos random sequence*",International Conference on Computer Modeling and Simulation, 2009 IEEE.

[7] Mao-Yu Huang, Yueh-Min Huang,"*Image encryption algorithm based on chaotic maps*", 2010.

[8] SeshaPallaviIndrakanti ,P.S.Avadhani,"*Permutation based Image Encryption Technique*", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[9] Amitava Nag, JyotiPrakash Singh, SrabaniKhan,SaswatiGhosh,"*Image encryption using affine transform and xor operation*",2011 IEEE.

[10] G. Nagaraju and T. V. Hyma Lakshmi,"*Image encryption using secret-key images and scan patterns*",Int. J. of Advances in Computer, Electrical & Electronics Engg., Vol. 2 , Sp. Issue of NCIPA 2012, 10th Dec. 2012 @ISSN: 2248-9584.

[11] Xuan Li,"*Image encryption scheme based on multiple chaotic maps*", Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013 IEEE.

[12] Sunil Kumar K.M, Kiran, Anand U Hire math, "*Image encryption using modified 4 out of 8 code and chaotic map*", 2013.

[13] Narendra K. pareek, VinodPatidar and K. K. Sud, "*Diffusion substitution bsed gray image encryption scheme*", Digital Signal.

[14] Ahmed, Hossam El-din H., Hamdy M. Kalash, and Osama S. Farag Allah, "*An efficient chaos-based feedback stream cipher (ecbfsc) for image encryption and decryption*",INFORMATICA-LJUBLJANA-31, no. 1 (2007): 121.

[15] M.Sabery.K, M.Yaghoobi,"*A new approach for image encryption using chatio logistic map*",International Conference on Advanced Computer Theory and Engineering, 2008 1EEE.