*THINK INDIA JOURNAL*

ISSN:0971-1260

Vol-22-Issue-10-November-2019

# A Research Paper on Image Encryption & Decryption Techniques

Monika[#1], Pooja[#2]

[1]Department of Computer Science
International Institute of Technology & Business (IITB),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[1]monikachauhan1019@gmail.com

[2]Department of Computer Science
International Institute of Technology & Business (IITB),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[2]poojakumari1992@gmail.com

***Abstract***— Security is one of the important aspects in computing. In data transfer, security must be considered as one of the method implemented to ensure secure data transfer. Data transfer is transferring information from a location or host to another host, or server. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used. In this we provide literature reviews on various image encryption techniques.

***Keywords— Image Encryption, Digital Image***

## I. INTRODUCTION

The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, and this method is called encryption. To make a message unintelligible, it scrambled according to a particular algorithm, which is agreed upon beforehand between the sender and the intended recipient. Then, recipient can reverse the scrambling protocol and make the message comprehensible. This reversal or scrambling is known as decryption. The advantage of using encryption and decryption is that, without knowing the scrambling protocol, the message is difficult to recreate. Cryptography has its roots in communication security [1]. Communication security is described in this figure 1 below.

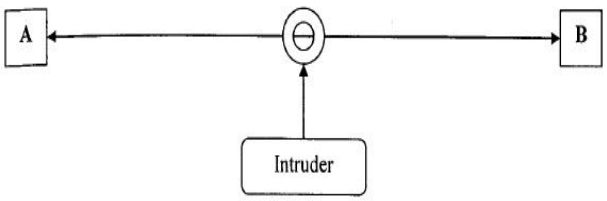


**Figure 1:** The Communication Security

The above figure is the description of two entities that tries to communicate over an insecure channel. The antagonist is an intruder who has full control over this channel, being able to read their messages, delete messages and insert messages. The two entities A and B trust each other. They want a protection from the intruder. Cryptography gives them the means to construct a secure logical channel over an insecure physical connection.

Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text. Using encryption security professional can virtually nullify the value of an interception and the possibilities of effective modification and fabrication [1].

Encryption is clearly addressing the need for confidentially of data. Additionally, it can used to ensure integrity that the data cannot be read and cannot be easily changed in the meaningful manner. It is basis of the protocol that enables to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security.

## II. DIGITAL IMAGE

A digital image is defined by an array of individual pixels and each pixel has its own value. The array, and thus the set of pixels, is called a bitmap. If we have an image of 512 pixels × 512 pixels, it means that the

ISSN:0971-1260

Vol-22-Issue-10-November-2019

data for the image must contain information about 262144 pixels [2].

Digital images are produced through a process of two steps: *sampling* and *quantization*. Sampling is the process of dividing the original image into small regions called pixels, whereas quantization is the process of assigning an integer value (i.e. color) to each pixel.

The number of colors (i.e. color space) that can be assigned to any picture element or pixel is a function of the number of bits, which is sometimes referred to as the color depth or bits resolution. This concept is also known as bits per pixel (bpp) that represents the color for each value. The color space is computed using the following equation:

$$ColorSpace = 2^b \quad \text{……..... (1)}$$

where:
*b*: the bit depth

The color values used in each bitmap depend on the specific bitmap format. This means that each pixel in a bitmap contains certain information, usually interpreted as color information. The information content is always the same for all the pixels in a particular bitmap. Thus, each color value in a bitmap is a binary number. A binary number is a series of binary digits that can be either 0 or 1 and called bits. This binary number in a given format will differ in length depending on the color depth of the bitmap, where the color depth of a bitmap determines the range of possible color values that can be used in each pixel. For example, each pixel in a 24-bit image can be one of roughly *16.8* million colors. This means that each pixel in a bitmap has three color values between 0 and 255 and then those colors are formed by mixing together varying quantities of three primary colors: red, green and blue.

Image storage size for an uncompressed image is computed using the following equation:

$$IMGSS = IMGR \times BR \quad \text{….. (2)}$$

where:
*IMGSS*: Image storage size
*IMGR*: Image resolution (i.e. image width × image height)
*BR*: Bits resolution (bits depth)

For example, the storage size of a 640 pixels × 480 pixels, true colored image is given as follows:
$IMGSS = W \times H \times BR$ = 640 × 480 × 24 bits = (7372800/1024/8) = 900 *KB*.

## III. IMAGE ENCRYPTION TECHNIQUES

The two main elements in the encryption process are the keys and the algorithms. The algorithms are defined as complex formulas that dictate the rules of how the plaintext will be encrypted to cipher text [3]. Keys are likely the strings of random bits that are used by the algorithms. In some of the encryption technologies, if two end-points need to communicate with one another, by using encrypted data, they have to use the same algorithm, and most of the time, the same key. In some different encryption technologies, they must use different but related keys for this algorithm. Cryptography algorithms are either asymmetric algorithms, which use asymmetric keys or symmetric algorithms, which use symmetric keys.

### 3.3.1 Symmetric key Encryption

In symmetric key encryption, the receiver and the sender use the same key for decryption and encryption. Symmetric key encryption is also called a secret key, because both sender and receiver must keep the key secret and protected. If two users want to exchange data using secret key encryption, both of them must acquire a copy of the same key.

### Asymmetric key Encryption

Asymmetric key algorithm is also known by the public key algorithm. Public key cryptography described a two-key cryptosystem in which two parties could communicate securely over a non-secure communication channel without having to share a secret key. They worked out the problem of the secret key distribution by using two keys instead of a single key. A public key, which can be known by everyone, and a private key, which should be kept secret and known only by the owner.

## IV. LITERATURE REVIEW

Various types of image encryption techniques are available as explained below.

Sankaran et. al. (2011) [4] proposed “a new chaotic algorithm for digital image encryption and Decryption. Because chaotic image encryption image algorithms suffer from weak security, i.e. small key space and it is one dimensional crypto system, authors developed a new image encryption schema based on three chaotic system. They carried out pixel position permutation by using chaotic system. The proposed system has two stages, the confusion stage and the diffusion stage. In confusion pixel position is scrambled over the entire image by using chaotic system. The chaotic system was controlled by initial condition and controlled parameters which were derived for 16-bit secret key.

ISSN:0971-1260

Vol-22-Issue-10-November-2019

Among the three chaotic dynamic systems i.e. Lorenz, Chen, and LU, one is selected by the system parameter which was obtained from the generated secret key."

K Pareek et. al. (2012) [5] proposed "a non-chaos based image, simple, fast and secured against any attack encryption scheme using an external key of 144-bits. The proposed encryption scheme uses both pixel substitution as well as pixel permutation process. Furthermore, a feedback mechanism is also applied to avoid differential attack and make the cryptosystem more robust. The proposed encryption scheme has high encryption rate, requires less computation and sensitive to small changes in the secret key so even with the knowledge of the approximate key values, there is no possibility for the attacker to break the cipher."

Jinping Fan et. al. (2013) [6] proposed "a colored image encryption and decryption algorithm based on Arnold transformation. The proposed algorithm depends on the encryption key instead of relying on the period of transformation time. Thus, the decryption time of the proposed algorithm is independent of the transformation time, but it's only decided by the encryption time".

T Bhaskara et. al. (2013) [7] implemented "security for image, by considering reading the image pixels and converting it into pixels matrix of order as height and width of the image. Then, replacing those pixels into some fixed numbers, while the secret key was generated using random generation technique. The proposed algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding. Encryption and Decryption of an image by this algorithm protect the image from an unauthorized access".

Kumar and Chahal (2014) [8] proposed "an algorithm which applies scrambling and substituation processes, that is the proposed algorithm provides more uniform histogram which is different from plain image histograms the proposed algorithm works in two phases; scrambling phase and substitution phase. The scrambling phase had the following steps: 1. Applying interchanging operation among rows with the help of key. 2. Applying interchanging operation among columns with the help of key. 3. Operating circular rotation on all rows with the help of key. 4. Operate circular rotation on all columns with the help of key. On the other hand, the substitution phase had the following steps 1. Converting image matrix into one-dimensional array. 2. Picking 50 pixels in sequence and convert into bits. 3. Applying the XOR operation on these bits with a key of 400 bits. 4. Applying a circular shift operation on the result of step 3 with the help of key. 5. Taking the complement of key 6. Applying again XOR operation on the result of step 4 and the complement of key."

Mrunali et. al. (2014) [9] proposed "a colored image encryption technique using visual cryptography scheme. The main advantage of visual cryptography is eliminating the complex computation problem in decryption process, while the secret images can be restored by staching operation. This property makes visual cryptography usefull for the low computation load requirement, and then they created the shares of binary image and encrypting those shares using the shred keys"

Xie et. al. (2015) [10] proposed "an algorithm to encrypt iris image, based on Advanced Encryption standard algorithm (AES). AES Algorithm is a kind of groping encryption algorithm with changeable block plaintext length and key length, AES is a symmetric encryption algorithm which uses the same key for encryption and decryption. The proposed algorithm was compared with scrambling encryption effect of the Arnold. The experiment results show that the image encryption security gained by the proposed algorithm is higher than Arnold algorithm".

Karrar Dheiaa et. Al. (2016) [11] proposed "the modified RSA cryptosystem has a higher security than the RSA cryptosystem, because decrypting any encrypted images requires factoring the large integer composed of the product of many large primes, and it requires knowing the size of the blocks that are formed from plain matrix. Therefore, this approach of encrypting and decrypting images using RSA cryptosystem with some modifications more immune against any attacks in the transmission of images in all agencies in the era of the information technology."

## IV. CONCLUSION

In data transfer, security must be considered as one of the method implemented to ensure secure data transfer. Data transfer is transferring information from a location or host to another host, or server. To have a secure data transfer, few method can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used. In this we provide literature reviews on various image encryption techniques.

## REFERENCES

ISSN:0971-1260

Vol-22-Issue-10-November-2019

[1] Kundan Kumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* Volume 3, Issue 3, May – June 2014

[2] Ralf Steinmetz und Klara Nahrstedt, "Multimedia Fundamentals", Volume 1, 2nd Edition Prentice Hall January 2002 ISBN 0130313998.

[3] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", Third Edition, © 2008 by Pearson Education, Inc.

[4] Sankaran, K., Krishna, B., "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colored images", IJIET, 137-141, 2011

[5] K Pareek, N., "Design and Analysis of a Novel Digital Image Encryption Scheme, Key Generation Method Using Image Features", Journal of Information Technology. 2012.

[6] Jinping Fan, Yonglin Zhang. (2013), "Colored image Encryption and Decryption" Based on Journal of Computer Applications, 97(12), 18-22, 2013.

[7] T Bhaskara; Yaragunti, Hema Suresh; Reddy, T Sri Harish; Kiran, S.(2013), "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique", International Journal of Computer Technology, 4.6883-891.

[8] Kumar, M . Chahal, A. (2014), "An Image Encryption Technique to Remove the Drawback of the One-Dimensional Scrambling Method of Image Encryption", International Journal of Computer Applications, 97(12), 18-22.

[9] Mrunali T. Gedam. (2014), "Image Encryption Technique Based on Visual Cryptography", International Journal of Research (IJR), Vol-11, No.1.

[10] Xie, R, Wang, M., & Hai, B. (2015), "Image Encryption Research Based on Key Extracted from Iris Feature", IJSIA, 9(6), 157-166.

[11] Karrar Dheiaa Mohammed AlSabti 1 and Hayder Raheem Hashim, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB", Global Journal of Pure and Applied Mathematics. ISSN 0973-1768 Volume 12, Number 4 (2016), pp. 3631-3640