International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
Vol. 48, Issue 01, Quarter 01 (January-February-March 2019)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Encryption of Image by Different Techniques: A Survey

Reenu Batra[1] and Kanishka Raheja[2]

[1,2]Department of Computer Science & Engineering, SGT University, Gurugram, India
[1]reenu_fet@sgtuniversity.org and [2]kanishka.raheja@gmail.com

Publishing Date: February 28, 2019

Abstract

In Multimedia Communication, Secure Image Transmission plays an important role. On internet we can transmit data in form of text, audio, image and video. Security of data is a challenging task over an unsecured communication channel. We may use encryption concept for transmitting data for security purpose. For this we have to encrypt our data image at sender point and decrypt image at receiver end. This paper provides an overview of various image encryption techniques used so far. With the help of this paper we will compare these encoding schemes applied on an image.

Keywords: *Security, Cipher, Encryption, Decryption.*

1. Introduction

With advance use of internet technology, people use a variety of images for communication over internet. Some of areas where security of image transmission plays an important role like military, international agencies, national and international affairs becauseimage may contain confidential data. For secure communication three factors are necessary for an image. These are confidentiality, integrity and authentication [6].

For the image cryptography we have basically three steps:

(i) Input original image
(ii) Encrypt image by using a key (encryption)
(iii) Decrypt image by using same key Decryption)
(iv) Output ciphered image

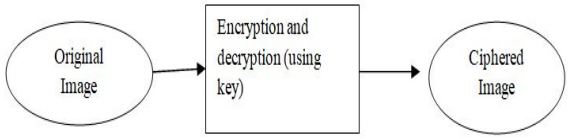

Figure 1: Cryptography Concept

Cryptography can be done by two different methods: one of method is called Symmetric key cryptography andother method is called Asymmetric key cryptography. Other name for symmetric key cryptography is secret key cryptography and Asymmetric key cryptography is also called public key cryptography. The main difference between in both of these methods is that one single key is used for both sender and receiver at source end and destination end, in symmetric method. Instead two different keys are used in asymmetric cryptography, we use a pair of keys for ciphering and deciphering image (public key and private key) [6]. Algorithms like RSA, AES and DES are applicable to encrypt text data. However, images have sufficient repetition pixel feature and all the near -by pixels have strong mutual relationship. So, image encryption requires an invulnerable security. Encryption methods/techniques are based on some factors like pixel permutation, pixel substitution and visual transformation [1]. ANN (artificial neural network) is a one-way nonlinear technique for securing the image and gets the outcome but it has difficulty in getting raw data from outcome received. Compression is another technique used for encoding of an image but it has difficulty in understanding the compressed image. However, compression can be lossy and lossless [4].

2. Image Security Parameters

While designing an encryption technique some of the factors must be keep in mind to make a more secure encryption of image.

2.1 Distribution of Numerical Data (Histogram)

Histogram is a pictorial representation, defines the distribution of frequency values and density estimation of continuous pixels.For an encrypted image histogram must be uniform so that it can be differentiated with plain text image having non-uniformhistogram [6].

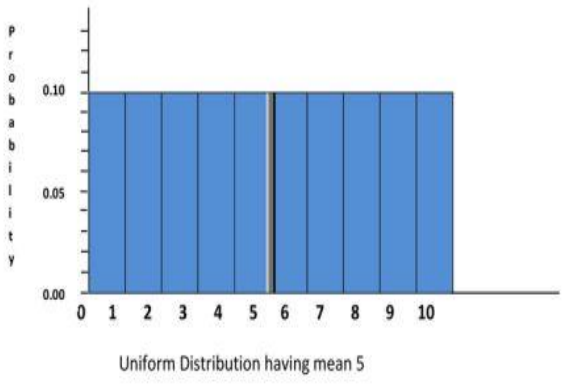

Figure 2: Graph Showing Probability and Uniform Distribution Relationship

2.2 Entropy

Entropy defines the how likely the chances of desired outcome, which is basically known as uniformity of distributions shown in Fig.2. For a good encryption technique there must be a uniform distribution. It depends upon the how much bits exist for each pixel value and chances of occurrence of a pixel value. For example an image that has gray scale value, has per pixel value of eight bits. It can be calculated as: $e(p)= -\sum Pr(p)* \log 2\ Pr(p)$, for each bit in a pixel.

2.3. Possible Key Values

A collection of key values required for an enciphering algorithm is called key space. **A** big area of key space required for enciphering anddeciphering process. If there is a key of size n bits, then the key size will be 2n. For a good encryption technique key size must be large so that key space.

2.4. Effectiveness of Key (Sensitivity)

For any of the encryption Standard, key sensitivity is required. As we assume the system will generate a completely different sequence despite of a minor changes in key value.
Adjacent Pixel correlation: For a ciphered image the correlation between near-by pixels must be very less. The nearby pixels may lie on horizontal axis or vertical axis or diagonal axis.We can calculate it by knowing the mean of pixels and covariance of pixels

3. Techniques used for Image Encryption

3.1 Block Image Encryption Algorithm (1997)

An encryption algorithm was given by Jiri Fredrich in year 1997 in which symmetric block encryption scheme was introduced by making use of invertible chaotic 2-D maps. This algorithm is mainly applicable on digital images.

3.2 Digital signatures-based Encryption of image (2003)

This technique was proposed in 2003 by making use of digital signature of plain image in to encrypted version of image [3]. Encoding of image can be done by using a error control code. At the time of the decryption process these digital signatures can be used to find out whether image is real or not and the real image will be an authentic image.

3.3 Encryption by using dividing method (2003) [1]

In this encryption of image is done with help of Binary XOR and image dividing Technique. In this firstly Binary Images are converted in to binary phase

encoding and then these images are encrypted with binary random phase images by using binary phase XOR operation. We can get Encrypted Image by combining binary encrypted images.

3.4 An approach "Advance Hill Cipher "(2008)

The difficulty with Hill Cipheralgorithm was that by using random key matrix we were not able to decrypt the encrypted image. So, an advanced algorithm was introduced in which involuntary matrix that is basically invertible. In this process we divide our whole image in to small units which are called blocks and then we apply involuntary key matrix to each of block and then we find out some kth value and multiply with matrix whose inverse is same as the of its own and then interchange rows with columns and columns with rows and then pass on this image to receiver [6].

3.5 Security of image using combination of permutation (2008)

A permutation technique was described having a different way to combine the permutation of original image and an encryption algorithm called RijnDael. In this encryption technique we first divide our image in to 4 × 4 pixels blocks and these blocks are rearranged using a permutation process. After this process an image is generated which is encrypted by using RijnDael Algorithm? This Technique results a low correlation between pixels and high entropy [6].

3.6 Encryption based on modified DES (2009)

In order to encrypt image using this technique firstly a pseudo random sequence is generated by making a use of logistic chaos sequencer and then a double encryption is used with improved DES [3]. As a result, a high security and high encryption speed is achieved.

3.7 Encryption by using Hash Function (2010)

A novel encryption algorithm was developed that was based on SHA-512. There are mainly two parts in this algorithm, in which first part is used to jumble first half portion of the image and in the second portion a basic function called hash function is used to generate a random number mask which is then processed with other part of image that we want to cipherby using a logical operation named XOR[6].

3.8 Ciphering by composing two chaotic logistics maps (2010)

In this image encryption technique a pair of logistics maps are incurred to make confusion between encrypted image and original image. A large external symmetric key of 104 bits is used. After the encryption of each pixel, secret is modified. Encryption of each pixel mainly depends upon key value, previous cipher pixel value and logistic map output [1].

3.9 Encryption by modified Advanced Encryption Standard based algorithm (2010)

To get a high security and better image encryption a modification is done in Advanced Encryption Standard (MAES). As compared to original AES, better results are achieved.

3.10 Encryption based on affine transform and XOR (2011) [7]

In this technique image pixels are shuffled using affine transform and then resulting image is encrypted using XOR operation [7]. The pixel values are redistributed on different locations using affine transform with help of four 8-bit keys. The transformed image is then encrypted by dividing in to 2×2 pixels block and each block is encrypted using four 8- bit keys[7].

3.11Image Encryption based on Permutation (2011)

This technique is also called random pixel permutation technique. In this process firstly, image is encrypted by using encryption process and then key is generated and finally identification process takes place. This process is very quick and effective.

3.12 Genetic Algorithm based Encryption (2011)

This way of ciphering the data is based on genetic algorithm and function called chaotic. The encrypted image is generated from plain image by use of chaotic function. For the genetic algorithm, this encrypted image is used as initial population for starting of process in order to optimize the encrypted image[9].

3.13 Encryption using chaotic map and noise effects (2011)[8]

Four maps: Cross chaotic, logistic, Ikeda, Hanon are compared with each other. It is found that chaotic maps give best result. When we encrypt our image using chaotic map and then apply noise on it followed by decryption process by removing applied noise, we get best result.

3.14 Encryption based on multiple chaotic systems (2011)[8]

In this encryption technique two chaotic systems are added together to form a new encryption technique: Lorenz chaotic system and Rossler chaotic system. The result gives high security and high speed.

3.15 Differential Evolution approach for encryption (2011)

A new encryption method was developed by Ibrahim S I Abuhaiba which was based on magnitude and phase manipulation. To gain more security there is need to check the sensitivity of key and check the size of key space[6].

4. Conclusion

In present time, protection of data over network is of major concern. In this paper, we analyze various techniques that can be applied on image encryption. These techniques vary according to key space, key sensitivity and security measures. The techniques that are so far discussed are useful in many applications to provide security. In this paper we also studied about cryptography concept and how cryptography can be imposed on various digital images by using a number of techniques. In this way we can transfer an image over network so that only authorized person can access the original data. By studying different encryption techniques, we can choose our best in terms of high security and high speed.

References

[1] Komal D Patel, Sonal Belani, “Image Encryption Using Different Techniques: A Review”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011).

[2] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture, Pattern Recognition and Image Analysis”, Vol.10, no.2, pp.236-247, 2000.

[3] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229-234.

[4] S.S. Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229- 1245.

[5] William stallings, —”Cryptography and Network Security: Principles & Practices”‖, second edition.

[6] Mohit Kumar, Akshat Aggarwal, Ankit Garg,” A Review on Various Digital Image Encryption Techniques and Security Criteria ”International Journal of Computer Applications (0975 – 8887) Volume 96– No.13, June 2014.

[7] Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, ParthaPratim Sarkar “Image Encryption Using Affine Transform and XOR Operation” 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[8] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu “A New Chaotic System for Image Encryption” 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73.

[9] Qiudong Sun, Ping Guan, YongpingQiu, YunfengXue “A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling” 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669-1672.