Digital Image Encryption Techniques: A Review

*Payal Sharma, **Manju Godara, ***Ramanpreet Singh
*Student M.Tech, JCD, Sirsa
** Assistant Professor, JCD, Sirsa
***Lecturer GKU, Talwandi Sabo
*bhj.payal@gmail.com, ***errpsingh@gmail.com

Abstract: As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. In this paper review of various encryption techniques that are existing is given. It also focuses on the functionality of techniques.

Keywords: Chaotic key, Cryptography, AES, Huffman Table.

1. Introduction

Image encryption is a technique which provide security to images by converting original image to another image which is difficult to understand. In the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images. Encryption is one the ways to ensure security. Nobody could get to know the content without a key for decryption.

2. Image Encryption is different from Text Encryption

Text encryption algorithms are not directly implemented to images because image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

3. Architecture of Image Encryption Model[1]

For encryption and decryption a symmetric key model has been used. The architecture of image encryption and decryption model is described in Figure –1 and Figure 2.

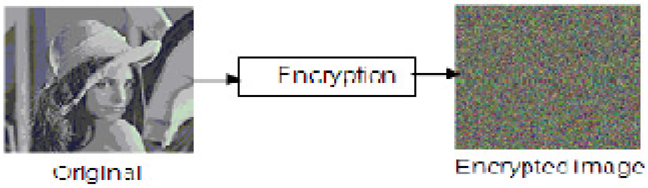

Fig 1. Image Encryption

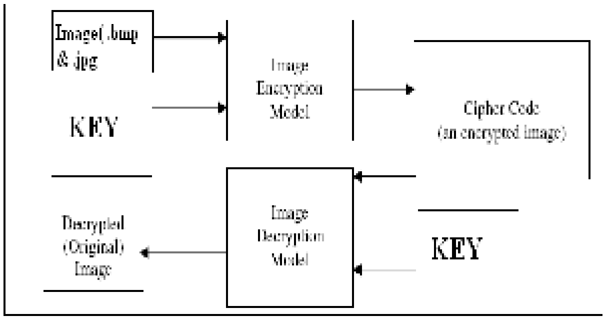

Figure 2

4. **Categories of Encryption Techniques:**

Encryption techniques are generally categorized into following three:

- **Position permutation techniques:** In this technique the order of the pixels of an image is changed so thet the information is invisible.
- **Value transformation techniques**: In this the weights and biases of the network are set according to a binary sequence generated from a chaotic system, for encryption or decryption of each signal element.
- **Combination**: This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values.

5. **Performance Parameters of Encryption Technique**

There are some few parameters on which encryption technique is evaluated.

- **Visual Degradation (VD):** This criterion measures the perceptual distortion of the image data with respect to the plain image. In some applications, it could be desirable to achieve enough visual degradation, so that an attacker would still understand the content but prefer to pay to access the unencrypted content. However, for sensitive data, high visual degradation could be desirable to completely disguise the visual content.

- **Compression Friendliness (CF):** An encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase.
- **Format Compliance (FC):** The encrypted bit stream should be compliant with the compressor. And standard decoder should be able to decode the encrypted bit stream without decryption.
- **Encryption Ratio (ER):** This criterion measures the amount of data to be encrypted. Encryption ratio has to be minimized to reduce computational complexity.
- **Speed (S):** In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.
- **Cryptographic Security (CS):** Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-ciphertext attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic.

6. Literature Review

The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique. To study and analyze more about the encryption techniques, the following literature survey has done and discussed in this chapter.

6.1 Securing Image Transmission Using In-Compression Encryption[1] : In this algorithm, Shaima A. El-said, Khalid F. A. Hussein, Mohamed M. Fouad , discover a new OMHT compression-encryption technique which is a modification to the MHT scheme. It generates different Huffman tables for each type of images instead of using fixed Huffman tables for all images as in MHT technique. The main advantage of using OMHT technique over other lossy compression technique is that it produces a much smaller compressed file than any compression method, while still meeting the advantage of encryption.

6.2 Modified AES Based Algorithm for Image encryption[2]

This technique is proposed by ,M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. They give a new modified version of AES, to design a secure symmetric image encryption technique. The main problem of AES encryption is textured zones exist in encrypted image. This problem was removed by the support of key stream generator for image encryption. The two main key stream generator used are (i) A5/1 key stream generator and (ii) W7 key stream.

6.3 **Image Encryption Using DCT and Stream Cipher[3]**

In this algorithm the DCT which is a mathematical transformation, is used. DCT takes a signal and transforms it from spatial domain into frequency domain. Many digital image and video compression schemes use a block-based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images.

6.**4 Image Encryption Using Block-Based Transformation Algorithm[4]**

This technique is proposed by Mohammad Ali ,Bani Younes and Aman Jantan. In this , transformation technique works as follows: the *original* image is divided into a random number of blocks. Then these blocks get shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. So this technique reduced the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

6.5 **Image Encryption Using Advanced Hill Cipher Algorithm[5]**

In this paper ,Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They took different images and encrypt them using both techniques original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And in the results it is clarified that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. In compared to it the proposed algorithm works for any images with different gray scale as well as color images.

6.6 **Digital image encryption algorithm based on chaos and improved DES[6]**

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. Their result show high starting value sensitivity, and high security and the encryption speed.

6.7 **A Novel Image Encryption Algorithm Based on Hash Function[7]**

In this Abbas Cheddad , Joan Condell , Kevin Curran , Paul McKevitt a novel way of encrypting digital images with password protection using 1D SHA-2 algorithm coupled with a compound forward transform. A spatial mask is generated from the frequency domain by taking advantage of the conjugate symmetry of the complex imagery part of the Fourier Transform. This mask is then XORed with the bit stream of the original image. Exclusive OR (XOR), a logical symmetric operation, that yields 0 if both binary pixels are zeros or if both are ones and 1 otherwise.

6.8 **A Technique for Image Encryption using Digital Signatures[8]**

In this paper , Aloka Sinha and Kehar Singh have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

Conclusion

There are so many technique to make an image secure. In this research we define so many techniques. Some of the encryption techniques used selective part of an image for encryption and some others apply encryption algorithm on whole image bit by bit. Each technique has its own suitability area. Each technique has its own limitations.

References

[1] Dr. D. M. Shah, "Image Encryption & Decryption model".

[2] Shaima A. El-said, Khalid F. A. Hussein, Mohamed M. Fouad ,"Securing Image ransmission Using In- Compression Encryption"

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. "Modified AES Based Algorithm for Image encryption"

[4] Mohammad Ali, Bani Younes and Aman Jantan,"Image Encryption Using Block-BasedTransformation Algorithm"

[5] Mohammad Ali ,Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm"

[6] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda "Image Encryption Using Advanced Hill Cipher Algorithm"

[7] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di "Digital image encryption algorithm based on chaos and improved DES"

[8] Abbas Cheddad , Joan Condell , Kevin Curran , Paul McKevitt "A Novel Image Encryption Algorithm Based on Hash Function"

[9] Aloka Sinha and Kehar Singh "A Technique for Image Encryption using DigitalSignatures"