ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Image Encryption and Decryption using Shifting Technique

B.Visalakshi[1], Dr. T. Meyappan[2]
M.Phil Scholar[1], Professor[2]
Department of Computer Science
Alagappa University, Karaikudi, India

Abstract:
In present stretches, the fortification of multimedia data is becoming very important. Images disproportionately contribute to communication in this age of multimedia. The protection of this image can be done with encryption. There are various techniques which are revealed from time to time to encrypt the images to make images more confident. Encryption is one way to ensure virtuous security from unapproved access in many fields like military communication and medical sciences. . Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., cipher text). In this paper, we divide the image into blocks and then transformed by shifting the columns from left to right and right to left. After that Blowfish algorithm applied.

Keywords: Blowfish, Blocks, Cryptography, Encryption, cipher text

I. INTRODUCTION

Cryptography is the science of secret writing is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet. [1]

There are five primary functions of cryptography today:

1. *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
2. *Authentication:* The process of proving one's identity.
3. *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
4. *Non-repudiation:* A mechanism to prove that the sender really sent this message.
5. *Key exchange:* The method by which crypto keys are shared between sender and receiver. Blowfish is a symmetric block cipher that can be effectively used for encryption and protection of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data.[2] The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet [3]. With the rapid growth of communication and internet technology, there is always a rising concern about the safekeeping of multi-media information such as image. A major challenge is to protect the confidentiality. Applications like information storage, information transformation, information security, telemedicine, military information security etc. which require information security. An image encryption technique is nothing but to convert original image to another image that is tough to recognize, to keep the image trusted between users. it is essential that nobody could get to know the content without a key for decryption.

The image to be encrypted was divided into blocks. After dividing it into blocks it was shuffled using shifting technique i.e. left blocks are shifted into right and the right one into left. Then a well-known Blowfish algorithm applied to provide confidentiality. [4]

II. LITERATURE SURVEY

M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images" [5] this paper describes several techniques to encrypt uncompressed and compressed images. In the usual ways to encryption, all the information is encrypted. But this is not mandatory. In this paper we follow the principles of a technique initially proposed by MAPLES and encrypt only a part of the image content in order to be able to visualize the encrypted images, although not with full precision. This concept leads to techniques that can simultaneously provide security functions and an overall visual check which might be suitable in some applications like, for example, searching through a shared image database. The principle of selective encryption is first applied to uncompressed images. Then we propose a simple technique applicable to the particular case of JPEG images. This technique is proven not to interfere with the decoding process in the sense that it achieves a constant bit rate and that bit streams remain compliant to the JPEG specifications. Then we develop a scheme called multiple selective encryption, discuss its properties and conclude.

S. Changgui, B. Bharat, "An efficient MPEG video encryption algorithm" [6] Multimedia data security is important for multimedia commerce. Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable to multimedia applications because of large data sizes and real time constraints. For multimedia applications, light weight encryption algorithms are attractive. They present an efficient MPEG video encryption algorithm. This algorithm uses a secret key randomly changing the sign bits of encoded differential values of DC coefficients of I pictures and the sign bits of encoded differential values of motion vectors of B and

P pictures. The encryption effects are achieved by the IDCT during MPEG video decompression processing. This algorithm adds very small overhead to MPEG codec. A software implementation is fast enough to meet the real time requirement of MPEG video applications. Experimental results show that this algorithm achieves satisfying results. We believe that it can be used to secure video-on-demand, video conferencing and video email applications.

S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," [7]

Fast lightweight encryption algorithms must be developed to satisfy the level of security and the real time constraints. However the proposed lightweight MPEG video encryption algorithms that have been proposed in the past suffer from certain drawbacks. While some of them require hardware support, the others are weak or reduce the MPEG compression ratio. The lightweight encryption algorithm called VEA is fast, satisfies the real time constraint and does not reduce the MPEG compression ratio. However, it relies on the key generator to generate a good encryption key and it cannot withstand the known-plaintext attack. Improvements to the VEA are proposed namely the rotation algorithm, the XOR algorithm and one that combines VEA with IDEA (I-VEA). They are able to secure MPEG video with minimal computational overhead, which do not reduce the MPEG compression ratio, do not rely upon the key generator to generate an effective key and can better resist the known-plaintext attack. The rotation algorithm is the fastest of the three, but is relatively weak. I-VEA is the most secure but it adds the maximum computational overhead. The XOR algorithm is a good compromise between the two.

S. P. Nana'vati., P. K. panigrahi. "Wavelets: applications to image compression- I" [8]

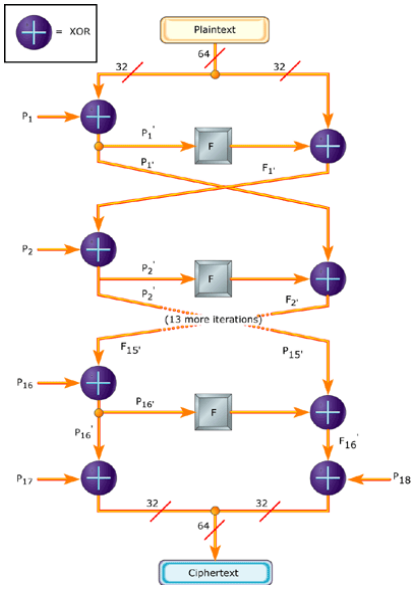
Digital imaging has had an enormous impact on, scientific and industrial applications. Uncompressed images require considerable storage capacity and transmission band width. The solution to this problem is to compress an image for desired application. Wavelet transform has recently emerged as the tool of choice for image compression. In this article, we discuss the basic principles underlying compression of images and point. Out the advantages of wavelet transform over the previously used discrete cosine transform.

W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images" [9]

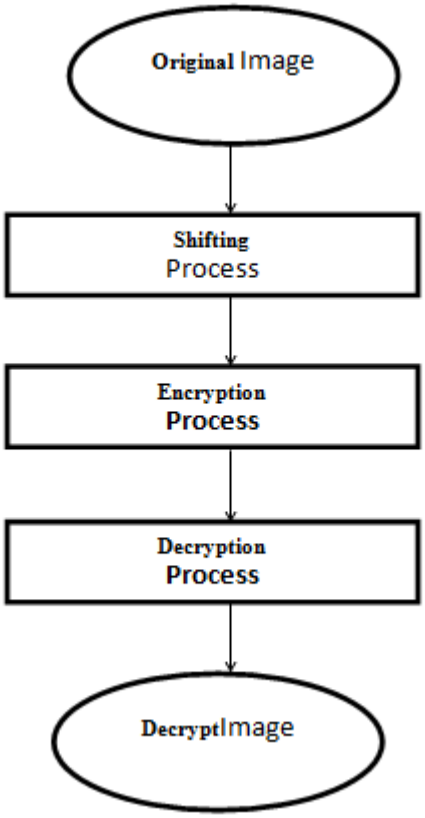
Chung and Chang proposed an encryption scheme for binary images based on two-dimensional run-encoding (2DRE) and scan patterns. In this paper, we indicate that their scheme is still not secure and efficient enough. Hence, an improvement scheme is proposed. There are two contributions in the proposed improvement scheme. One is to exchange the sequence of compression and encryption. The other is to adopt XOR and substitution operations for encryption. Hence, the improvements on encryption time, compression ratio and security are possible.

III. METHOD

In this, the four combination technique is applied to divide and shuffle the positions of the pixels of the original image, encrypt the transformed image, and then embed secret information (the number of horizontal and vertical blocks) in the encrypted image data prior to transmission to the receiver. lowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.



Block diagram of Shifting Technique



The objectives of the proposed system are follows:

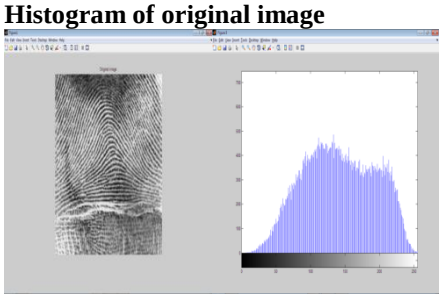
1.A new algorithm has been developed for secure transmission of image data over wired/wireless network.
2. The system has been comparing the correlation, entropy and histogram of different images with and without the proposed algorithm.
3. The system has been produced various security levels of the encrypted images generated by the combination technique and the Blowfish algorithm.
4. A method has been introduced to exchange the secret image information between the sender and the receiver that will be used for secure transmission.

IV. RESULTS AND DISCUSSION

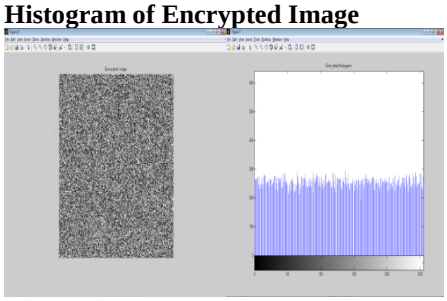
Histogram Analysis

- Histograms may reflect the distribution information of the pixel values of an image.
- An attacker can analyse the histograms of an encrypted image by using some attacking algorithms and statistical analysis on the encrypted image to get some useful information of the original image.
- It is important to ensure that encrypted and original images do not have any statistical similarities.
- The histogram analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity level.

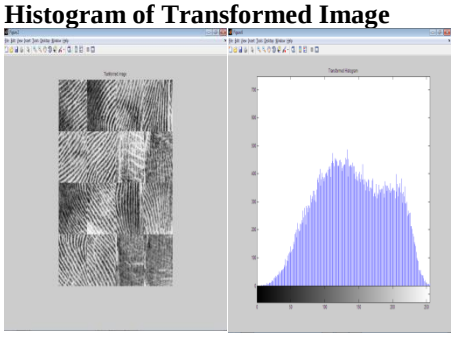
Histogram of original image



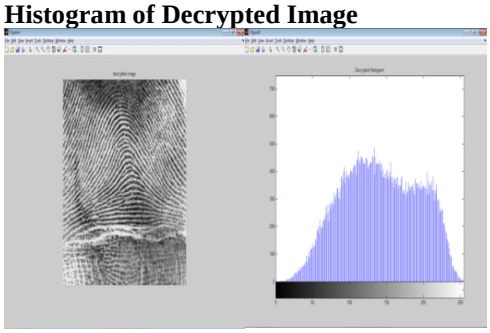
Histogram of Encrypted Image



Histogram of Transformed Image



Histogram of Decrypted Image



Correlation Factor

- In addition to the histogram analysis, I have also analyzed the correlation factor.
- I find the correlation between the original image and the decrypted image.
- If the correlation coefficient equals to zero or very near to zero, then the original image and its encryption are totally different i.e., the encryption image has no features and the highly independent from the original image.
- If the correlation coefficient equals to -1, this means encrypted image is negative of the original image. Equation to find the correlation factor

correlation_factor = corr2(Y, I)

Correlation and Entropy values of commonly used Encryption Algorithms

Number	Image encryption algorithm	Measurement	
		Correlation	Entropy
0	Proposed technique(Shifting) 16 x 16	0.0480	7.6448
1	[Block, bit, pixel] Combination	0.0812	2.0632
2	3D Jigsaw transform	0.6095	2.3735

V. CONCLUSION

Proposed algorithm of this paper is simple and strong method. This has improved image security using a combination of block based shifting and encryption technique. This proposed algorithm shows good performance, low correlation and high entropy. Histogram analysis and experimental results shows that proposed scheme has high security level.

VI. REFERENCES

[1]. An Overview of Cryptography Gary C. Kessler April 2017

[2]. BLOWFISH ENCRYPTION ALGORITHM FOR INFORMATION SECURITY Saikumar Manku1 and K. Vasanth2 1 VLSI Design, Sathyabama University, Chennai, India

[3]. A New Image Encryption Approach using Block-Based on Shifted Algorithm Ahmed Bashir Abugharsa, Abd Samad Bin HasanBasari and Hamida Almangush Misurata University Faculty IT UniversitiTeknikal Malaysia Melaka (UTeMM) Misurata University Faculty IT

[4]. Image Encryption Using Block-Based Transformation Algorithm Mohammad Ali BaniYounes and ArnanJantan

[5]. M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[6]. S. Changgui, B. Bharat, "An efficient MPEG video encryption algorithm," Proceedings of the Symposium on reliable distributed systems, IEEE computer society Press, 1998, pp. 381-386.

[7]. S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," proceeding of international conference, single processing, pattern recognition and application, 2002, pp. 25- 28.

[8]. S. P. Nana'vati., P. K. panigrahi. "Wavelets: applications to image compression- I,". Joined of the scientific and engineering computing, vol. 9, no. 3, 2004, pp. 4- 10.

[9]. W. Lee, T. Chen and C. ChiehLee, "Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2003, pp. 191-200.

VII. ACKNOWLEDGEMENT

As the outset, I would like to express my heartfelt gratitude to The Almighty God, for showering his blessings on me to bring out this project successfully.

More words can‘t express the gratitude, to **Dr.V.Palanisamy, *MCA.,M.Tech., Ph.D.*, Professor and Head, Department of Computer Science and Engineering, Alagappa University** who had given the opportunity, guidance and encouragement to do this course. I wish to express my heartfelt thanks to my research guide

Dr.T. Meyyappan M.Sc., M.B.A., M.Tech., M.Phil., Ph.D., Professor, Department of Computer Science, Alagappa University for his valuable guidance to me in the right and easy way to finish the dissertation work very successfully. I also express my special thanks to all faculty members of the Department of Computer Science and Engineering, and Computer Center who spent most of their time for us and for their valuable suggestions and Kind co- operations. I also thank my beloved parents and my family members, my friends for their endless encouragement and helpful suggestions offered to complete this dissertation successfully.