International Journal on Emerging Technologies **3**(1): 102-104(2012)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Review New Symmetric Image Encryption Scheme Based On Correlation Pattern

Ankit Gupta*, Namrata Joshi* and Chetan Nagar*

Department of Computer Science & Engineering

**Jawaharlal Institute of Technology Khargone, (M.P.)*

(Recieved 12 April 2012 Accepted 27 April 2012)

ABSTRACT : Encryption is mainly used to transmit the data over networks. There are so many techniques introduced which are used to protect the confidential image data from any unauthorized access. Multimedia data contains different types of data that includes text, audio, video, graphic, images with the increasing use of multimedia data over internet, here comes a demand of secure multimedia data. Most of the encryption algorithm available is generally used for text data and not suitable for multimedia data. In this dissertation a new symmetric image encryption scheme based on correlation pattern. The idea of this system is to find the pixel interdependency correlation between dependent pixel and independent pixel of image and get grayscale images. Then create the slots of bit and generate the pattern and apply the symmetric key algorithm are use for encryption. Proposed method is secure against the entropy, brute-force, statistical, and differential attacks from a strict cryptographic viewpoint. This cryptosystem has a very powerful diffusion mechanism(a small change in the plain text makes a great change in the cipher image) thus the proposed cryptosystem can be used in different applications, depending on the core algorithm used, Advantage of this approach, is that it reproduce the original image with no loss of information for the encryption and decryption process.

Keywords: Homomorphic Encryption, Secure Multiparty Computation, Johnson-Lindenstrauss embedding

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes therefore the most ancient and basic problem of cryptography is secure communication over an insecure channel. Party A wants to send to party B a secret message over a communication line, which may be tapped by an adversary. The recent advances in technology, especially in computer industry and communications, allowed potentially enormous market for distributing digital multimedia content through the Internet. However, the proliferation of digital documents, image processing tools, and the worldwide availability of Internet access has created an ideal medium for copyright fraud and uncontrollable distribution of multimedia such as image, text, audio, and video content [2]. Image encryption techniques to provide end-to-end security when distributing digital content over a variety of distributions systems. Encryption is a common technique to uphold image security in storage and transmission of digital images are exchanged over network types. Image encryption [12] has application in various fields include internet communication, multimedia systems, medical imaging and Tele- medicine and military communication. The information security has become more important with the progress in the exchange of data and various encryption systems to encrypt and decrypt image and no single encryption algorithm which is satisfied different types of image.In order to dissipate the high correlation among pixels and increase the entropy value, we have introduced a pixel interdependency and differentiate sequential dependent and independent pixel of image and create pattern before it passes them to the encryption algorithm. In this case that correlation, histograms and entropy has used to measure the security level of the images, advantages of this results in a lower correlation , higher entropy value, measures to the security level of the encrypted images. This is similar or different encryption of the variable length secret key is needed in the transformation and encryption process, which is used to build the secret transformation table with a variable number of blocks. If the secret key is changed, another seed will be generated and then the different secret transformation table is obtained. This encryption process can be decreases the mutual information among the encrypted image variables and thus increasing the entropy value Hence, many different techniques should be used to protect confidential image data from unauthorized access. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. Once the cipher text has been produced, it is saved in storage or transmitted over the network. Upon reception, the cipher text can be transformed back into the original plaintext by using a decryption algorithm. Unlike optical encryption, [14] which deals only with light and depends on certain parameters, such as wavelength, phase, and polarization of light waves, the proposed image cryptosystem works directly on digital images. There is no need in the proposed cryptosystem to deal with light using expensive optical fiber circuits. Optical encryption also has a disadvantage

represented in the difficulty of implementation of simple encryption operations such as the Xor operation implemented easily in the proposed cryptosystem.

II. SECURITY ISSUE

Multimedia security in general is provided by a method or a set of methods used to protect the multimedia content. These methods are heavily based on cryptography and they enable either communication security, or security against piracy (Digital Rights Management and watermarking), or both. Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. Such media can be treated as binary sequence and the whole data can be encrypted using a cryptosystem such asAdvanced Encryption Standard (*AES*) or Data Encryption Standard (*DES*) [3]. In general, when the multimedia data is static (not a real-time streaming) it can treated as a regular binary data and the conventional encryption techniques can be used. Deciding upon what level of security is needed is harder than it looks. To identify an optimal security level, the cost of the multimedia information to be protected and the cost of the protection itself are to be compared carefully.

III. DESIGN PRINCIPLES OF AN IMAGE CRYPTOSYSTEM

An efficient image cryptosystem must have a high overall security performance in addition to being flexible. Image security requires the following characteristics [16]

1. The encryption system should be computationally secure. It must require an extremely long computation time to break. Thus, unauthorized users should not be able to read privileged image
2. Encryption and decryption should be fast enough to keep the high performance of the system. The algorithms for encryption and decryption must be simple enough to be carried out by users with a personal computer.
3. The security mechanism should be as widespread as possible. It must be widely acceptable to design a cryptosystem like a commercial product.
4. The security mechanism should be flexible.
5. There should be no expansion of the encrypted image data.

IV. HOMOMORPHIC IMAGE ENCRYPTION

In this technique Ibrahim F. Elusory [19] have proposed homomorphic image cryptosystem. The idea of this system is based on encrypting the reflectance component after the homomorphic transform and embedding the illumination component as a least significant bit watermark into the encrypted reflectance componentThe main idea of homomorphic image processing is based on modeling the image as a product of a constant illumination and varying reflectance. The product is dealt with as a summation using the logarithmic operation. The reflectance component can be separated using a high-pass filter, while the illumination component can be separated using a low-pass filter. Most of the image details lie in the reflectance component while the illumination component is approximately constant. We can carry out the encryption process in the homomorphic domain on the reflectance component, which is the most significant component of the image. Rather than encrypting

the illumination component, which causes redundancy in the image information, it is appended as a least significant bit LSB watermark in the encrypted reflectance component. We use two algorithms for the encryption of the reflectance component—the RC6 block cipher algorithm and the chaotic Baker map algorithm and make a comparison between

V. A TECHNIQUE FOR IMAGE ENCRYPTION USING DIGITAL SIGNATURE

In this scheme, Aloha Sinha and Kehar Singh [4] have proposed a new technique to encrypt an image for secure image transmission using digital signature of the original image is added to the encoded version of original image, the encoding of the images is done using an error control code. An error control code is determined in real-time on the size of the originalimage. The digital Signature enables the recipient of a message to authenticate the sender of a message and verify that the message is intact. create new symmetric block encryption schemes. Achaotic map is generalized by introducing parameters and then discretized to a square lattice of points which represent pixels or some other data items. Although the discretized map is a permutation and thus cannot be chaotic, it shares certain properties with its continuous counterpart as long as the number of iterations remains small.

VI. PROPOSED SCHEME

In this paper, we proposed novel method morphology for image encryption based onpixel inter dependency correlation method. Basically pixel interdependency correlation method is a part of contrast preserving of homomorphic image but in scheme contrast and brightness of a image is doesn't matter. Throw the pixel interdependency we generate dependent and independent set of pixel according to reconstruction of image. From thismethod we generate two different sets, one is dependent pixel and another set is independent pixel. The dependency and independency of another pixel maintain a correlation factor for separation after that we generate binarization of image in the term of pattern it's also called binary pattern image encryption. For the purpose of encryption we use XOR function. Theheart of encryption is sharing a key that's sharing key symmetric. The symmetric encryptionis weak in comparison of asymmetric encryption .instead of that the computational time symmetric encryption is minimum.

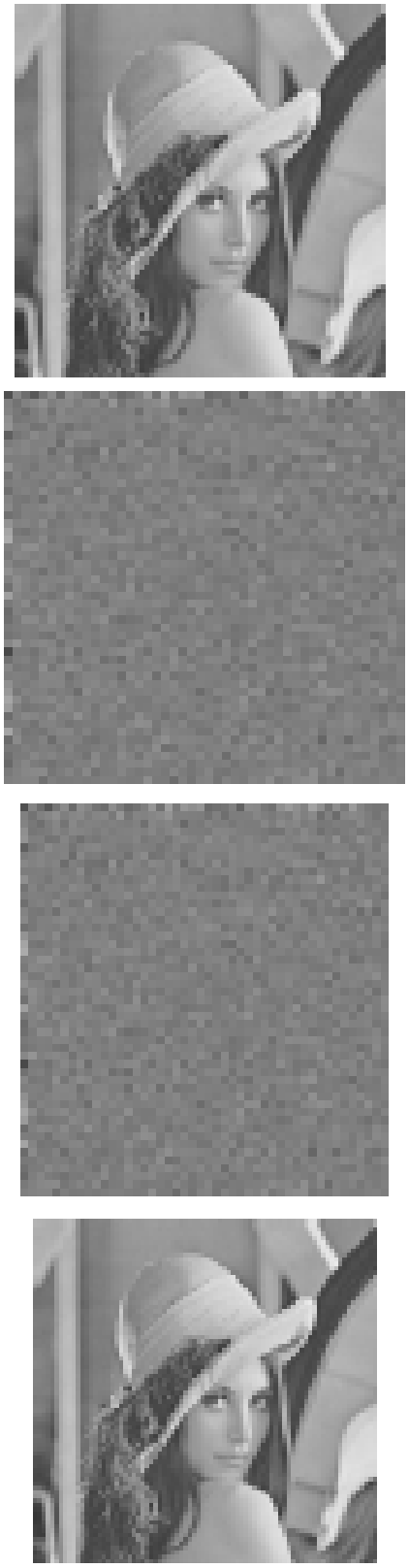

Fig.1: By proposed method (a) Original image (b) encrypted image at sender side (c) encrypted image at reciver side (d) Reconstructed image(decryption and get original image).

VII. CONCLUSIONS

This dissertation describes an application of presented a new image encryption scheme based on correlation pattern. In this scheme obtain first obtain decomposed image by apply transform function on original image and now find the pixel interdependency correlation between the dependent and independent pixel of image. Finally create binary image then generate pattern of the bit and apply the symmetric key encryption algorithm. This system 6. has multilevel of security because encryption is performed in the homomorphic domain

REFERENCES

[1] National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication No. 46, U.S. Government Printing Office, Washington, DC (1977)

[2] Borko Furht, Daniel Socek, Ahmet M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques".

[3] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," *Journal of computer Science*, **1**(1): 2006, p.127, http://www.enformatika.org

[4] Aloha Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[5] Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm " IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[6] Digital Image Processing. R. Gonzalez and R. Woods. Addison-Wesley. (1993).

[7] Li Na, "Digital image enhancement by gray-scale transformation method," Journal of Beijing Polytechnic Colleg, vol. **8**, pp. 36-39 Mar. (2009).

[8] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, *Egypt*, (2006).

[9] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. Of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. *IEEE International Symposium on Publication* Date: 2002, Vol. **2**, 2002, page(s):708–711

[10] Li, H.; Manjunath, B. S. und Mitra, S. K.: Multisensor image fusion using the wavelet transform, in: Graphical Models and Image Processing, Vol. **57**(3): S. 235-245 (1995)

[11] Naveed Islam, William Puech, and Robert Brouzet, "Symmetric ciphers based on two- Dimension chaotic maps," in IWDW. 2009, pp. 121–135,