Secure Transmission of an Image using Partial Encryption based Algorithm

Parameshachari B D
Department of ECE,
JSSATE, Mauritius.
(Research Scholar, Jain University, Bangalore, India)

K M Sunjiv Soyjaudah, PhD.
Department of Electrical & Electronic Engineering,
University of Mauritius, Reduit, Mauritius

Sumitrha Devi K A, PhD.
Department of Master of Computer Applications,
R V College of Engineering,
Bangalore, India.

ABSTRACT

Encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. In this paper we propose a novel concept of combined partial image encryption using phase manipulation and sign encryption. Entire encryption process involves two stages where image to be encrypted are applied to phase manipulation block. In first stage Fourier Transform (FT) is applied to get phase and magnitude of the input image. Phase of the image are scrambled to get modified image after applying Inverse Fourier Transform. In second stage the modified image is partially encrypted by using sign encryption. Sign Encryption finally gives resultant partially encrypted image by extracting the sign bits of modified image. Experiment is conducted for an image using MATLAB software. From the experiment we obtained partially encrypted image at the end of encryption process. Decryption process employs exactly reverse process of encryption which results in the reconstructed images.

General Terms

Security, Encryption

Keywords

Decryption, Phase manipulation, partial encryption, sign encryption.

1. INTRODUCTION

Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data, irrespective of the fact that the data is being transmitted over a medium or is stored on a storage device [1]. It provides a powerful means of verifying the authenticity of data and identifying the culprit, if the confidentiality and integrity of the data is violated. Because of the development of electronic commerce, cryptographic techniques are extremely critical to the development and use of defence information systems and communications networks. Unlike text messages, image data have their special features such as bulk capacity, high redundancy, and high correlation among pixels, not to mention that they usually are huge which together make traditional encryption methods difficult to apply and slow to process [2].

The issue in traditional cryptosystem in many different areas such as wireless networking, mobile phone services and applications in homeland security is energy consumption for encryption of the large volume visual data. So we are dealing with partial encryption. The objective of the Partial encryption is to reduce the computational workload and processing time and to attain the required security level.

The rest of this paper is organized as follows: Section 2 explains the related work. Section 3 provides the concept of phase manipulation technique. Proposed partial image encryption method using combination of phase manipulation technique and sign encryption is described in Section 4. This paper is concluded by providing the summary of the present work in Sect. 5.

2. RELATED WORK

Prasanna et al. [3] have presented an image encryption method with magnitude and phase manipulation using carrier images. Here they used the concept of carrier images and one dimensional Discrete Fourier Transform for encryption purpose and it deals with private key cryptosystem, works in the frequency domain. *Cheng and Li, 2000* [4] proposed partial encryption methods that are suitable for images compressed with two specific classes of compression algorithms: (a) quadtree compression algorithms, and (b) wavelet compression algorithms based on zerotrees. *H. Cheng and Li, 2002* [5], proposed a novel solution called partial encryption, in which a secure encryption algorithm is used to encrypt only part of compressed data. They proposed partial encryption for quadtree compression. It allows the encryption and decryption time to be significantly reduced without affecting the compression performance of the underlying compression algorithm. *Podesser, Schmidt and Uhl, 2002* [6], selective bit plane encryption using AES is proposed. Several experiments were conducted on 8 bit grayscale images, and the main results retained are following: (i) encrypting only the MSB is not secure; a replacement attack is possible (ii). Encrypting the first two MSBs gives hard visual degradation, and (iii) Encrypting three bit planes gives very hard visual degradation. This scheme is not tunable as fix number of bits are encrypted. *Zeng and Lei, 2003.* [7] Proposed, selective encryption in the frequency domain (8x8 DCT and wavelet domains) is proposed. The general scheme consists of selective scrambling of coefficients by using different primitives (selective bit scrambling, block shuffling, and/or rotation). In 2005, Roman Pfarrhofer and Andreas Uhl [8], proposed selective encryption of JBIG encoded visual data exploiting the interdependencies among resolution layers in the JBIG hierarchical progressive coding mode. Engel and Uhl, 2006. In [9], a JPEG2000 lightweight encryption scheme is proposed. Only lower resolutions are compressed with classical dyadic wavelet transform. For higher resolutions, the algorithm relies on a secret transform domain constructed with anisotropic wavelet packets (AWPs). The aim of this proposal is to allow transparent encryption for applications requiring low-resolution preview. *Nidhi S Kulkarni, Balasuramanian and Indra Gupta, 2008* [10], proposed encryption technique reduces intelligent information in an image by scrambling the image first and then changing the pixel values. The scrambling arrangement is done with the help of a random vector and the pixel values are changed by a simple substitution method which adds confusion and diffusion property to encryption technique. *Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla,2009* [11], proposed only 6.25%-25% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time. *Ju-Young Oh, Dong-Il Yang, Ki-Hwan Chon, 2010* [12], proposed to expand the advandced encrytion standard (AES)-Rijndael with five criteria: the first is the compression of plain data, the second is the variable size of the block, the third is the selectable round, the fourth is the optimization of software implementation and the fifth is the selective function of the whole routine. Jay M. Joshi, Upena D. Dalal [13], proposed to gain a deep understanding of video data security on multimedia technologies and to provide security for real time video applications using selective encryption for H.264/AVC. In [14] enhanced the Chung-Chang's scheme and then a more efficient and secure encryption scheme is obtained. Hence, the proposed scheme improves on Chung-Chang's scheme on the part of encryption time, compression ratio and security. Furthermore, image size affects the speed of encryption; that is, the higher the compression, the better the efficiency. In [15] proposed a partial image encryption technique involves two methods, the first is by pixel value manipulation and other second is by using SCAN mapping method. From the experimental results we conclude that the proposed image encryption method gives very good results. In [16] surveyed that the existing works on the partial encryption techniques and also analyze partial encryption schemes with respect to various parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security.

3. MODIFICATION OF AN IMAGE USING PHASE MANIPULATION TECHNIQUE

Figure 1 shows the block diagram of phase manipulation technique. In this phase manipulation technique we apply Fourier Transform (FT) to all input images to get phase and magnitude values of each images. Phase values of all images are applied to phase scrambling block to give scrambled phase to each images. This scrambled phase along with the original magnitude is applied to Inverse Fourier Transform (IFT) to obtain modified images.

4. PROPOSED TECHNIQUE

The concept of proposed technique can be explained by using the block diagram as shown in Figure 2 image to be partially encrypted by applied to phase manipulation block. Fourier Transform is applied to all input images to get phase and magnitude of all images. By using phase scrambling and Inverse Fourier Transform we get Modified image. Finally these modified images are encrypted by using Sign encryption. Sign encryption means encrypt the sign bits of the modified image with a cipher, as shown in Figure 2. If the modified image coefficient is smaller than 0, then its sign bit is denoted by 0, otherwise, by 1. Thus, the sign-bits can be extracted from the modified image coefficients, encrypted by traditional ciphers and returned to the corresponding modified image coefficients. The results are as shown in Figure 3.

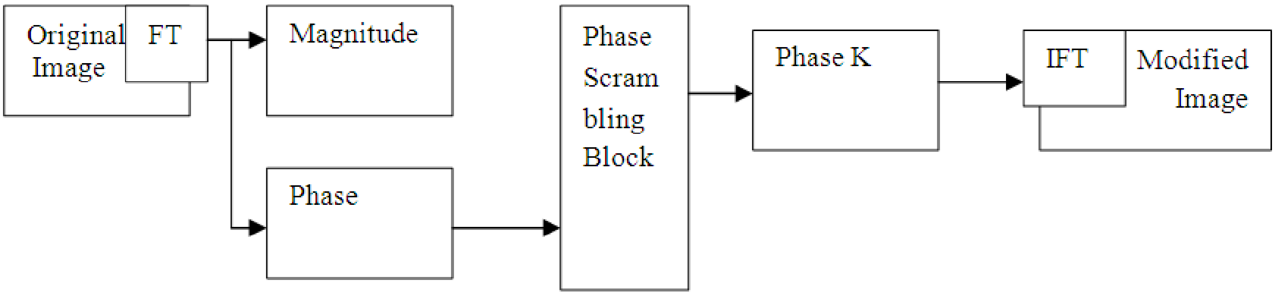


Fig 1: Block Diagram of Phase Manipulation Technique

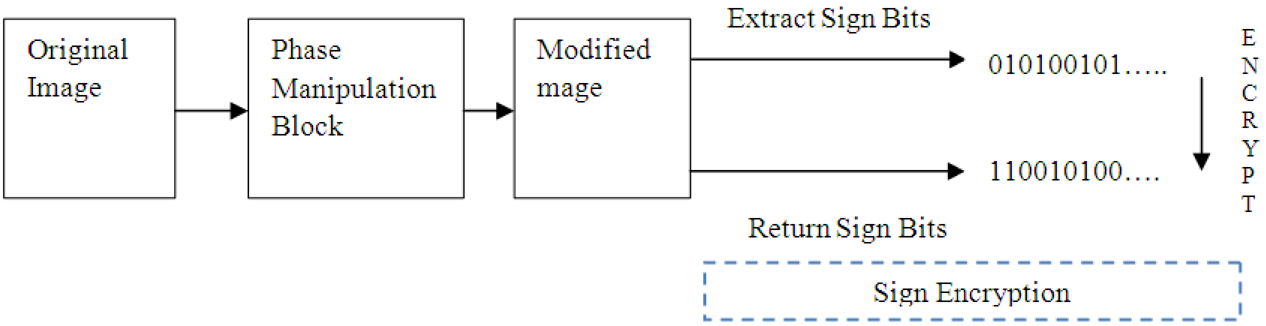
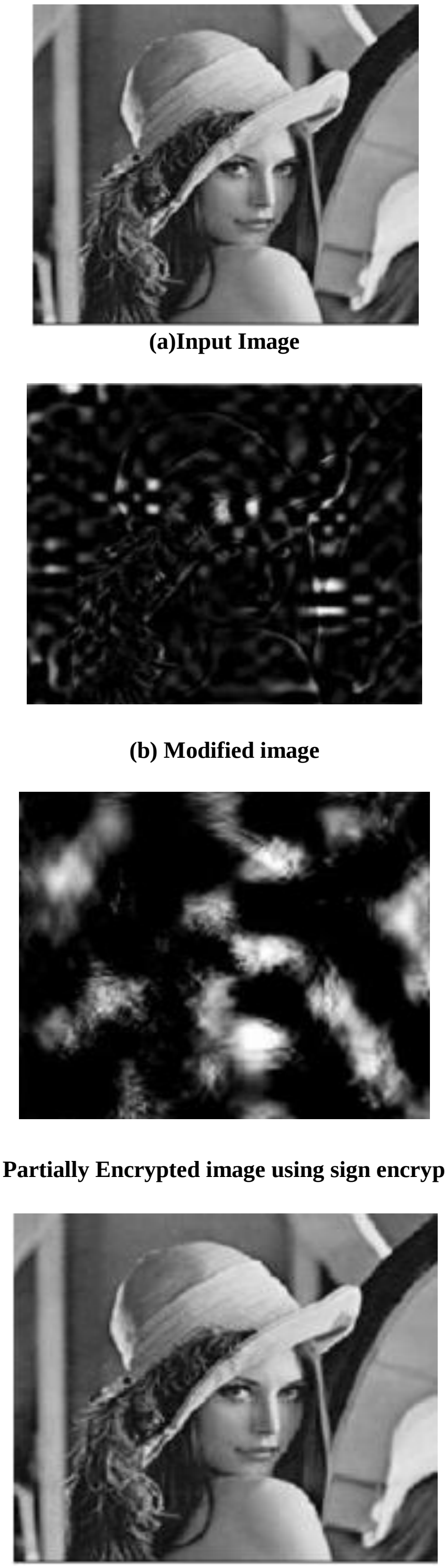


Fig 2: Block Diagram of the Proposed Method



(a)Input Image

(b) Modified image

(c) Partially Encrypted image using sign encryption

(d) Decrypted image

Fig 3: Partial encryption and decryption image.

Table 1 shows the performance and comparison among existing image encryption methods and proposed method with respect to encryption algorithm, speed and cryptographic security. Table 2 shows the Performance Analysis of the encrypted and decrypted images in terms of PSNR (peak signal noise ratio) when tested with different test images of size 512×512. A lower PSNR is obtained in the case of Encrypted Image and a higher PSNR is obtained in the case of decrypted Image. Higher PSNR value shows a better quality of the image. Entropy is a statistical measure of randomness. Entropy is a statistical measure of randomness. Table 3 shows the entropy of different test images of size 512×512.

Table 1. Comparison among existing image encryption methods with proposed method

Methods	Ref	Encryption Algorithm	Speed	Cryptogr-aphic Security
Existing Methods	[4],2000	Not Specified	Fast	Not satisfied
	[5],2002	Not Specified	Fast	Low
	[6],2002	AES	Fast	Medium
	[7],2003	Not Specified	Variable	Low
	[8],2005	Joint Binary Image Experts Group (JBIG)	Fast	High
	[9],2006	Not Specified	Fast	High
	[10],2008	Not Specified	Fast	Moderate
	[11],2009	permutation cipher	Fast	Moderate
	[12],2010	AES	Fast	Moderate
	[13],2011	ISMACryp	Fast	Low
	[14],2012	Scan mapping	Fast	Fast
	[15],2013	Pixel manipulatio n & scan mapping	Fast	Fast
Proposed Method		Phase manipulation in frequency domain and Sign encryption	Fast	Fast

Table 2. Performance Analysis

Test Images	PSNR of the encrypted Image	PSNR of the decrypted Image
Lena	25.7862	95.7745
House	25.5018	95.5298
Airplane	25.7146	95.6129
Step	25.7501	95.6820

Table 3. Entropy of the different Test Images

Test Images	Entropy of the Encrypted Image
Lena	7.5742
House	7.5607
Airplane	7.5823
Step	7.5641

5. CONCLUSION

Partial encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network. In this paper we are presented a novel concept of pixel value manipulation using phase manipulation in frequency domain and sign encryption for partial encryption method. From the viewpoint of security, the experimental results reveal that the proposed partial encryption technique achieves better security than the individual encryption approaches. PSNR values of the encrypted images are low and are resistant to statistical attacks including the ciphertext-only attack and the known/chosen plaintext attack. The proposed algorithm has the best performance; the lowest correlation and the highest entropy than the existing partial encryption methods. Hence better security has been provided.

6. REFERENCES

[1] Schneier B., 1996, “Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C”, John Wiley & Sons, Inc., USA.

[2] Borie J., Puech W., Dumas M., 2004, *“Crypto-Compression System for Secure Transfer of Medical Images”,* 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004).

[3] Prasanna SRM et al, 2006, “An image encryption method with magnitude and phase manipulation using carrier images”, IJCS 1(2):132–137

[4] H. Cheng and X. Li. 2000, “Partial Encryption of Compressed Images and Video”, IEEE Transactions on Signal Processing, 48(8), pp. 2439-2451.

[5] Howard Cheng and Xiaobo Li, 2002, “Partial Encryption of Compressed Images and Videos,” IEEE Transaction on Signal Processing, Vol. 48, No. 8, , pp. 2439- 2451.

[6] M. Podesser, H. P. Schmidt and A. Uhl. 2002, “Selective Bitplane Encryption for Secure Transmission of Image Data in MobileEnvironments”, 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7.

[7] W. Zeng and S. Lei, 2003, “Efficient Frequency Domain Selective Scrambling of Digital Video,” IEEE Transactions on Multimedia, Vol. 5, No. 1, pp. 118–129.

[8] Pfarrhofer, R., Uhl, A.2005, “Selective Image Encryption Using JBIG” In: Dittmann, J., Katzenbeisser, S., Uhl, A. (eds.) CMS 2005. LNCS, vol. 3677, pp. 98–107. Springer, Heidelberg.

[9] D. Engel and A. Uhl, 2006, “Lightweight JPEG2000 encryption with anisotropic wavelet packets,” in Proceedings of IEEE International Conference on Multimedia and Expo (ICME ‟06), pp. 2177–2180, Toronto, Canada.

[10] Nidhi S Kulkarni, Balasuramanian and Indra Gupta. 2008, “Selective encryption of multimedia images”, XXXII National Systems Conference, NSC 2008, December 17-19.

[11] Hammed A younis,Turki Y Abdalla and Abdulkareem Y Abdalla,2009, “Vector Quantization Techniques For Partial Encryption of Wavelet Compressed Digital Images” ,Iraq Journal Electrical and Electronic Engineering.

[12] Ju-Young Oh, Dong-Il Yang, Ki-Hwan Chon, 2010, “A Selective Encryption Algorithm Based on AES for Medical Information”, the Korean Society of Medical Informatics.

[13] Joshi, J.M., Dalal, U.D., 2011, “Selective Encryption using ISMA Cryp in Real Time Video Streaming of H.264/AVC for DVB-H Application”, World Academy of Science, Engineer- ing and Technology 79.

[14] Parameshachari B D and Dr. K M Soyjaudah, 2012, “A Study of Binary Image encryption using Partial Image Encryption Technique” International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, pp-955-959.

[15] Parameshachari B D and Dr. K M S Soyjaudah, 2013, “A New Approach to Partial Image Encryption” Proceedings of ICAdC, AISC 174, pp. 1005–1010, © Springer India 2013.

[16] Parameshachari B D, Panduranga H T and Dr. K M S Soyjaudah, 2012, “A Overview on Partial Image Encryption Approaches”, International Journal of Engineering Research and Development (IJERD), Volume 1, Issue 2, pp. 49-54.