International Journal of Information & Network Security (IJINS)
Vol.3, No.5, October 2014, pp. 308~315
ISSN: 2089-3299

Optimized Partial Image Encryption Using Pixel Position Manipulation Technique Based on Region of Interest

Parameshachari B D[1], Dr. K M Sunjiv Soyjaudah[2], Dr. Sumithra Devi K A[3]
[1]Department of ECE, K S Institute of Technology, Bangalore, Karnataka, India.
(Research Scholar, Dept. of Electronics Engineering, Jain University, Bangalore, Karnataka, India)
[2]Department of Electrical & Electronic Engineering, University of Mauritius, Reduit, Mauritius.
[3]Department of Master of Computer Applications, R V College of Engineering, Bangalore, Karnataka, India.

Article Info

Article history:

Received Jun 12th, 2014
Revised Aug 20th, 2014
Accepted Aug 26th, 2014

Keyword:

Region of interest,
Partial encryption,
Random key generator,
Exclusive-OR,
Partial decryption,

ABSTRACT

Today's, the most important locomotive to provide confidentiality is image encryption. In real-time applications the classical and modern ciphers are not appropriate because of vast quantity of data. However, certain applications like Pay-TV or Payable Internet Imaging Albums do not require entire part of an encryption, but requires a part of the image to be transparent to all users. Partial encryption is an approach to encode only the most essential portion of the data in order to afford a proportional confidentiality and to trim down the computational requirements and also execution time for encryption is reduced. In this paper, partial image encryption of color images using pixel position manipulation technique based on region of interest is proposed. It offers the amenities of partial encryption and rebuilds the images partially. Here input image is divided in to sub blocks, then selected blocks are encrypted using the proposed technique. The proposed technique promises the rapid security by encrypting the selected blocks of an image.

Corresponding Author:

Parameshachari B D,
Department of Electronics and Communication Engineering,
K S Institute of Technology, Bangalore, Karnataka, India,
E-mail: parameshbkit@gmail.com

1. INTRODUCTION

The product of the area of mathematics in information theory and the various ways of manage and manipulate information addresses area gives the data encryption. There are two fundamentals methods in Cryptography; one is, called plain data, converted to an unidentifiable data called cipher data. This process is also called encipher the data or encryption. The Second method is to convert cipher data back to the original plain data, this process is called to decipher, or decrypting the data. The encrypted data is allowed to access only an authorized person with known secret key. The fundamental concept of most data encryptions algorithms is secret key [1-5].

Multimedia data requires either full encryption or partial encryption depending on the application requirements. For example military and law enforcement applications require full encryption. Nevertheless, there is a large spectrum of applications that demands security on a lower level, as for example that ensured by partial encryption. Such approaches reduce the computational requirements in networks with diverse client device capabilities [6]. In this paper, the aim of partial encryption of an image is to encrypt only regions of interest (ROI) which are defined within particular areas of the image. The goal of partial encryption is to encrypt a well defined range of parameters or coefficients, as for example would be the higher spectrum of frequencies. Partial encryption can be used to process and transmit images acquired by a surveillance video-camera. Indeed, in order to envisage these images in real time, they must be rapidly transmitted and the full encryption is not really necessary. On the other hand partial encryption diminishes

the data size to be encrypted and accordingly requires lower computational time which is an important quality in wireless and portable multimedia systems.

The concept of region based partial image encryption finds use in time crucial applications wherein security is also anxiety such as, internet banking transactions, military image database and communication and medical imaging systems. Special and reliable security in transmission of digital images is desired in many applications, such as pay-TV, confidential video conferencing and corporate communications. Looking at the requirements of the hour and the existing techniques, the initiative of region based partial image encryption finds a major role in the field of image security. The remaining paper is arranged as follows. Section 2 describes the basics of partial image encryption and region of interest. Section 3 illustrates the proposed method. Section 4 monitors the results of the experiments and conclusion of this paper is described in section 5.

2. OVERVIEW OF PARTIAL IMAGE ENCRYPTION

Selective image encryption can be realized in the spatial domain by decomposing the image into bit-planes before compression.Consequently, encryption is achieved by encrypting a subset of the mostsignificant bit-planes [9-10].The significant bit-planes have higher adjacent correlations and carry more perceptual information proposed by Subba Rao et al.[11]. The majority of the selective encryption schemes encrypt a selected number of DC or AC coefficients for JPEG images, when the image is transformed into the frequency domain using discrete cosine transform [12-14].

The utilization of partial encryption has increased with the increase in prerequisite for conditional access of multimedia data. This paper proposes an partial encryption technique in which the coefficient value of only selected coefficients are changed, thus controlling the transparency of the multimedia data at the time of encryption. The coefficients to be encrypted are decided on the basis of a user defined criterion or region of interest, which acts as partial encryption technique. According to the partial encryption, is applied only to the selected part of the image, not the whole part of the image. Selected part of the image based on the region of interest area is directing to decrease the execution time for encryption. The implementation of partial image encryption suitable for the real time applications like image encryption for medical, image encryption for satellite among others. The main objective of partial encryption of a bit stream is to formulate the complete stream somehow inadequate for anybody that who cannot decrypt the ciphered subset. Figure 8.1shows the Selection of region of interest area.

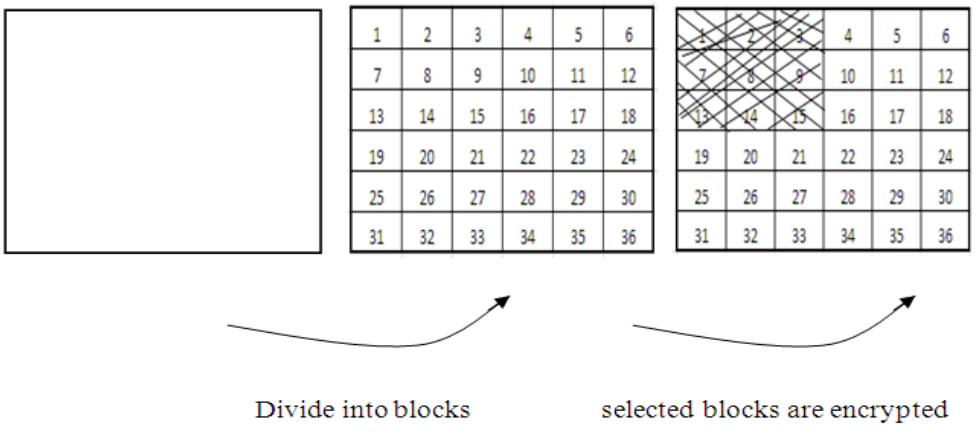

Figure 1: Block diagram for Selection of region of interest area

3. PROPOSED METHOD

This paper explains the concept of partial image encryption. Here input color image is divided in to sub blocks, then selected blocks are fed into the encryption block. Encrypt the selected blocks using XOR (Exclusive-OR) and mod (modulus after division) operator with a random key generator. Then combine the encrypted selected blocks and unselected blocks gives partially encrypted image.

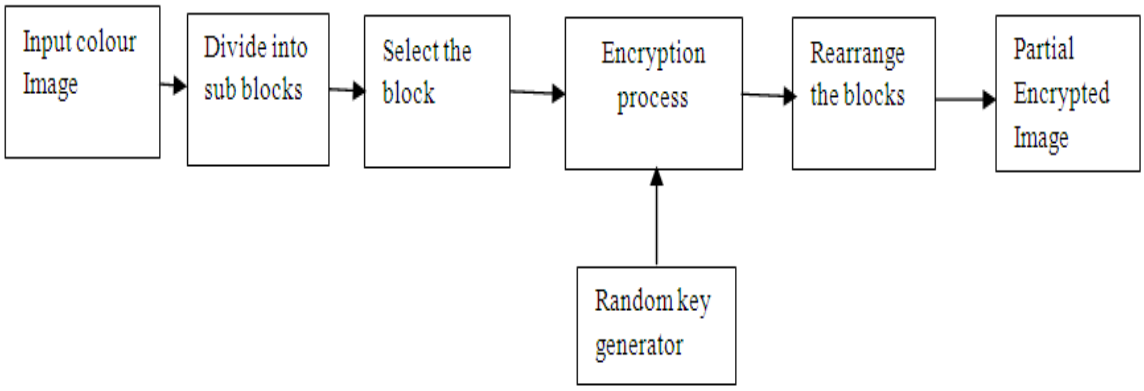

Figure 2: Block diagram of the proposed technique

4. EXPERIMENTAL RESULTS

The proposed system is implemented successfully using MATLAB R2010a and the following results are obtained. From the experimental results we can observe that sub block based partial image encryption is sufficient to secure the significant information in an image. The decryptied image is analogous to the input image demonstrate that the algorithm has also been successful in decrypting it suitably. To demonstrate that our proposed algorithm has strong resistance to statistical attacks, test is carried out on the histogram of enciphered image. Several color images are selected for this purpose and their histograms are compared with their corresponding ciphered image. Fig. 4, Fig. 6, Fig. 8, and Fig. 10, shows the histogram of the different color images. It is clear that the histogram of the encrypted image is appreciably different from the particular histogram of the original image and tolerate no statistical similarity to the plain image. Hence statistical attack on the proposed image encryption procedure is difficult.

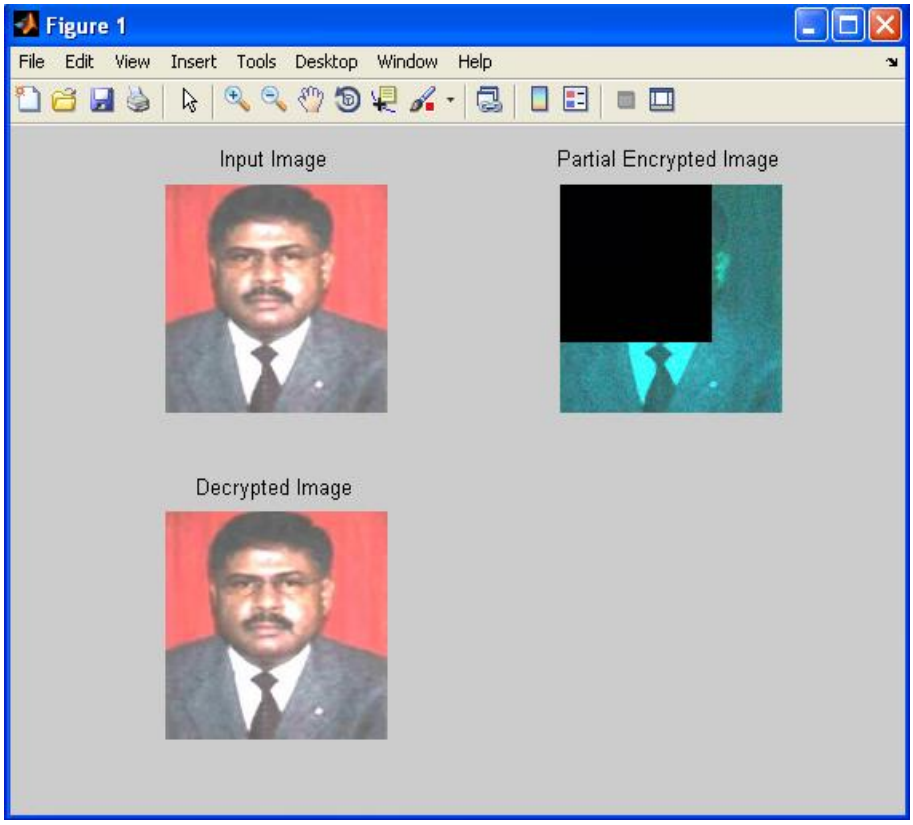

Figure 3: Partial encryption and decryption of the input color image

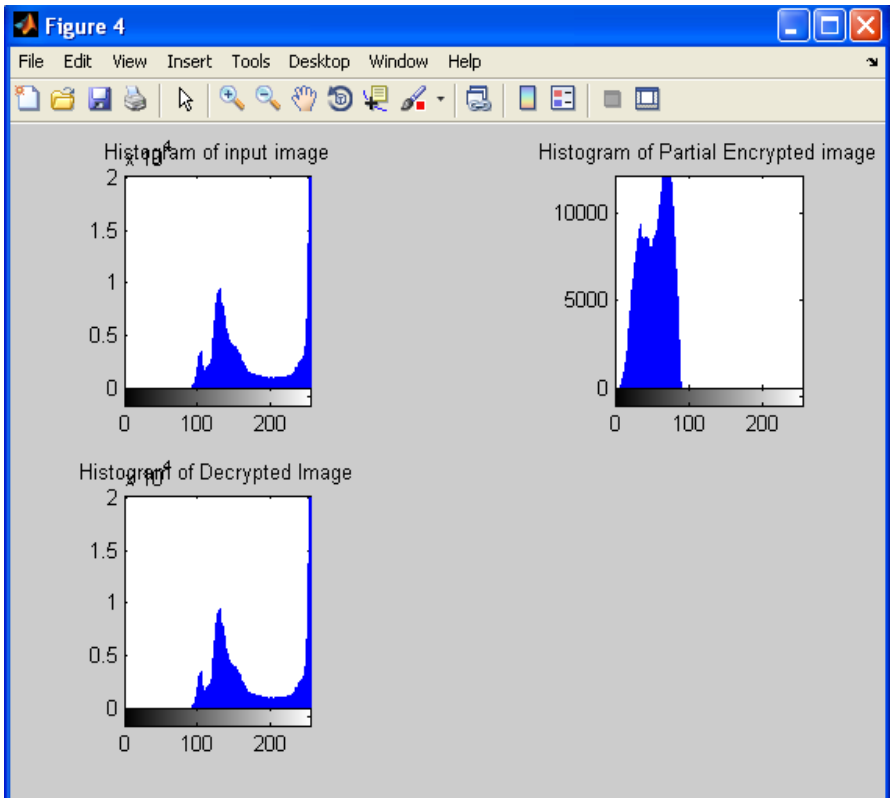

Figure 4: Histograms of Partial encryption and decryption of the input color image of figure 3

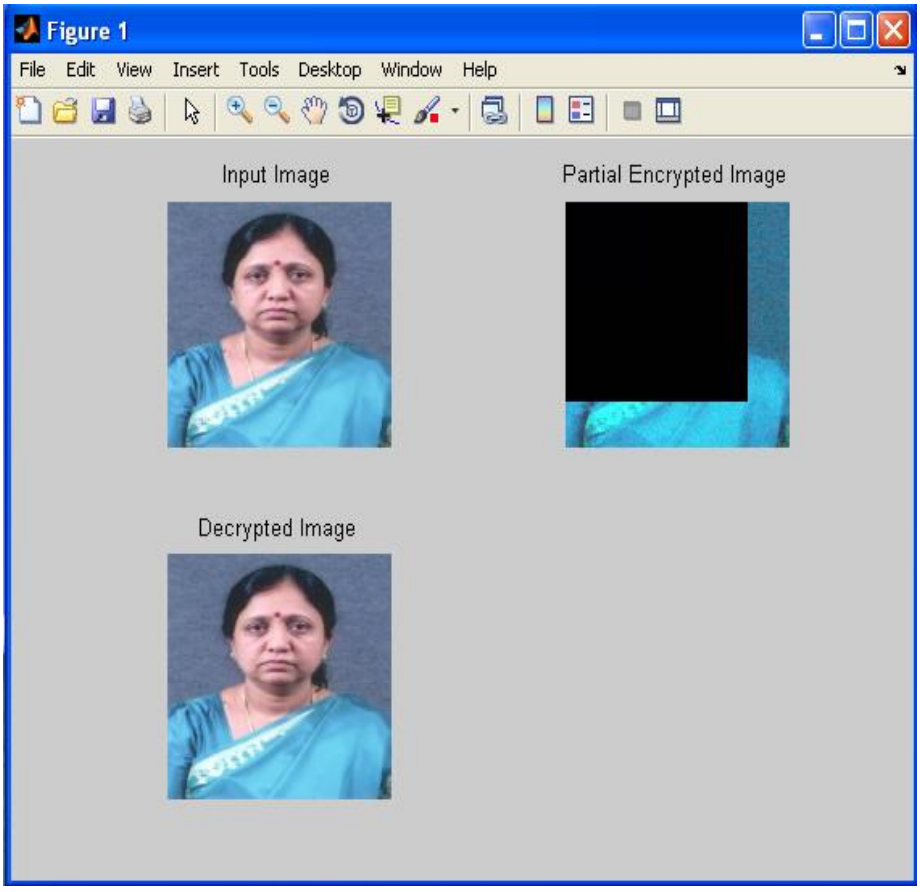

Figure 5: Partial encryption and decryption of the input color image

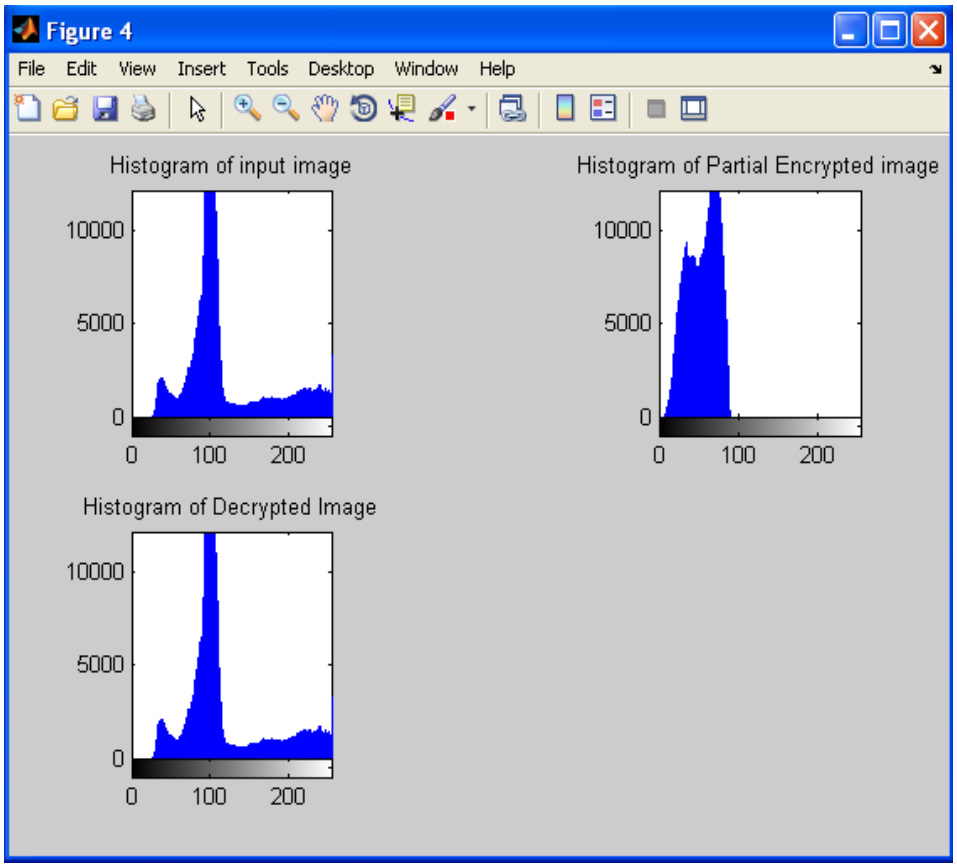

Figure 6: Histograms of Partial encryption and decryption of the input color image of figure 3

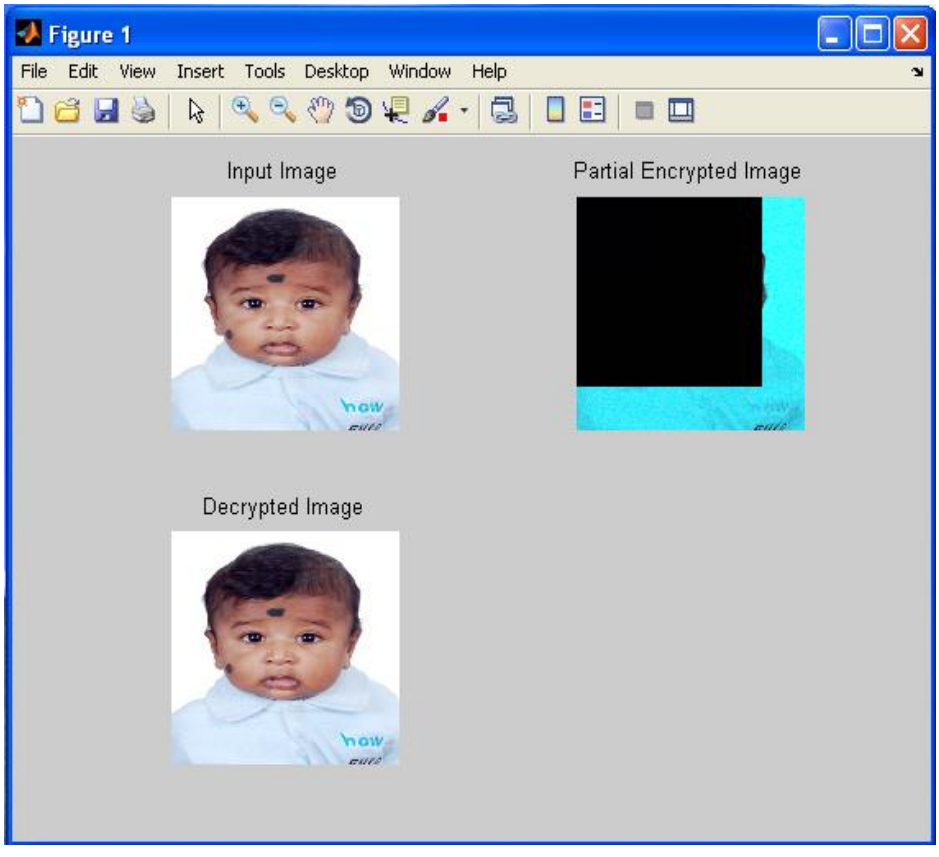

Figure 7: Partial encryption and decryption of the input color image

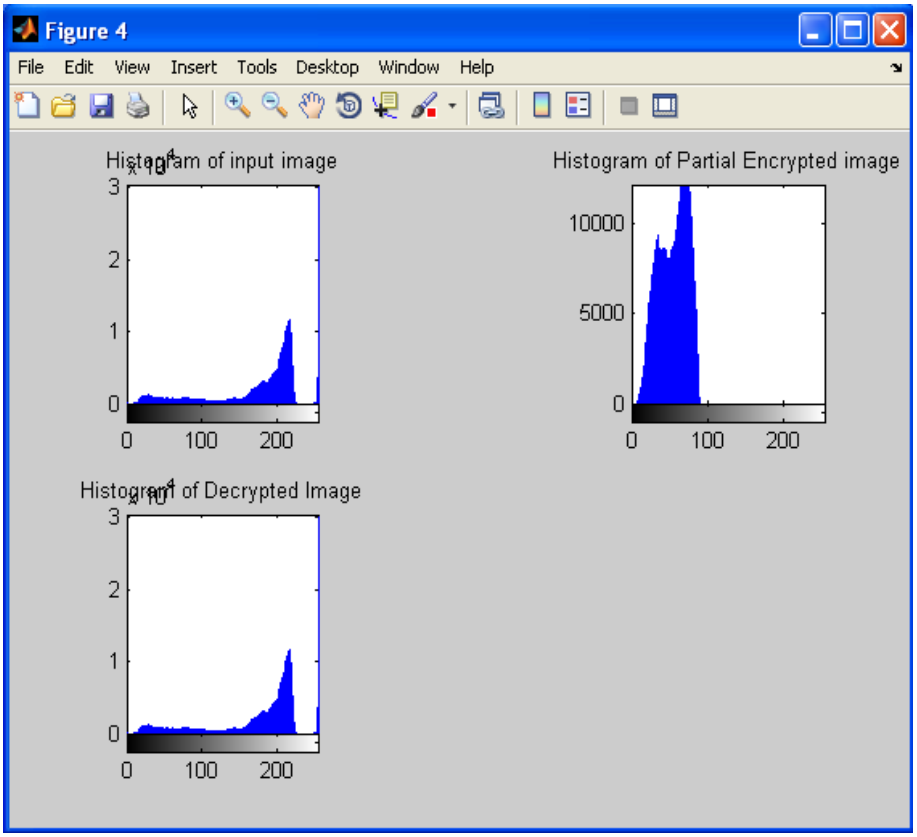

Figure 8: Histograms of Partial encryption and decryption of the input color image of figure 3

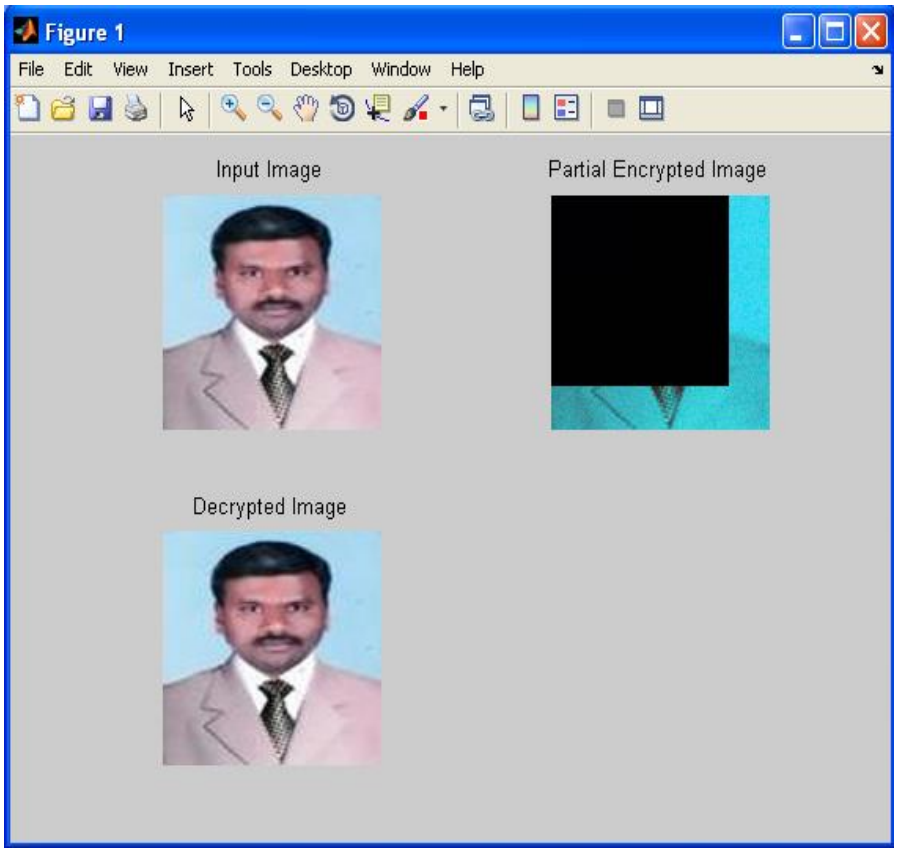

Figure 9: Partial encryption and decryption of the input color image

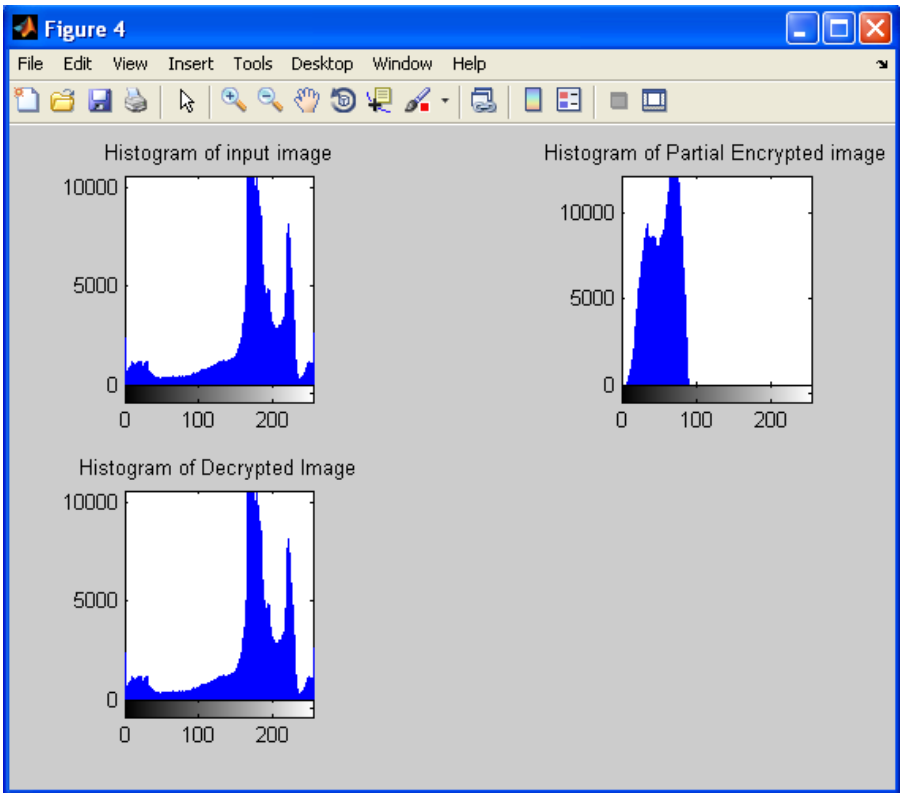

Figure 10: Histograms of Partial encryption and decryption of the input color image of figure 3

5. CONCLUSION

In this paper, proposed a simple but effective method of partial image encryption of color images using pixel position manipulation technique based on region of interest proposed. The aim of the overall study was to develop a partial image encryption processing system that was secure prior to entering the electronic communication system and to decrypt such an image after reception. All steps of partial encryption and decryption were simulated using MATLAB.The proposed partial encryption technique controls the transparency and security in a proficient conduct by encrypting the selected blocks of an image based on region of interest. Thus the experimental results show that the proposed techniques achieved quick security, flexibility, effectiveness and reliable.

REFERENCES

[1]. Petkovic, M., Jonker, W. Preface, "Special issue on secure data management," Journal of Computer Security, 17(1), pp.1-3 (2009)
[2]. Bernstein, D.J., Chen, T.R., Cheng, C.M., Lange, T. & Yang, B.Y. "ECM on graphics cards". In A. Joux (Ed.), Advances in Cryptology - Eurocrypt 2009 (28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings) Vol. 5479. Lecture Notes in Computer Science (pp. 483-501). Berlin: Springer (2009)
[3]. Bernstein, D.J., Lange, T., Peters, C.P. & Tilborg, H.C.A. van. "Explicit bounds for generic decoding algorithms for code-based cryptography". In International Workshop on Coding and Cryptography (WCC 2009, Ullensvang, Norway, May 10-15, 2009. Pre-proceedings) (pp. 168-180). Bergen: Selmer Center, University of Bergen (2009)
[4]. Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A.K., Molnar, D., Osvik, D.A. & Weger, B.M.M. de. "Short chosen-prefix collisions for MD5 and the creation of a 18 rogue CA certificate". In S. Halevi (Ed.), Advances in Cryptology - CRYPTO 2009 (29th Annual International Cryptology Conference, Santa Barbara CA, USA, August 16-20, 2009. Proceedings) Vol. 5677. Lecture Notes in Computer Science (pp. 55-69). Berlin: Springer (2009)
[5]. Kahate A., "CRYPTOGRAPHY AND NETWORK SECURITY", Tata-McGraw-Hill, 2nd edition (2008)
[6]. H. Cheng and X. Li. Partial Encryption of Compressed Images and Videos. IEEE Trans. On Signal Processing, 48(8):2439–2445, Aug. 2000.
[7]. Peng Chang and John Krumm, "Object Recognition with Color Co-occurrence Histograms", IEEE Conference on Computer Vision and Pattern Recognition, Fort Collins, CO, June 23-25, 1999.
[8]. Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing", second edition, Pearson Education, 2003.
[9]. Norcen, R., Podesser, M., Pommer, A., et al., 2003. Confidential storage and transmission of medical image data. Comput. Biol. Med., 33(3):277-292.

[10]. Podesser, M., Schmidt, H.P., Uhl, A., 2002. Selective bitplane encryption for secure transmission of image data in mobile environments. Proc. 5th Nordic Signal Processing Symp., p.1034-1037.
[11]. Subba Rao, Y.V., Mitra, A., Mahadeva Prasanna, S.R., 2006. A partial image encryption method with pseudo random sequences. LNCS, 4332:315-325.
[12]. Droogenbroeck, M.V., Benedett, R., 2002. Techniques for a selective encryption of uncompressed and compressed images. Proc. Advanced Concepts for Intelligent Vision Systems, p.90-97.
[13]. Stutz, T., Uhl, A., 2006. Transparent image encryption using progressive JPEG. LNCS, 4176:286-298.
[14]. Krikor, L., Baba, S., Arif, T., et al., 2009. Image encryption using DCT and stream cipher. Eur. J. Sci. Res., 32(1): 48-58.

BIBLIOGRAPHY OF AUTHORS

Parameshachari B D working as a Assistant Professor in the department of ECE at K. S. Institute of Technology, Bangalore. Worked as Associate Professor at NCERC, Kerala and Senior Lecturer at JSSATE, Mauritius. He is also Worked at KIT, Tiptur. He obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India. Parameshachari area of interest and research include image processing and cryptography. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

Professor K M Sunjiv Soyjaudah received his B. Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from King's College, University of London in 1991, and his Ph. D. degree in Digital Communications from University of Mauritius in 1998. He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes source and channel coding modulation, image processing, cryptography, voice and video through IP, as well as mobile communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius. Registered Ph.D Guide in University of Mauritius, Reduit, Mauritius and Jain University, Bangalore, Karnatka, India.

Dr. Sumithra Devi K A, Professor and Director, in Master of Computer Applications at R V College of Engineering, Bangalore, India. She received B.E. from Malnad College of Engineering, Hassan. She received M.E and Ph D from UVCE, Bangalore and Avinashilingam University for Women, Coimbatore, INDIA respectively. Reviewer for many International Journals / Conferences like WEPAN, WICT, EDAS, IACSIT, ISCAS, JEMS, Published 14 journals and 65 International/ National Conferences. Professional Member in many IEEE, IETE, CSI, ISTE. Member in BoS and BoE, for Visvesvaraiah Technological University, Belgaum, Karnataka. Registered PhD Guide in Visvesvaraiah Technological University, Belgaum; Jain University, Bangalore; Prist University, Sathyabhama University, Tamilnadu. Authored a chapter "CAD algorithm for VLSI design" in the book "VLSI Design ", published by In-Tech Publications, ISBN 979-953-307-512-8, 2011, and authored book on Operating System, published by Shroff Publisher India