Simple and Secure Image Encryption

V.V.Divya, S.K.Sudha and V.R.Resmy

[1] **Dept. of Computer science and Engineering, Sarabhai Institute of Science and Technology, Trivandrum, Kerala ,India**

[2] **Dept. of Computer science and Engineering, Sarabhai Institute of Science and Technology, Trivandrum, Kerala ,India**

[3] **Dept. of Computer science and Engineering, Sarabhai Institute of Science and Technology, Trivandrum, Kerala ,India**

Abstract

- Image Encryption is a wide area of research. Encryption basically deals with converting data or information from its original form to some other form that hides the information in it. The protection of image data from unauthorized access is important. Encryption is employed to increase the data security. The Encrypted Image is secure from any kind cryptanalysis.

In the proposed work, the image to be encrypted is decomposed into 8X8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT , Then, only selected DCT coefficients i.e the DCT coefficients correlated to the higher frequencies of the image block are encrypted. For encryption the DCT coefficients are xored with pseudorandom bit, Pseudorandom bit is generated by Non-Linear Shift back Register. The bits generated by Non-Linear Shift back Register cannot be predicted so cryptanalysis becomes difficult. To enhance the security further the unencrypted DCT coefficients are shuffled, since some information may also be stored in DCT coefficient correlating to lower frequency, While encrypting selected DCT coefficients alone will provide complete perceptual encryption, it would be possible for an attacker to gain information about the image from the other coefficients, especially in images that have a lot of edges.

Keywords – Encryption, Decryption, DCT

1. Introduction

Nowadays internet is used for faster transmission of large volume of important and valuable data, since internet has many points of attack, it is vulnerable to many kinds of attack, so this information need to be protected from unauthorized access, To protect data from unauthorized access there are many Data Protection techniques like NULL'ing Out, Masking Data, Watermarking, Encryption etc are implemented[1-2].

Data Encryption is one of the widely used techniques for data protection. In Data Encryption, data is converted from its original to other form so that information cannot be accessed from the data without decrypting the data i.e the reverse process of encryption. The original data is usually referred as plain data and the converted form is called cipher data. Encryption can be defined as the art of converting data into coded form which can be decode by intended receiver only who poses knowledge about the decryption of the ciphered data. Encryption can be applied to text, image, video for data protection. In the proposed work Encryption is employed to enhance image security. For encryption process the image is converted from spatial domain to frequency domain by using Discrete Cosine Transform (DCT). The DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies[3-7]. The objective of proposed system includes protection of information and property from theft, corruption while allowing the information to remain accessible and productive to its intended users. This includes the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The work is implemented with simplicity and security in mind.

2. Methodology

The methodology used in this work produce a simple and secure solution for image encryption and decryption. This technique is easy to implement and understand.
The following steps give a brief idea about the methodology involved in the entire work.

2.1 ALGORITHM FOR ENCRYPTION

1) Input image to be encrypted
2) Divide the image into 8x8 blocks.
3) Perform DCT on all this blocks and save the results in another array.
4) Encrypt the selected coefficient by XORing with a random bit generated by random bit generator.
5) Reconstruct the image.

2.2 ALGORITHM FOR DECRYPTION

1) Input encrypted image.
2) Encrypt the selected coefficient by XORing with a random bit generated by random bit generator.
3) Divide the image into 8x8 blocks.
4) Perform IDCT on all this blocks and save the results in another array
5) Decrypted Image is obtained.

3. RESULTS

The proposed system is implemented successfully and the following results are obtained

Experiment No : 1

Fig:3.1.1 a) Original Image

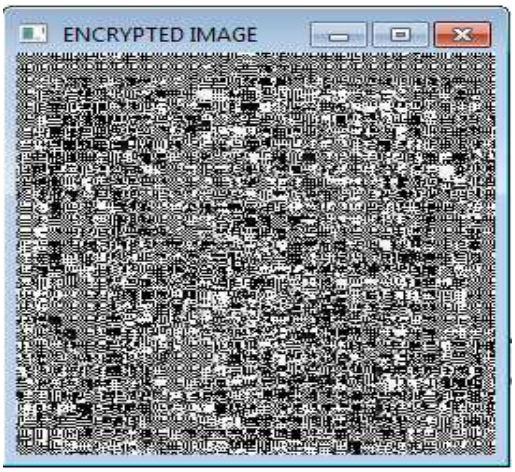

Fig: 1.1b)Encrypted Image

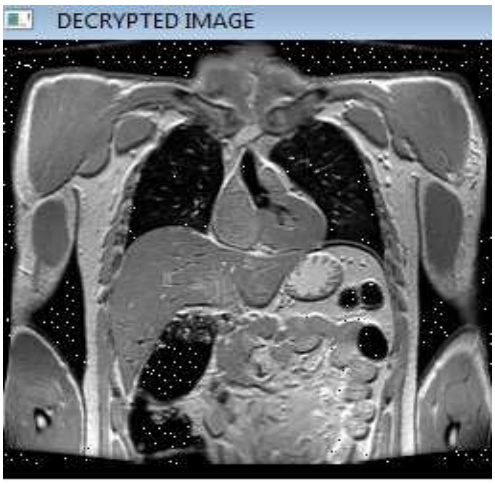

Fig:3.1.1c) Decrypted Image

Experiment No: 2

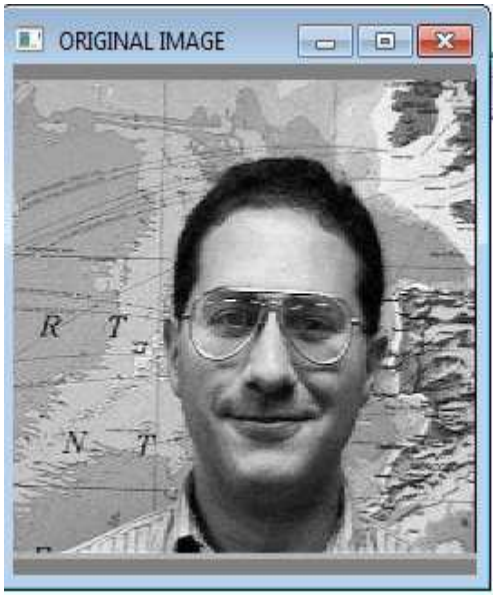

Fig:3.2.1 a) Original Image

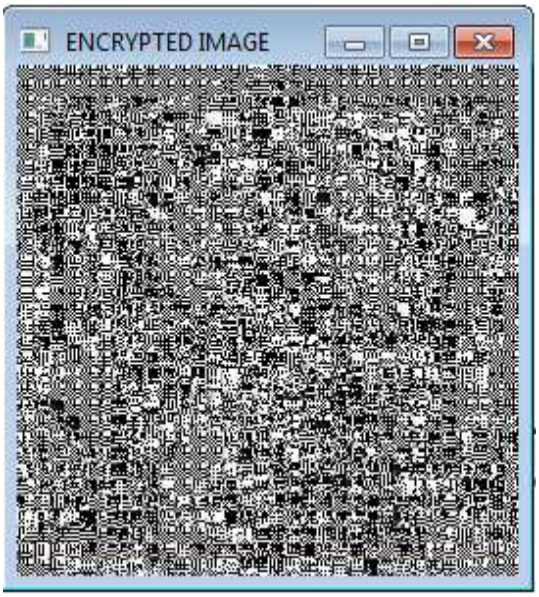

Fig:3.2.2b) Encrypted Image

Fig:3.1.2c) Decrypted Image

4. Conclusions

In this work a technique for faster image encryption is proposed. Here we are adopting partial image encryption to decrease the time required for encryption and decryption, Instead of encrypting the whole image only the selected portion of the image are encrypted, this makes the encryption faster and reduces the time complexity. Compression is not included in this method since compression requirement for each image is not unique. To add additional security to the image in the cryptosystem, after encrypting the selected higher coefficients, all the coefficients can be scrambled. The idea behind scrambling all the coefficients is to withstand any type of attack.

.

References

[1] Xiliang Liu, "Selective encryption of multimedia content in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.

[2] Marwa Abd El-Wahed,Saleh Mesbah and Amin shoukry "Efficiency and Security of some Image Encryption Algorithm".

[3] Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban Faculty of Information and Technology, Applied Science University "Image Encryption Using DCT and Stream Cipher."

[4] H. Cheng and X. Li. Partial Encryption of Compressed Images and Videos. IEEE Trans. On Signal Processing, 48(8):2439–2445, Aug. 2000.

[5] W. Puech and J. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT", *13th European Signal Processing Conference*, Turkey, September 2005.

[6] Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images", IEEE International Conference on Image Processing, 2006.

[7] Mahammad Ali Bani Younes and Aman Jantan, " Image encryption using Block-Based Tranformation Algorithm" IAENG International Journal of Computer science,35:1,IJCS_35_1_3

[8] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

[9] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli,

[10] Said E.EI-Khamy,Mohammad Abou EL-Nasr, Amina H. El-Zein "A partial Image Encryption Scheme Based on DWT and ELKNZ Chootic Stream Cipher", Member IEEE

[11] Jiang Delei ,Bai Sen and Dong Wenming, "An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter" Chongqing Communication Institute, Image Commuication Lab Chongqing, 400035,China.

[12] Han Shuihua, Yang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation" Department of Information System, School of Managemnet, Xiamen University

V.V.Divya received her B.Tech Degree in computer science and Engineering from Anna university , Chennai,India. She received her M.Tech Degree in computer and Information Science from M.S University, Thirunelveli, India. Currently she is working as Asst. Professor in Sarabhai Institute of Science and Technology, Trivandrum, India.

S.K.Sudha received her M.Tech Degree in Computer Science from Department of Computer Science, University of Kerala, India. Currently she is working as Asst. Professor in Sarabhai Institute of Science and Technology, Trivandrum, India.

V.R. Resmy received her M.Tech Degree in Computer Science from Department of Computer Science, University of Kerala, India. Currently she is working as Asst. Professor in Sarabhai Institute of Science and Technology, Trivandrum, India.