ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

Secure image transformation using Encryption and Compression techniques

A.Poorani, B.Manju,M.E.,

PG Scholar, Department Of Computer Science and Engineering, RVS Technical Campuscbe, Coimbatore
Assistant Professor, Department Of Computer Science and Engineering, RVS Technical Campuscbe, Coimbatore

ABSTRACT:A novel scheme of compressing encrypted images with auxiliary information is proposed. The content owner generates some auxiliary information and also encrypts the original uncompressed images that will be used for data compression and image reconstruction. After that, the channel provider who cannot access the original content may compress the encrypted data by a quantization scheme with optimal parameters that are derived from a part of auxiliary information and compression ratio-distortion criteria, and then transmit the compressed data that includes the quantized data, an encrypted sub-image, another part of auxiliary information and the quantization parameters.The principal image content may be rebuilt with the compressed encrypted data and the secret key at receiver side. In the proposed system, cryptography and Steganography methods is combined into one system for getting a better security and confidentiality.

KEYWORDS: compression ratio-distortion performance, Image encryption, image compression.

I. INTRODUCTION

Nowadays, the Security of digital multimedia such as image, text, video, and audio etc are transmitted over the networks has become very significant. These multimedia data transmitted over the network are terminated. Transmission channel is always bandwidth-constrained and insecure. Hence prior to the broadcast, it is desirable to compress and encrypt the data. The security to the data is provided using several cryptography and steganography techniques. Cryptography, it helps to encrypt the message. Here intruder can understand the encrypted message or information; however it is in an unintelligible form. Steganography, it helps to hide the existence of the information, thus it is not visible to a third party.

A. DIGITAL IMAGE PROCESSING

Digital Image Processing is has opened new research prospects in the field and one of the most important areas of Research. It refers to processing digital image by means of digital computers. Image Processing is a very thoughtful key that can change the outlook of many proposals and designs. Essential steps in Digital Image Processing and Image Enhancement, Image Acquisition, Color Image Processing, Compression, Image Restoration, Image Recognition and Segmentation.

In today's Scenario, Image Segmentation has become a very significant task. A significance of Segmentation is usually the first stage in any attempt of interpret or analyse an image repeatedly. Segmentation is a separating of a digital Image into set of pixels (multiple regions), due to some homogeneity principle. The problem of segmentation is a well-studied one in literature and also used for a wide variety of approaches. Different approaches are well-matched to different types of images and the quality of output of a particular algorithm. It is difficult to measure quantitatively owing to the fact that there may much correct segmentation for a single image.

Predictable approaches for sampling images or signals follow Shannon's theorem says that the sampling rate must be at least twice the maximum frequency present in the signal called as Nyquist rate. However the compression ratio is lesser. In this paper, the encryption and compression to the data is provided by compressive sensing.

B. COMPRESSIVE SENSING

Compressive sensing is a new evolving technology that helps to compress the data in a rate greater than the conventional method. In compressive sensing, encryption and compression is achieved by a single linear measurement step. This step is attained by using a measurement matrix that is generated by using a secret key. In between, the sender and receiver can shared the secret key.

II. RELATED WORK

A novel scheme of scalable coding is proposed in this paper for encrypted images[1]. The original pixel values are screened by a modulo-256 addition with non-random numbers which are derived from a secret key in the encryption phase. Later decomposing the encrypted data into a down sampled subimages and then several data sets with a multiple-resolution construction, also an encoder computes the Hadamard coefficients and the subimage of each data set to decrease the data quantity. Now, the data computes coefficients and subimage are observed as a set of bit streams. Since the hierarchical coding method, the principle unique content with greater resolution may be reconstructed once more bit streams are established.

Preserving confidential images are legal and an ethical requisite[2]. Information is stored by the computer system in the form of files. That File is considered as a basic entity for keeping the information. Consequently the problem of securing image information or data on computer system may be defined as the problem of securing data file. In today’s computing environment, it is worldwide accepted fact which securing file data is very significant. Goodencryption creates a source look completely traditional, random algorithms are incapable to compress encrypted data. Instead of this reason, all traditional systems make sure to compress before they encrypt. The concept of public key encryption is used for the encryption and decryption of images. In this public key’s of sender and receiver is known to encryption and decryption; however private key’s are kept secret. Neither the security nor the compression efficiency will be lost by performing compression in the encrypted area.

The strength of combining cryptography and steganography methods is focused to enhance the security of communication over an open channel or network [3]. By using the Singular Value Decomposition (SVD), andcompressive sensing method, the data to be sending are secured based on embedding scheme. The data is encrypted using the compressive measurements of the data and the resultant data is embedded in the protection object spending the SVD based load line embedding algorithm. Hence, this approach helps to send the secret data after hiding in a cover image. To encrypt and compress the data in a single step the compressive sensing method is used. This proposed system delivers more security to the compressed data and significantly reduces the attacks. It demonstrates that the proposed scheme is highly robust and efficient and also used to hide the secret images.

By using structurallyArnold transform and random matrices [4], a new digital image encryption method based on fast compressed sensing approach is proposed. Considering the natural images to be compressed in any field, the fast compressed sensing based approach increases the quality of the image, reduces the dimension of the digital image and saves computational time by choosing even 25 % of the measurements. Initial, dimension reduction is used to compress the digital image with scrambling result. Next, Arnold transformation is used to give the reduced digital image into more complex procedure. Formerly, the complex image is again encrypted by double random phase encoding process embedded with a host image; the two random keys with fractional Fourier transform are used as secret keys. The decryption process is recovered by using TwIST algorithm at the receiver. Thus proposed schemes demonstrated that the results to be fast, secure, robust and complex. This results including peak-to-peak, signal-to-noise ratio between the original and reconstructed image are displayed to examine the validity of this technique.

The existence of computer networks has encouraged new problems with privacy and security [5].The prompt growth of computer networks permitted large files such as digital images to be easily transmitted over the internet. In this paper, the objective of image compression is to decrease redundancy and triviality of the image data in order to be able to transmit or store data in an efficient procedure. A scheme for lossy compression of an encrypted image with stretchy compression ratio is proposed. A pseudorandom permutation is used to encrypt an original image and encrypted data are capably compressed by discarding the extremely fine information of coefficients generated from orthogonal transforms. Later receiving the compressed information with the assistance of spatial correlation in natural image, a receiver can reconstruct the principle content of the unique image by iteratively informing the values of coefficients. By this way, smoother the original image andhigher the compression ratio, the better quality of reconstructed image. Hence, this compression ratio typically affects the picture quality and also the tradeoff between picture quality and compression ratio is a vital one to consider once compressing images.

III. PROPOSED SYSTEM

By analyzing the existing techniques, the content owner encrypts the uncompressed plain signals for privacy protection. The task of compression can be left to a storage-device or channel provider who has limited obtainable resources but not the encryption key. In the proposed system, the content owner initially covers all pixel values in original uncompressed image to acquire an encrypted image and then provides the encrypted data to the channel supplier. If the bandwidth is sufficient, the channel supplier transfers the encrypted data.

The main scope of this paper project is to encrypt and then compress the image with sufficient auxiliary information or data. After the encryption and then compress process, the receiver side compressed image efficiently reconstructed with auxiliary information or data. The original content should not be modified at the time of reconstruction process. In this, it can also balance the bandwidth range in sender, channel provider and the receiver side by transmitting the “bandwidth sufficient” and “bandwidth insufficient “messages.

A. 2D Discrete Cosine Transforms:

A discrete cosine transform (DCT) states a finite sequence of data points in terms of a sum of cosine functions hesitating at different frequencies. DCTs are important to numerous applications in science and engineeringlossy compression of images(JPEG) and audio (MP3) wherever small high-frequency components can be rejected to spectral procedures for the numerical result of partial differential equations.

The basic operation of the DCT is as follows:

1.The input image is N by M;
2.F (i,j) -intensity of the pixel (row i, column j)
3.F (u, v) -DCT coefficient in row k1 and column k2 of the DCT matrix.

For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.Fig3.1. explainsthe is an 8 by 8 array of integers in DCT. This array contains each pixel's gray scale level and 8 bit pixels have levels from 0 to 255.

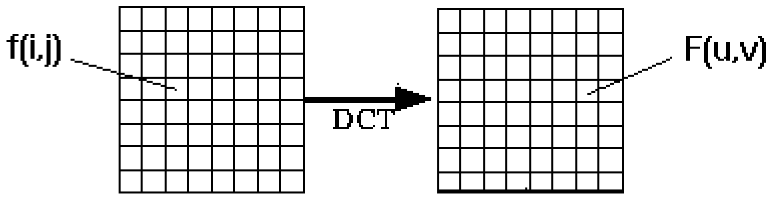

Fig3.1 2D Discrete Cosine Transforms

DCT Encoding

The general equation for a 1D (*N* data items) DCT is defined by,

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

and the corresponding ***inverse*** 1D DCT transform is simple $F^{-1}(u)$, i.e., where,

$$\Lambda(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for}\xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The general equation for a 2D (*N* by *M* image) DCT is defined by,

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

and the corresponding ***inverse*** 2D DCT transform is simple $F^{-1}(u,v)$, i.e.,where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

B. System Architecture

Architecture diagram explains the relationship between different components of an organization. Fig.3.1 explains the encryption and decryption process in 2D Transform.

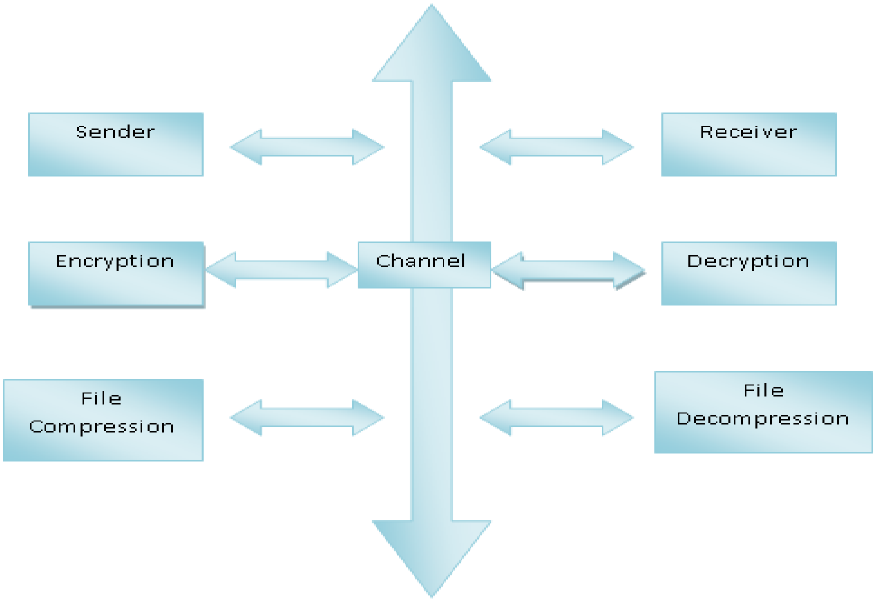

Fig 3.2System Architecture

IV. RESULT AND DISCUSSION

On the basis of the DCT scheme, conduct the test evaluation of this protocol. This mainly focused for improving the efficiency of the proposed protocol. In the below fig 4.1, the existing scheme is compared with proposed DCT scheme. Thus, the PSNR value of decrypt image is identified accurately.

Table 1.1 Comparisons between Existing scheme and Proposed scheme

Performance Metrics	**ExistingScheme**	**DCT Scheme**
Energy Efficiency	Average	Good
Throughput and performance	Poor	Improved

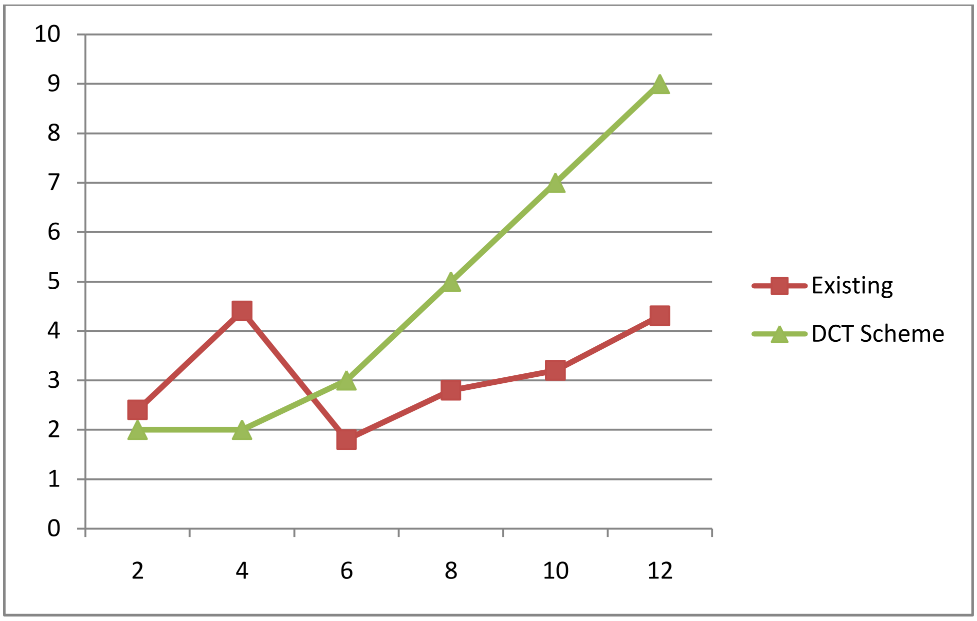

Fig.4.1. Comparison of Existing and Proposed Scheme

V. CONCLUSION

In this paper, a DCT is proposed for compressing encrypted images with auxiliary data. From this,attacker cannot reveal the original image content without secret key. DCT can have reconstructed image, these reconstructed image having the higher PSNR value. The proposed system considers the PSNR value of decrypt image and the attacker cannot get the original image at receiver side at the time of decryption. The proposed compression method is not suitable for other encryption approaches, such as AES or DES. Compared with previous approaches, the compression performance is consequently improved and also the computational complexity is significantly reduced. In future, the study of the ratio-distortioncompatibility and performance can be analysed with different encryption method.

REFERENCES

[1] S.V.V.D.Jagadeesh, 2T.Sudha Rani, “An Effective Approach Of Compressing Encrypted Images”, in Proceedings of the nternational Journal of Research in Computer and Communication Technology Advance Technology, 2007.

[2] P.S.Kishore, N.Ajay Nagendra, K.Pratap Reddy , V.V.S.Murthy, " Smoothing And Optimal Compression of Encrypted Gray Scale Images ", In Proceedings of the International Journal of Engineering Research and Applications , 2008.

[3] A.V. Sreedhanya and K.P. Soman, “Ensuring Security to the Compressed Sensing Data Using a Steganographic Approach,” in the proceedings of Bonfring International Journal of Advances in Image Processing, Vol. 3, No. 1, March 2013.

[4] Nitin Rawat, Pavel Ni, Rajesh Kumar, “A Fast Compressive Sensing Based Digital Image Encryption Technique using structurally Random Matrices and Arnold Transform”, pp.1-13 2013..

[5] Asha P. Ghodake, Sujata Mendgudle, “Security and Privacy of Image by Encryption, Lossy Compression and Iterative Reconstruction,”International Journal of Computer Applications 62(1):16-20 · January 2010.

[6] M. Johnson , P. Ishwar , V. M. Prabhakaran , D. Schonberg and K. Ramchandran, "On compressing encrypted data", IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, 2004

[7] Z. Erkin , A. Piva , S. Katzenbeisser , R. L. Lagendijk , J. Shokrollahi , G. Neven and M. Barni, "Protection and retrieval of encrypted multimedia content:When cryptography meets signal processing", EURASIPJ. Inf. Security, pp. 1-20, 2007

[8] N. S. Kulkarni , B. Raman and I. Gupta, "Multimedia encryption: A brief overview", Recent Adv. Multimedia Signal Process. Commun., vol. SCI 231, pp. 417-449, 2009

[9] G. Jakimoski and K. P. Subbalakshmi, "Security of compressing encryptedsources", Proc. 41st Asilomar Conf. Signals,Systems and Computers (ACSSC 2007), pp. 901-903, 2007.

[10] D. Schonberg , S. C. Draper and K. Ramchandran, "On blind compression of encryptedcorrelated data approaching the source entropy rate", Proc.43rd Annu. Allerton Conf., 2005

[11] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-levelandcolorimages",Proc. 16th Eur. Signal ProcessingConf. (EUSIPCO 2008), 2008.

[12] A. Kumar and A. Makur, "Distributed source coding based encryptionand lossless compression of gray scale and color images", Proc. IEEE 10th Workshop Multimedia Signal Processing, pp. 760-764, 2008.