ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

Scalable Compression of Encrypted Images

S.M.Ghorpade[1], K.R.Khandagle[2]

PG Student [Communication Engineering], Dept. of ECE, MIT Engineering College, Aurangabad, Maharashtra, India[1]

Assistant Professor, Dept. of ECE, MIT Engineering College, Aurangabad, Maharashtra, India[2]

ABSTRACT: The dissertation provides a novel scheme of scalable coding for encrypted images. In the encryption phase, the original image is encrypted by using chaos encryption method. After encryption image is given for compression to reduce the data amount. The compression is carried out by using Lifting Discrete Wavelet Transform (DWT). After this a reverse procedure is applied to get an original image back. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed.
The project presents data protection system for secret communication through common network based on encrypted color images under image frequency domain. Here, the system will be implemented for true RGB color image and the Blue plane will be chosen for hiding the secret text data. Then image is separated into number of blocks locally and lifting discrete wavelet transform (DWT) will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption method. The proposed encryption technique uses the key to encrypt an image and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. By using the decryption keys, the image will be extracted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image. The system performance proves with the image quality parameters such as root mean square error (MSE) and peak signal to Noise ratio (PSNR).

KEYWORDS: Image Encryption, Image Compression, Lifting Wavelet Transform, Blue Plane, PSNR, MSE.

I.INTRODUCTION

As the world has been totally digitized, along with digitalism, use of multimedia has also rapidly increased. But with sudden increase in use of multimedia has raised an important issue of securing the multimedia data as these data prone to being getting hacked or leaked due to its availability. As the multimedia data is transmitted over networks on large scale, we need to have a reliable technique to prevent data getting leaked or attacked. In today's connected world for sending and receiving the images the most important thing is security. In recent years, encrypted signal processing has attracted considerable research interests. Earlier the technique used for sending and receiving images was different but as the day passes new technology had invented and it has provided more security to the data.

Along with this increasing use of digital images comes the serious issue of storing and transferring the huge volume of data. For this compression techniques are used. Image encryption and Image compression plays an important role between sender and receiver. The goal of image encryption is that the attacker or hacker or intruder should not obtain the statistical information. Various Cryptographic techniques are developed to secure the data between transmission and reception. The images have to be encrypted before compression to give high level security. We design a highly efficient image encryption –the-compression system using lossless and lossy compression. The frequency domain and adaptive filtering can be engaged in the encrypted area based on the homomorphic properties of cryptography and a complex signal representation method can be used to decrease the size of encrypted information and computation difficulty

The compatibility of image depends on two factors i.e. PSNR and MSE. This both terms are inversely proportional to each other. If PSNR is 100% then the compression is known as lossless as the image can be reconstructed exactly. If any values are changes then PSNR will be lost and is known as lossy compression. For this we use wavelet transform and Lossless Compression. The most important feature of wavelet transform is it allows multi resolution decomposition. An image that is decomposed by wavelet transform can be reconstructed with desired resolution. The

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

procedure for this is a low pass filter and a high pass filter is chosen, such that they exactly halve the frequency range between themselves. This filter pair is called the Analysis Filter pair. First of all, the low pass filter is applied for each row of data, and then we obtain low frequency components of the row. As the LPF is a low pass filter, the output data consists of frequencies only in the first half of the original frequency range.

So in order to help people we had developed an interactive system that will help in reconstruction of image with the help of MATLAB. The proposed system will be useful in day to day life. As mentioned in the applications this project is a real time application for all real time places.

II.LITERATURE SURVEY

- **High Performance Scalable Image Compression with EBCOT**

A new image compression algorithm is proposed, based on independent Embedded Block Coding with Optimized Truncation of the embedded bit-streams (EBCOT). The algorithm exhibits state-of-the-art compression performance while producing a bit-stream with a rich feature set, including resolution and SNR scalability together with a random access property. The algorithm has modest complexity and is extremely well suited to applications involving remote browsing of large compressed images. The algorithm lends itself to explicit optimization with respect to MSE as well as more realistic psycho visual metrics, capable of modelling the spatially varying visual masking phenomenon.

- **Scalable Image Coding Using Reversible Integer Wavelet Transforms**

Reversible integer wavelet transforms allow both lossless and lossy decoding using a single bit stream. We present a new fully scalable image coder and investigate the lossless and lossy performance of these transforms in the proposed coder. The lossless compression performance of the presented method is comparable to JPEG-LS. The lossy performance is quite competitive with other efficient lossy compression methods.

- **Lossless Compression of Encrypted Grey-Level and Color Images**

The feasibility of lossless compression of encrypted images has been recently demonstrated by relying on the analogy with source coding with side information at the decoder. However previous works only addressed the compression of bit level images, namely sparse black and white images, with asymmetric probabilities of black and white pixels. In this paper we investigate the possibility of compressing encrypted grey level and colour images, by decomposing them into bit-planes. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed, as well as the possibility of exploiting the correlation between colour bands. Some experimental results are shown to evaluate the gap between the proposed solutions and the theoretically achievable performance.

- **On Blind Compression of Encrypted Correlated Data Approaching the Source Entropy Rate**

Traditional data transmission over an insecure noiseless channel consists of first compressing data for efficiency and then encrypting it for security. Reversing the order of these operations is considered in Johnson et al. In this paper we build on this work by considering systems that must operate without knowledge of the underlying source statistics, and sources with memory (in particular two-state hidden Markov processes). We present and analyse an in-credential scheme based on exponentially increasing block lengths that is designed to balance the resolution rate of parameter estimation with the redundancy rate of communication. We show that the redundancy at best declines proportional to the inverse of the square root of the block length. We implement these ideas using low-density parity check (LDPC) codes. In an average practical test, to transmit a binary source of 100; 000 bits, ideally compressible to 17; 912 bits with perfect knowledge and an ideal code, required only 26; 787 bits. In comparison, to transmit this source with full knowledge of the source statistics required 21; 704 bits.

- **On Compressing Encrypted Data**

When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. Although counter-intuitive, we show surprisingly that, through the use of coding with side information principles, this reversal of order is indeed possible in some settings of interest without loss of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

either optimal coding efficiency or perfect secrecy. We show that in certain scenarios our scheme requires no more randomness in the encryption key than the conventional system where compression precedes encryption. In addition to proving the theoretical feasibility of this reversal of operations, we also describe a system which implements compression of encrypted data.

- **Fingerprinting Protocol for Images Based on Additive Homomorphic Property**

Homomorphic property of public-key cryptosystems is applied for several cryptographic protocols, such as electronic cash, voting system, bidding protocols, etc. Several fingerprinting protocols also exploit the property to achieve an asymmetric system. However, their enciphering rate is extremely low and the implementation of watermarking technique is difficult. In this paper, we propose a new fingerprinting protocol applying additive homomorphic property of Okamoto–Uchiyama encryption scheme. Exploiting the property ingenuously, the enciphering rate of our fingerprinting scheme can be close to the corresponding cryptosystem. We study the problem of implementation of watermarking technique and propose a successful method to embed encrypted information without knowing the plain value. The security can also be protected for both a buyer and a merchant in our scheme.

III.SYSTEM MODEL AND ASSUMPTIONS

It consists of main two phase Encryption and compression phase. The general concept of our project is first we take i/p RGB image after that we separate only blue plane of that image. After that we do encryption process on that image. Some coding is applied which is known as encoding process. After that image is compressed this is known as Encryption then compression technique. For encryption we use Chaos Encryption method. For compression technique Lifting wavelet transform is used. After completing all this process we get reconstructed image which is highly secure. And we can measure the efficiency on the basis of two factors PSNR and MSE. These two terms are related to each other. The value of MSE must be low to get the better output.

IV.PROPOSED SCHEME

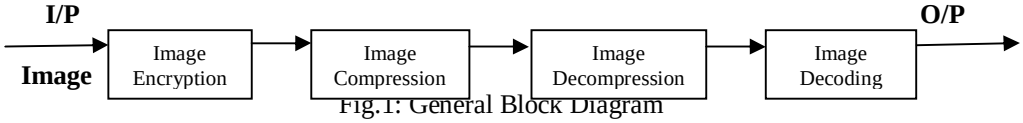

Fig.1: General Block Diagram

General block diagram of the system is shown above.

1. Take I/P image: Take the i/p RGB image in any image format and separate only blue plane of that image.
2. Image Encryption: In the below diagram plain image is referred as a normal image. Then it undergoes an encryption process. Encryption is done with Chaos Encryption method and the plain image is converted into cipher image. Cipher image means in some proper code which only intended people can read it. Encryption is the process of encoding message or information in such a way only authorized persons can see it. Encryption is the most effective way to achieve data security.

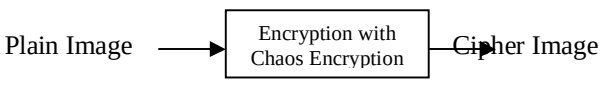

Fig.2: Encryption Phase

3. Image Compression: Wavelet transform is used to compress an image. Here, by using lifting wavelet transform the redundancies of an image are removed and the size of image gets reduced.

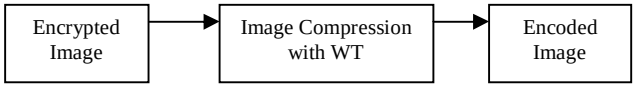

Fig.3: Encoded Phase

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

4. Image Decompression: It is totally opposite to compression. For decompression of a compressed image inverse lifting wavelet transform is used. At output we get a decompressed encrypted image which was given at input

Fig.4: Decompression Phase

5. Image Decryption: The same chaos encryption method based on logistic map which is used for encryption phase is also used for decryption phase. Same chaotic sequence is used for decryption. At the end we get the image given at input.

Fig.5: Decryption Phase

6. Reconstructed output Image: In this section the output image is obtained by combining reconstructed blue plane with red plane and green plane of input image. This is highly secured and same as that of original input image.

V.SECURITY

When we use any system the more important issue is security. In our project the main concentration is given to security. The image we get after reconstruction is highly secured.

VI.PERFORMANCE ANALYSIS

Performance analysis depends on two factors:

1. PSNR(Peak Signal To Noise Ratio):

2. MSE(Mean Square Error):

1. PSNR: PSNR represents a measure of the peak error. To calculate the PSNR value the block first calculates the mean squared error using the following equation.

   PSNR=$10log_2\left(\frac{R^2}{MSE}\right)$

   R is the maximum fluctuation in the input image data type. For example, if the input image has a double precision floating point data type, then *R* is 1. If it has an 8bit unsigned integer data type, *R* is 255, etc.

2. MSE: The MSE represents the cumulative squared error between the compressed and the original image. The lower the value of MSE, lower the error.

   $\mathrm{MSE} = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N}$

M and *N* are the number of rows and columns in the input images, respectively.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

VII. RESULT AND DISCUSSION

In the fig 1, it shows the pop window when we do the encryption and decryption process:

Fig.6: Image Encryption output GUI

The functions of the buttons in figure 6 are as follows:

1. Load Image: In this we take the RGB image of any format.
2. Encryption: If we click on this button encryption process gets started.
3. Image Encoding: If we click on this button the process of compression gets started.
4. Image Decoding: If we click on this button the process of decompression gets started.
5. Reconstruction: If we click on this button we get back the original image which is known as Reconstructed Image.
6. Close: After we get back the original image it gets closed.

On the basis of above two factor we have taken some images into input side and get the reconstructed image and also calculated the PSNR value and MSE value. Results are shown below in fig 7:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 2, February 2016

Input Image	Output Image	PSNR Value	MSE Value
		**32.34 dB**	**9.52**
		**42.27 dB**	**3.85**

Fig.7. Snapshot of input and output Images

VIII. CONCLUSION

We have tried to obtain clearer image with high resolution. Firstly the image is encrypted then compressed. For encryption purpose chaos encryption method and compression purpose lifting wavelet transform is used. In order to achieve the final goal first we have generalized the image encryption schemes related to scalable coding, i.e. wavelet based algorithms. After receiving the image we have calculated the PSNR and MSE value. PSNR and MSE are inversely related to each other. If PSNR is low MSE will be high and vice-versa. There are two types of Compression techniques namely loseless and lossy compression. If the value of PSNR is 100% then the compression is known as losseless as the image can be reconstructed exactly. If any values are changes then it is known as lossy compression.

REFERENCES

1. 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," EURASIP J. Inf. Security, vol. 2007, pp. 1–20, Jan. 2007.
2. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
3. J. R. Troncoso-Pastoriza and F. Pérez-González, "Secure adaptive filtering," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 469–485, Jun. 2011.
4. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.
5. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
6. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Process.Image Commun., vol. 26, no. 1, pp. 1–12, Jan. 2011.