Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.585 – 590

RESEARCH ARTICLE

Implementation of Encrypted Image Compression Using Resolution Progressive Compression Scheme

M. Arunkumar, S. Prabu

Associate Professor, Department of Information and Technology, PSNA College of Engg and Technology, Dindigul, Tamil Nadu, India

Professor, School of Computing Science and Engineering, VIT University, Vellore, India

kmarun_vicky@yahoo.co.in

Abstract— When it is desired to transmit redundant data over an insecure channel, it is customary to encrypt the data. Here the image data is first encrypted and then it undergoes compression in resolution. Here the decoder gets only lower resolution version of the image. The source dependency is exploited to improve the compression efficiency.

Index Terms— Advanced Encryption Standard, Encrypted images, Image Processing, Markov Decoding

I. INTRODUCTION

Image processing is any form of information processing, in which the input is an image. Image processing studies how to transform, store, retrieval the image. Digital Image Processing is the use of computer algorithms to perform image processing on digital images.

Many of the techniques of image processing were developed with application to satellite imagery, medical imaging, object recognition, and photo enhancement. With the fast computers and signal processors available in the 2000s, digital image processing has become the most common form of image processing, and is generally used because it is not only the most versatile method, but also the cheapest.

An image can be defined as a two-dimensional function f(x, y) (2-D image), where x and y are spatial coordinates, and the amplitude of f at any pair of (x, y) is gray level of the image at that point. For example a gray level image can be represented as: f_{ij} where $f_{ij}= f(x, y)$ When x, y and the amplitude value of f are finite, discrete quantities, the image is called a "digital image". The finite set of digital values is called picture elements or pixels. Typically, the pixels are stored in computer memory as a two-dimensional array or matrix of real number.

Color images are formed by a combination of individual 2-D images. Many of the image processing techniques for monochrome images can be extend to color image (3-D) by processing the three components image individually.

Digital image processing refers to processing a digital image by mean of a digital computer, and the study of algorithms for their transformation. Since the data of digital image is in the matrix form, the DIP can utilize a number of mathematical techniques. The essential subject areas are computational linear algebra, integral transforms, statistics and other techniques of numerical analysis. Many DIP algorithms can be written in term of matrix equation, hence, computational method in linear algebra become an important aspect of the subject.

Digital image processing encompasses a wide and varied field of application, such as area of image operation and compression, computer vision, and image analysis (also called image understanding). There is the consideration of three types of computerized processing: low-level processing is characterized by that both its inputs and outputs are images; mid-level processing on images is characterized by the fact that its input are images, but outputs are attributes extracted from those images, while higher-level processing involves "making sense" of an ensemble of recognized objects as in image analysis, and performing the cognitive function associated with human vision. In particular digital image processing is the practical technology for area of: Image compression, Classification, Feature extraction, Pattern recognition, Projection, Multi-scale signal analysis.

II. COMPRESSION OF ENCRYPTED IMAGES

Security in communication systems has become increasingly important in recent times. The Internet has become a hostile environment with both wired and wireless channels offering no inherent assurance of confidentiality. Strong encryption schemes, such as the Advanced Encryption Standard (AES), have been designed to provide confidentiality for arbitrary binary data. However, communications have become increasingly multimedia in nature and such strong encryption schemes do not take into account the special characteristics of multimedia data and the way in which they are accessed. Images and video are typically large in size compared to text and audio, and often already consume significant computational resources at both the source and receiver for coding and decoding, respectively. Also, applications such as remote surveillance may involve the streaming of sensitive visual image data over untrusted networks. Confidentiality may be required, but blindly applying a strong encryption scheme such as AES would demand a prohibitive amount of computational resources for the large volume of real-time data. Other applications, such as online collaboration, may involve the use of power limited mobile devices, such as mobile phones and personal digital assistants (PDAs) with embedded imaging capabilities, forming ad-hoc wireless networks. Most of the computational resources of the devices are dedicated to the coding and decoding of the visual data, making the application of schemes such as AES exceedingly difficult or impossible.

For secure transmission of data through the communication channel, the data is usually first compressed and then encrypted at the source and at the destination the data is received and is decrypted followed by decompression [1]. This is illustrated in the figure 1.

But this traditional method is not suitable for some applications. For example if John want to send information to Ken, while Ben is the network provider. John wants to keep the information confidential to Ben. In this situation, John encrypts the data using a simple cipher and gets its forwarded. Thus Ben can compress the data without accessing the secret key. If Ken holds the secret key used by John, then he will be able perform joint decryption and decompression. Thus the overall performance of the system can be increased by doing this. This is illustrated in the figure 2.

The rest of the paper is organized as follows. Section III gives about the related work in this area. Section IV gives a detailed explanation of the proposed system. Section V concludes and discusses about the future work.

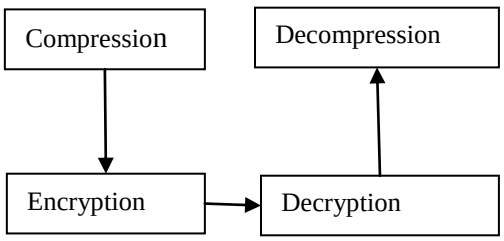

Fig. 1. Conventional approach for secure data transmission.

III. RELATED WORK

In the existing system, Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding [3]. For encrypted real-world sources, such as images, the key to improve the compression efficiency is how the source dependency is exploited. Trellis Coded Vector Quantization [3] can also be used for compressing the encrypted image sources. It has been reported that good results are produced for the binary images. But still challenges remain when it comes practical in real world

applications. The coding efficiency can be improved only by exploiting the source dependency. Both these two techniques have the following disadvantages.

- Markov decoding in a Slepian-Wolf coding is expensive with computational complexity.
- The source dependency is not fully utilized.
- Since image and video are highly nonstationary, the Markov model cannot describe its local statistics precisely.
- For 8-bit gray scale images, only two most significant bit-planes are compressible by employing a 2-D Markov model in bit planes [10].

A. Encryption

Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

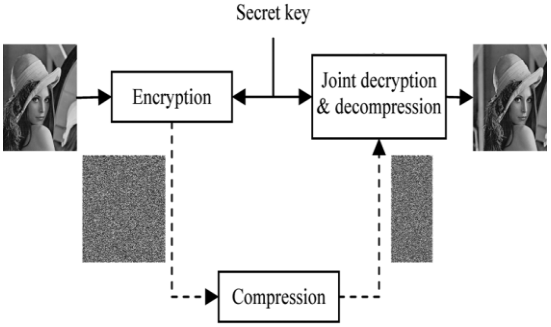

Fig. 2. Secure transmission using compression of encrypted data.

Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption.

B. Image Compression

Data Compression is one of the technologies for each of the aspect of this multimedia revolution. Cellular phones would not be able to provide communication with increasing clarity without data compression. Data compression is art and science of representing information in compact form. Uncompressed multimedia (graphics, audio and video) data requires considerable storage capacity and transmission bandwidth. Despite rapid progress in mass-storage density, processor speeds, and digital communication system performance, demand for data storage capacity and data-transmission bandwidth continues to outstrip the capabilities of available technologies. In a distributed environment large image files remain a major bottleneck within systems. Image Compression is an important component of the solutions available for creating image file sizes of manageable and transmittable dimensions. Platform portability and performance are important in the selection of the compression/decompression technique to be employed.

Image compression has become increasingly important with the continuous development of Internet, remote sensing and satellite communication techniques. Due to the high cost of providing a large transmission bandwidth and a huge amount of storage space, many fast and efficient image compression engines have been introduced.

In image processing applications such as web browsing, photography, image editing and printing, a lossy coding such as JPEG is sufficient as an image compression tool. Although some information loss can be tolerated in most of these applications, there are certain images processing applications that demand no pixel difference between the original and the reconstructed image. Such applications include medical imaging, remote sensing, satellite imaging and forensic analysis where a lossless compression is extremely important.

IV. PROPOSED WORK

In the proposed system, in order to achieve efficient compression of encrypted images, a Resolution Progressive Compression scheme is used. Here the encryption is performed using RSA algorithm. Here it compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. The success of RPC scheme is due to enabling partial access to the current source at the decoder side to improve the decoder's learning of the source statistics.

The encoder gets the ciphertext and decomposes it into four subimages, namely, the 00, 01, 10, and 11 sub-images. Each sub-image is a downsampled-by-two version of the encrypted image. When the decomposition image is obtained, we try

to find a way how to code the wavelet coefficients into an efficient result, taking redundancy and storage space into consideration.

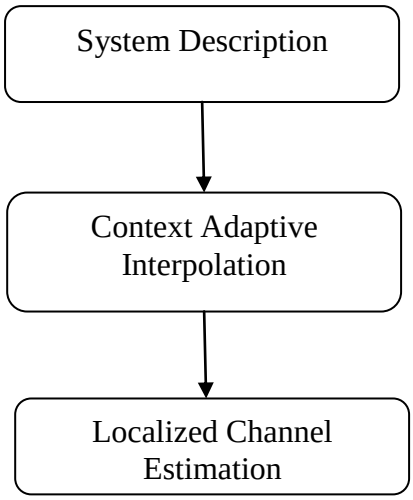

Fig. 3. Block Diagram of RPC Scheme.

SPIHT is one of the most advanced schemes available, even outperforming the state-of-the-art JPEG 2000 in some situations. The basic principle is the same; a progressive coding is applied, processing the image respectively to a lowering threshold. The difference is in the concept of zerotrees (spatial orientation trees in SPIHT). This is an idea that takes bounds between coefficients across subbands in different levels into consideration. The first idea is always the same: if there is a coefficient in the highest level of transform in a particular subband considered insignificant against a particular threshold, it is very probable that its descendants in lower levels will be insignificant too, so we can code quite a large group of coefficients with one symbol. In the SPIHT algorithm, each 2x2 block of coefficients in the root level corresponds to three trees of coefficients, as shown in Fig. 4. The coefficient at (i, j) is denoted as $C_{i,j}$.

The following sets of coefficients are defined.

•O(i,j) is the set of coordinates of the children of the coefficient at (i,j) .

•D(i,j)is the set of coordinates of all descendants of the coefficient at (i,j).

•H is the set of coordinates of all coefficients in the root level.

. L(i,j)= D(i,j)- O(i,j)

Given a threshold $T= 2^n$, a set of coefficients S is significant if there is a coefficient in S whose magnitude is at least T.

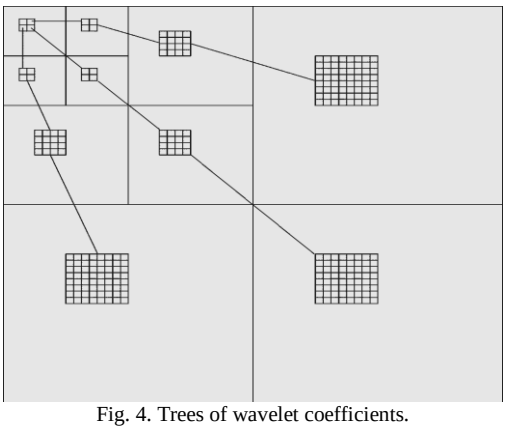

Fig. 4. Trees of wavelet coefficients.

We define the function

$$S_n(S) = \begin{cases} 1 \text{ if is significant with respect to } T = 2^n \\ 0, \text{otherwise} \end{cases}$$

Three lists are maintained by the algorithm:
1) list of insignificant sets (LIS);
2) list of insignificant pixels (LIP);
3) list of significant pixels (LSP).

The LIS contains two types of entries, representing the sets D(i,j) and L(i,j). The LIP is a list of insignificant coefficients that do not belong to any of the sets in the LIS. The LSP is a list of coefficients that have been identified as significant. The SPIHT algorithm encodes the wavelet coefficients by selecting a threshold such that $T \leq \max_{(i,j)} |Cij,| < 2T$, where (i,j) ranges over all coordinates in the coefficient matrix. Initially, the LIP contains the coefficients in H, the LIS contains D(i,j) entries, where (i,j) are coordinates with descendants in H , and LSP is empty. During the sorting pass, the significant coefficients in the LIS are identified by partitioning the sets D(i,j)into L(i,j) and the individual coefficients in O(i,j) or L(i,j) into D(k,l),where $(k,l) \varepsilon O(i,j)$.

During the refinement pass, all coefficients in LSP that have been identified as significant in previous passes are then refined in a way similar to binary search.ach significant coefficient is moved to the LSP. The threshold is decreased by a factor of two, and the above steps are repeated. The encoding process stops when the desired bit rate is reached. The output is fully embedded so that the output at a higher bit rate contains the output at all lower bit rates embedded at the beginning of the data stream.

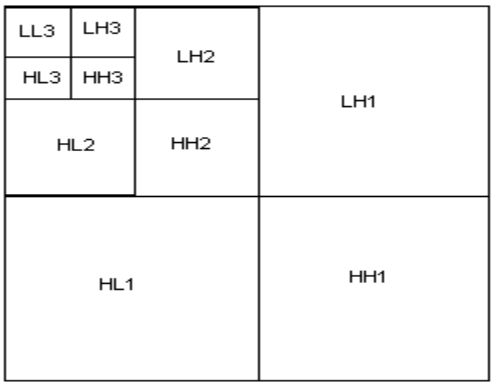

Fig. 5. Layout of three-level decomposition of the unencrypted image.

The algorithm has several advantages. The first one is an intensive progressive capability we can interrupt the decoding (or coding) at any time and a result of maximum possible detail can be reconstructed with one-bit precision. This is very desirable when transmitting files over the internet, since users with slower connection speeds can download only a small part of the file, obtaining much more usable result when compared to other codec such as progressive JPEG. Second advantage is a very compact output bitstream with large bit variability – no additional entropy coding or scrambling has to be applied.

Decoding starts from the 00 sub-image of the lowest-resolution level, say, level N. We suggest transmitting the uncompressed 00_Nsub-image as the doped bits. Thus, the 00_N sub-image can be known by the decoder without ambiguity, and knowledge about the local statistics will be derived based on it. Next, other sub-images of the same resolution level are interpolated from the decrypted 00_N sub image.

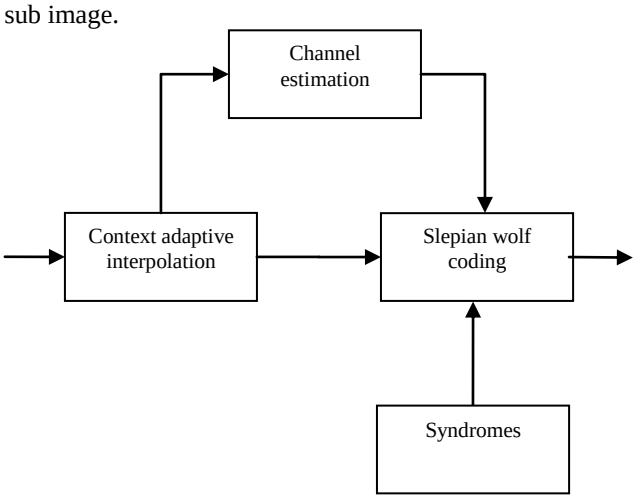

Fig. 6. Decoders Diagram in decoding the sub image

A feedback channel is needed for the encoder to know how many bits to transmit for each sub-image, which generally increases the transmission delay. However, this cost is reasonable because the encoder has no idea about the source statistics and cannot determine the coding rate. It is the decoder who is able to learn such information and advise the encoder. On the other hand, the feedback channel does consume some bandwidth, but the consumption is not directly related to the compression efficiency, and the amount of information transmitted through the feedback channel is minimal.

The SI generation in our scheme is through interpolation. For the sake of simplicity, for any pixel in the target sub-image, we only use the four horizontal and vertical neighbors or the four diagonal neighbors in the known sub-image(s) for the interpolation. Intuitively, the SI quality will be better, if the neighbors are geometrically closer to the pixel to be interpolated. Hence, we use a two-step interpolation in each resolution level to improve the SI estimation. First, sub-image 11 is interpolated from sub-image 00; after sub-image 11 is decoded, we use both 00 and 11 to interpolate 01 and 10.

Slepian-Wolf decoding treats the SI as a noisy version of the source to be decoded. We can consider that there is a virtual channel between the source and the SI. To perform Slepian-Wolf decoding, it is also necessary for the decoder to estimate the statistics of the virtual channel. The encoder decomposes each encrypted image into four resolution levels. The sub-images in the lowest-resolution level are sent without compression. But the decoder still performs inter sub-image interpolation. For the other sub-images, we transmit the four least significant bit-planes (LSB) as raw bits, because there is not much gain to employ Slepian-Wolf coding on them. The four LSBs are sent prior to the MSBs, such that the decoder can have better knowledge about the pixels before starting decoding the MSBs. The four MSBs, on the other hand, are Slepian-Wolf encoded using rate-compatible punctured turbo codes in a bit-plane based fashion. The sending rate of each Slepian-Wolf coded bit-plane is determined by the decoder's feedback.

V. CONCLUSION

An efficient compression of encrypted image data scheme was proposed, employing SPIHT compression algorithm and RSA algorithm. Here this method provides a better coding efficiency and less computational complexity than existing approaches.
This technique allows only partial access to current sources at the decoder side. Thus, further in the future we could try to use for compression of encrypted videos where Resolution Progressive Compression Scheme can be used for interframe and intraframe correlation learning at the decoder side.

REFERENCES

[1] 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, Oct. 2004.
[2] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.
[3] Y. Yang, V. Stankovic, and Z. Xiong, "Image encryption and data hiding: Duality and code designs," in *Proc. Inf. TheoryWorkshop*, Lake Tahoe, CA, Sep. 2007, pp. 295–300.
[4] D. Schonberg, "Practical Distributed Source Coding and its Application to the Compression of Encrypted Data," Ph.D. dissertation, Univ. California, Berkeley, 2007.
[5] J. D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 471–480, Jul. 1973.
[6] Li Wern Chew, Li-Minn Ang and Kah Phooi Seng, "Lossless Image Compression using Tuned Degree-K Zerotree Wavelet Coding", Proceedings of the International MultiConference of Engineers and Computer Scientists Vol I, IMECS 2009, March 18 - 20, 2009, Hong Kong.
[7]A. A. Kassim, W. S. Lee: *Embedded Color Image Coding Using SPIHT With Partially Linked Spatial Orientation Tree*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, pp. 203-206, 2003.
[8] Q. Yao, W. Zeng, and W. Liu, "Multi-resolution based hybrid spatiotemporal compression of encrypted videos," in *Proc. IEEE Int. Conf. Acous., Speech and Sig. Process.*, Taipei, Taiwan, R.O.C., Apr. 2009, pp. 725–728.
[9] J. Bajcsy and P. Mitran, "Coding for the Slepian-Wolf problem with turbo codes," in *Proc. IEEE Global Telecommun. Conf.*, San Antonio, TX, Nov. 2001, pp. 1400–1404.
[10] Wei Liu, Wenjum Zeng, Lina Dong, and Qiuming Yao, "Efficient Compression of Gray Scale Images", Vol. 19, no.4, Apr 2010.
[11] J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": *International Journal of Imaging Systems and Technology*, No. 3, 2005, pp. 178-188.
[12] M. J. Weinberger, J. J. Rissanen, and R. B. Arps, "Applicationsof universal context modeling to lossless compression of gray-scale images," *IEEE Trans. Image Processing*, vol. 5, pp. 575–586, Apr. 1996.

