RESEARCH ARTICLE OPEN ACCESS

Scalable Image Encryption Based Lossless Image Compression

Mrs. Nimse Madhuri S[#1], Dr. P. M.Mahajan[#2]
[#1]M.E Student Department of E & T. C. Engineering,
[#2]Associate Professor Department of E & T. C. Engineering, J. T. Mahajan College of Engg, Bhusawal.

Abstract
Present days processing of the image compression is the main protective representation with considerable data process on each image progression. Traditionally more number of techniques were introduced for during efficient progression in image compression on the data set representation process of application development. A content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content.\

Index Terms: Reversible data hiding operations, data hiding, Cryptography, Steganography, Reversible data hiding.

I. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data.

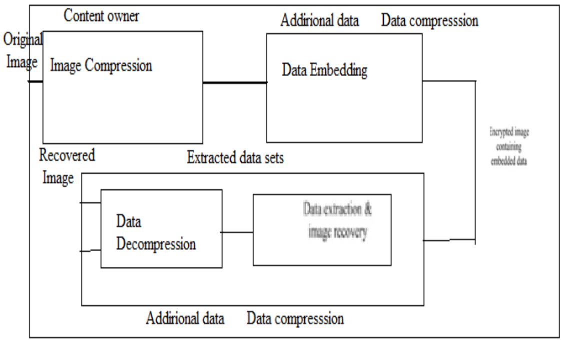

Figure 1: Image compression process with architecture.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data medication. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource.

II. LITERATURE REVIEW

Scalable image compression may achieve deal with more number of concepts related to quality maintenance with image compression also. We have to take the analysis of the different data profession and compression algorithms and analysis in recent application progress in formation technique development. This procedure may perform various development feature processes in all the data relative progress in authorized event management of the image compression of the transparent images also. These are the recent application process event management application process in developed image compression process for data transfer and other activities present in the image compression and provide security events present in the original image compression framework and development process. For example, when the mystery information to be transmitted are scrambled, a channel supplier without any information of the cryptographic key may have a tendency to clamp the scrambled information because of the constrained channel asset. While an scrambled paired picture could be layered with a lossless way by discovering the disorders of low-thickness equality check codes, a lossless packing technique for encoded light black picture utilizing dynamic deterioration and rate-perfect punctured turbo codes. With the lossy packing technique. a scrambled light black picture could be productively compacted via tossing the exorbitantly unpleasant and fine data of coefficients produced from orthogonal change. While having the layered information, a beneficiary may reproduce the central substance of unique picture by recovering the estimations of coefficients. The calculation of change in the scrambled area has likewise been considered. In light of the homo-morphic properties of the underlying cryptosystem, the discrete Fourier change in the scrambled space might be actualized.

In spite of the fact that an information hider does not know the unique substance, he can layer the minimum critical bits of the scrambled picture utilizing an information concealing key to make a scanty space to suit the extra information. With a scrambled picture containing extra information, the recipient may separate the extra information utilizing just the information concealing key, or get a picture like the first one utilizing just the encryption key. At the point when the collector has both of the keys, he can separate the extra information and recuperate the first substance without any lapse by misusing the spatial association in regular picture if the sum of extra information is not excessively expansive.

III. BACK GROUND WORK

Reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the data hiding key. At the receiver side he first need to extract the image using the encryption key in order to extract the data and after that he’ll use data hiding key to extract the embedded data. It is a serial process and is not a separable process.

For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes [1], a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in[1]. With the lessee compression method presented in [1], an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients.

IV. REVERSIBLE DATA HIDING

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. Many reversible data hiding methods have been proposed recently .As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission.

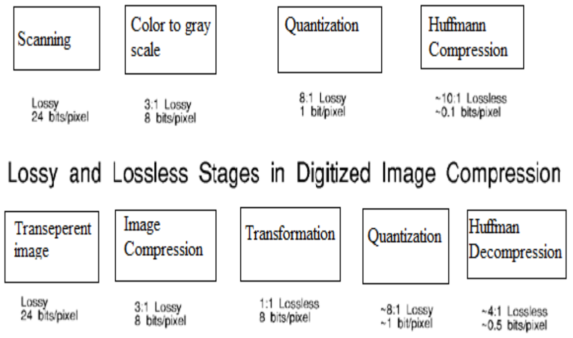

Figure 2: Procedure for image compression image extraction with suitable processing.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in some circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource. Encryption is an effective means of privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable.

V. PROPOSED APPROACH

The proposed scheme is made up of image encryption, data embedding and data extraction, image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data.

If the receiver has only the data-hiding key, the can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If he receiver has both the data-hiding key and the encryption key, can extract the additional data and recover the original image without any error when the amount of additional data is not too large. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

VI. EXPERIMENTAL RESULTS

Image Encryption

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue.

Data Embedding

This module implements an additional data embedding and enclosed into Data-Hiding Key. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

Image Decryption

This module implements an Image Decryption Process .The content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data.

Here, three quality metrics were used to measure the distortion in directly decrypted image:

- PSNR
- The Watson metric
- A universal quality index.

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression).

The Watson metric is designed by using characteristics of the human visual system and measures the total perceptual error, which is DCT-based and takes into account three factors: contrast sensitivity, luminance masking and contrast masking. Additionally, the quality index works in spatial domain, as a combination of correlation loss, luminance distortion and contrast distortion. Higher PSNR, lower Watson metric or higher means better quality. In these figures, while the abscissa represents the embedding rate, the ordinate is the values of PSNR,Watson metric or quality index.

VII. CONCLUSION

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data.

REFERENCES

[1] "*Study on Separable Reversible Data Hiding in Encrypted Images*", International Journal of Advancements in Research &

Technology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, "*Efficient compression of encrypted grayscale images*," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, "*Lossy compression and iterative reconstruction for encrypted image*," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1,pp. 53–58, Feb. 2011.

[4] T. Bianchi, A. Piva, and M. Barni, "*On the implementation of the discrete Fourier transform in the encrypted domain,*" *IEEE Trans. Inform.Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[5]. Spread spectrum image steganography.

[6]. *Altering based approach to adaptive steganography*.

[7]. Chung-Li Hou,ChanChun Lu,Shi-Chun Tsai and Wen- Guey Tzeng *An optimal Tree Based Parity Checking*.

[8] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "*An efficient buyer-sellerwatermarking protocol based on composite signal representation*," in*Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[9] S. Lian, Z. Liu, Z. Ren, and H. Wang, "*Commutative encryption andwatermarking in video compression*," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[10] 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 Processing: Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.

[11] D. Kundur and K. Karthik, "*Video fingerprinting and encryption principles for digital rights management*," *Proceedings IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[12] X. Zhang, "*Reversible data hiding in encrypted image*," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.