REVERSIBLE DATA HIDING FOR ENCRYPTED IMAGE

[PAPER ID: ICITER-D181]

TRUPTI A. GHULE
Department of Electronics & Telecommunication Engineering
Vishwabharti Academy College of Engineering, Savitribai Phule Pune University
Ahmednagar [M.S.], India truptighule1992@gmail.com

PROF. J.K.SINGH
Department of Electronics & Telecommunication Engineering
Vishwabharti Academy College of Engineering, Savitribai Phule Pune University
Ahmednagar [M.S.], India singhkumarjitendraa@yahoo.co.in

ICITER-2016

ABSTRACT:
Reversible data hiding in encrypted images is the most successful approachto its excellent property of lossless data recovery. Recently, maximum attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover may be losslessly recovered after embedded data is extracted while protecting the image content's secretly. Each and every previous methods embed data by reversibly data from the encrypted images, which can be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method of reserving data hiding before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data to the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

KEYWORDS : Reversible data hiding, image encryption, privacy protection, histogram shift.

INTRODUCTION:

Reversible data hiding in Image encryption is the art and science of invisible communication. This is accomplished through hiding secret information in other information, thus hiding the existence of the communicated information. In image encryption the information is hidden exclusively in images.

The idea and practice of hiding information have a history. In past Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of the nearest of his most trusted slaves and tattooed the message on the slave's scalp. When the slave's hair grew back then the slave was dispatched with the hidden message [2]. In the Second World War the Microdot a unique technique was developed by the Germans. Information, especially photographs, was reduce in size until it was the size of a typed period.It is Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periodson the paper containing secret information [3].

Today Image encryption is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Image encryption used to protect information from unwanted parties, but neither technology alone is perfect and can be compromised. The potential of Image encryption in communicating trade secrets or new product information. Avoiding communication through well-reputed channels greatly reduces a risk of information being leaked in transit.Hiding information in a picture of the company picnic is less suspicious than communicating an encrypted file. This paper intends to offer a state of the art overview of the algorithm used for Image encryption to illustrate the security potential of Image encryption for military and law of forensic use.

The cover image and the message image, create an Encrypted-image. For example, when a confidential message is hidden within a cover image, the result is an Encrypted -image and if we subtract cover image from Encrypted image we get message image i.e. secret message. A possible formula of the process may be represented as:

1. Cover image+ message image= Encrypted image
2. Encrypted image- Cover image= message image.

PREVIOUS ARTS:

Lot more researches has been done in the area of reversible data hiding. In the last few years, various efficient methods have been proposed for reversible data hiding. Some work in area of reversible data hiding is as follows:

Using Random Number Generation technique and Huffman coding, The Bhaskara Reddyet.al suggested an Effective Algorithm of Encryption and Decryption of Images . In this paper, they implemented security for image. They have considered an image, read its pixels and convert it into pixels a matrix of order as height and width

ICITER-2016

of the image. Replace that pixel into some fixed numbers, using random generation technique generate the key . Encrypting the image using this key, performing random transposition of encrypted image, converting it into one dimensional encrypted array and on that array finally Huffman coding applied, due this size of the encrypted image is reduced and image is encrypted again. The decryption is the reverse process of encryption. Hence the proposed method provides a high security for an image with minimum memory usage. They designed and implemented a new algorithm for encryption of images and decryption of images. This algorithm is based on a Ceaser Cipher algorithm, the random generation technique, concept of shuffling the rows i.e. rows transposition and Huffman Encoding. Encryption of an image and Decryption of an image by this algorithm protect the image from an unauthorized access. Using this Algorithm, it provides high security to an image and occupies minimum memory space. The drawback of this is a some problems in the decoding section such that, here Huffman coding is used.

Following the main steps in the encryption algorithms

Step 1. Replace each pixel with fixed number values.

Step 2. Using the random generation technique, Generate the secret key.

Step 3. Huffman Coding.

The steps in image decryption are the reverse of encryption algorithm.

In Subhanya R.J, Anjani Dayanandh N [9] presented the paper “Difference Expansion Reversible Image Watermarking Schemes using Integer Wavelet Transform Based Approach”. This represent a new scheme of image watermarking to secure intellectual properties and to safeguard the content of digital images. Image watermarking is an effective way to protect the copyright. The work related with the watermarking algorithm that embeds an image/ text data invisible into a video based on Integer Wavelet Transform and it minimize the mean square distortion between the original and watermarked image is also to increase to the Peak signal to noise ratio. Here the message bits (image) are (is) hidden in gray/color images. The size of secret or confidential data/image is smaller than cover image. To transfer the secret image/text confidentiality, the secret image/text itself is not hidden, the keys are generated for each gray or color component and the IWT, which is used to hide the keys in the corresponding gray or color component of this cover image. The watermarks are invisible and it robust against noise and commonly image processing methods. Using this method, they can improve the quality of the watermarked image and it gives more robustness of the watermark and also increasing PSNR and minimizing MSE as compared to the variety of state-of-the-art algorithms. The proposed method has a Low hiding capacity and complex computations.

Zhang suggests a unique method for separable reversible data hiding. Here content owners first use of an encryption key, encrypts the original uncompressed image to produce an encrypted image. After that the data-hider compresses the LSB (least significant bits) of encrypted image using a data-hiding key to develop a sparse space to accommodate the extra data. At the receiver end, the data embedded in the created space may be easily retrieved from the encrypted image containing extra data according to the data-hiding key. Since the data embedding is only affects the least significant bits (LSB), a decryption with the encryption key can result an image similar to the original version. While using both of the encryption as well as data-hiding keys, the embedded additional data are successfully extracted and the original image may be perfectly recovered by exploiting the spatial correlation in natural image.

In C. Anuradha and S. Lavanya [11] proposed a secure and authenticated discrete reversible Data hiding in cipher images which deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. After, a data hider may compress the least significant bits of the encrypted image using a data hiding key to produce a sparse space to accommodate some additional data. With an encrypted image containing additional data, A receiver has the data hiding key, the receiver can extract the additional data though receiver doesn't know the image content. The receiver has the encryption key, can decrypt the received data to obtain an image similar to the original image, but can't extract the additional data. If the receiver has both the data hiding key and the encryption key, that can extract the additional data and recover the original content without any error by exploiting the spatial correlation in the natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has anyone key as known, and then he can take anyone information from the encrypted data. In order to achieve authentication SHA-1 algorithm is used. Reversible data hiding scheme for encrypted image with a low computational complexity is proposed, which consists of image encryption, data embedding and data extraction/ image recovery phases. The data of original images are entirely encrypted by a stream cipher. Although a data hider does not know the original content, he embed additional data into the encrypted image by modifying a part of the encrypted data. An encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, also the decrypted version is similar to the original image. According to the data hiding key, with the aid of spatial correlation in the natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered. Although someone with the knowledge of encryption key may obtain a decrypted image and detect the presence of hidden data using LSB steg analytic methods, if he does not know the data hiding key, it is still impossible to extract the additional data and also recover the original image. For ensuring the correct data extraction and the perfect image recovery, It may be the block side length having a big value or introduce an error correction mechanism before data hiding to protect the additional data with a cost of payload reduction.

Che-Wei Lee and Wen-Hsiang Tsai1[12] proposed a lossless data hiding method based on histogram shifting, which employs a system of adaptive division of cover images into blocks to yield not only large data hiding capacities but also high stego image with high qualities. The method is shown to break a bottleneck of data-hiding-rate increasing as the image block size of 8 × 8, which is used in existing histogram-shifting methods. Four ways of block divisions are designed, in that one which provides the largest data hiding capacity is selected adaptively.

PRAPOSED WORK:

The proposed methods can be summarized as the framework, as illustrated in Fig. 1.

In this framework, a content owner encrypts the original image with an encryption key. After producing the encrypted image, the content owner hands over it to a data hide and the data hide

can embed some auxiliary data into the encrypted image by losslessly according to a data hiding key. After that a receiver may be the content owner himself or an authorized third party can extract the embedded data with the data hiding key, further recover the original image from the encrypted image according to the encryption key.

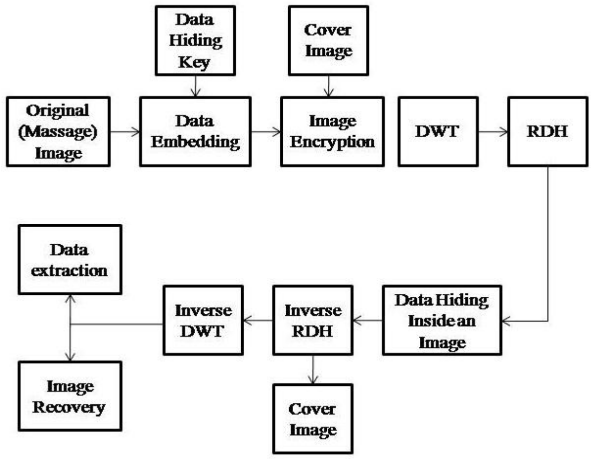


Fig.1 .Block diagram of the RDH

A. DISCRETE COSINE TRANSFORM (DCT) BASED IMAGE ENCRYPTION:

Like other transforms, the Discrete Cosine Transform (DCT) attempts to decorrelate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency.DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

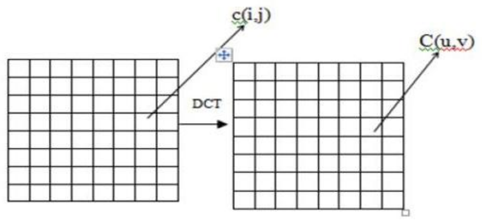


Fig. 2. Discrete Cosine Transform of An Image

The general equation for a 1D DCT (N data items) is defined by the following equation: (1) for u = 0, 1, 2, . . . , N-1. The general equation for a 2D DCT (N by M image) is defined by the following equation: (2) for u,v = 0, 1, 2, . . . , N-1. The input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; The C(u,v) is the row u and column v of the DCT matrix. Signal energy lies at low frequency in the image can appears in the upper left corner of the DCT. The compression can be achieved since the lower right values represent higher frequencies, and it generally small enough to be neglected with little visible distortion. DCT is used in Image encryption, as Image is broken into 8×8 blocks of pixels. The DCT is applied to each block when working from left to right, top to bottom. Each block is compressed through the quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

For Discrete Cosine Transform with block size (M _N), the connection between the transform domain coefficients Y (u; v) and the spatial domain image pixels X(i; j) is

$$Y(u,v)=\frac{2c(u)c(v)}{\sqrt{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} cos\left\lfloor\frac{(2i+1)u\pi}{2M}\right\rfloor\ cos\left\lfloor\frac{(2j+1)v\pi}{2N}\right\rfloor. \tag{1}$$

Where u=0,1…..,M-1, v=0,1……N-1

$$C(k) = \begin{cases}\frac{1}{\sqrt{2}}, & if\ k=0;\\ 1, & otherwise\end{cases} \tag{2}$$

ICITER-2016

B. DISCRETE WAVELET TRANSFORM (DWT) BASED IMAGE ENCRYPTION:

The Discrete Wavelet Transforms (DWTs) field is an amazingly recent one. The basic principles of wavelet theory were put forth in a paper by Gabor in 1945, Although the Discrete Wavelet Transform is merely one more tool added to the toolbox of digital signal processing, it is a very important concept for data compression. Its utility in image compression has been effectively demonstrated. This project discusses the DWT and demonstrates one way in which it can be implemented as a real-time signal processing system. Although this project will attempt to describe a very general implementation, the actual project used the STAR Semiconductor SPROC lab, digital signal processing system.1 A complete wavelet transform system as described herein is available from STAR Semiconductor. A wavelet, in the sense of the DWT, is an orthogonal function that can be applied to a finite group of data. Functionally, it is very much like the Discrete Fourier Transform (DFT), in that the transforming function is orthogonal, and a signal passed twice through the transformation is unchanged, and also the input signal is assumed to be a set of discrete-time samples. Both transforms are convolutions.[7]

The Wavelet transform (DWT) is used to convert a spatial domain into the frequency domain. The use of wavelet in the image of stenographic model lies in the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. DWT is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer a corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, the input is convolved with high pass filter (HPF) and a low pass filter (LPF).

The response of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. Here, the reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. Digital Image encryption exploits the use of a host data to hide a piece of information like that it is imperceptible to a human observer. Wavelet transforms maps the integers to integers allow perfect reconstruction of the original image. Hence proposed an algorithm that embeds the message bit stream into the LSB's of the integer wavelet coefficients of the true color image. The algorithm is also applies a preprocessing step on the cover image, which adjust saturated pixel components in order to recover the embedded message without lose. Experimental results show by the high invisibility of the proposed system even with large message size. Energy tends to a cluster spatially in each sub-band, when the Wavelet techniques provide excellent space and frequency energy compaction. For DWT, the link between the spatial or temporal domain signals, f(t), and the DWT of f(t), d(k; l), is

$$f(t) = \sum_{k=-\infty}^{\infty} \sum_{i=-\infty}^{\infty} d(k, 1)\, 2^{-k/2}\, \psi(2^{-k}t-l) \quad (3)$$

whereψ(•)denotes the mother wavelet.

Frequency based techniques are robust against attacks involving image compression and filtering. Because of the watermark, it is actually spread throughout the image, not only operating on an individual pixel. This is one of the many advantages of embedding the watermark in the transformed domain as opposed to watermarking in spatial domain Depending on application, image transform can be applied either on the whole image, or to block by block manner. Algorithms for achieving frequency domain watermarking would be modify the selected coefficients in the transformed domain. Generally the following formula is [I'i = Ii + α.Ii.Wi]used where I' and I represents the original and watermarked images respectively, W denotes the watermark, i represents the position to be embedded and _ is the watermark strength factor.[8]

For verification or detection, the receiver needs to verify if a specific watermarking pattern exists or not. A correlator is often used for the full extraction of watermark. The correlation C(I0;W) between the possible attacked image I0 and watermark W, can be calculated by

$$C_{(I',W)} = 1/L \sum I'_i \,.\, W_i (4)$$

Given a pre-determined threshold T, it can be compared with the correlation for deciding the presence of the watermark. Therefore, the decision rule for the presence of the watermark can be expressed by

$$C_{(I',W)} = \begin{cases} \geq T \text{watermark is present} \\ \leq T \text{watermark is not present} \end{cases} \quad (5)$$

The Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and also high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands produced are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). Approximation band consists of low frequency wavelet coefficients, which contain a significant part of the spatial domain image. The another bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

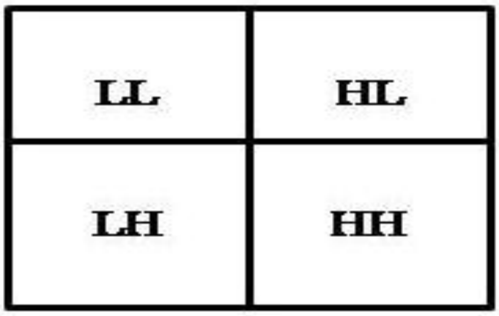
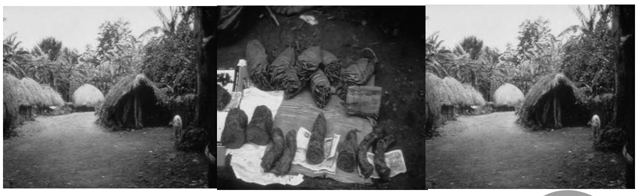


Fig. 3 . DWT Bands

EXPERIMENTAL RESULTS:

Initially a data are hidden into an image using Reversibledata hiding for encryption, then thisdata hidden image is compressed using scalablecompression algorithm and finally hides the data hidden image in a cover image. The reconstructed image canbe obtained by using the inverse of each process in reverseorder.



(a) (b) (c)

Fig. 4. (a) Original image, (b) Massage Image, (c) Encrypted image.

Table I. PSNR of Reversible Data Hiding

Sr. no .	Original Image	Cover Image	DCT PSNR	DWT PSNR
1.	Peppers.png	Onion.png	32 dB	54 dB
2.	Peppers.png	Cameraman.tif	33 dB	56 dB

CONCLUSION:

Reversible data hiding (RDH) in encrypted images is a new technology which is Drawing enormous attention because of its ability to support the content owners privacy and maintain integrity of data also real reversibility of data is realized, that is a data extraction and image recovery are free from any error because of these requirements of cloud data management. Reversible data hiding schemes for encrypted image with a low computational complexity is analyzed, which consists of image encryption, data hiding and data extraction or image recovery phases. The original images are encrypted by an encryption strategy. So a study about an encryption strategy is performed. Although a data hider does not know the original content, he can embed the secret or massage data into the encrypted image by modifying a part of the encrypted data. So methods for data embedding are also noticed. The proposed method can take advantage of all traditional RDH techniques for plain images and it achieve excellent performance without loss of perfect secrecy. Furthermore, the method can achieve real reversibility, separate data extraction and considerably improved on the quality of marked decrypted images.

ACKNOWLEDGMENT:

I wish to express my deep sense of gratitude to my guide Prof. J.K.Singh for her guidance and technical support in completing this seminar report.

I would also like to thank Prof. A.K. Yadav, Prof. and Head, Electronics and Telecommunication Engineering Department for her encouragement and guidance to us.

It's my pleasure to thank Dr. L. B. Abhang, Principal, who is a constant source of encouragement for all the students.

I am very much thankful to all the faculty members whose presence always inspires me to do better. I am also thankful to my colleagues and friends for their co-operation during the completion of this project work.

REFERENCES:

i. Kede Ma, Weiming Zhang, Xianfeng Zhao, "*Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption*" IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013

ii. T. Kalker and F.M.Willems, "*Capacity bounds and code constructions for reversible data-hiding,*" in Proc. 14th Int. Conf. Digital Signal Processing(DSP2002), 2002, pp. 71–76.

iii. Zhang, B. Chen, and N. Yu, "*Capacity-approaching codes for reversible data hiding,*" in Proc 13th Information Hiding (IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

iv. W. Zhang, B. Chen, and N. Yu, "*Improving various reversible data hiding schemes via optimal codes for binary covers,*" IEEE Trans.Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

v. J. Fridrich and M. Goljan, "*Lossless data embedding for all image formats,*" in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

ICITER-2016

vi. J. Tian, *“Reversible data embedding using a difference expansion*,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

vii. Z. Ni, Y. Shi, N. Ansari, and S. Wei, “*Reversible data hiding,”* IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

viii. D.M. Thodi and J. J. Rodriguez, *“Expansion embedding techniques for reversible watermarking,”* IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.

ix. X. L. Li, B. Yang, and T. Y. Zeng, “*Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,”* IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

x. P. Tsai, Y. C. Hu, and H. L. Yeh, “*Reversible image hiding scheme using predictive coding and histogram shifting,”* Signal Process., vol. 89, pp. 1129–1143, 2009.

xi. L. Luo et al., *“Reversible imagewatermarking using interpolation technique*,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

xii. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “*Reversible watermarking algorithm using sorting and prediction,”* IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

xiii. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography.* Boca Raton, FL, USA: CRC, 1996.

xiv. K. Hwang and D. Li, “*Trusted cloud computing with secure resources and data coloring*,” IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

xv. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, *“On compressing encrypted data,”* IEEE Trans. SignalProcess., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

xvi. 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.

xvii. X. Zhang, *“Reversible data hiding in encrypted images,”* IEEE SignalProcess. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

xviii. W. Hong, T. Chen, and H.Wu, “*An improved reversible data hiding inencrypted* images using side match,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

xix. X. Zhang, *“Separable reversible data hiding in encrypted image,”* IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

xx. Miscelaneous Gray Level Images [Online]. Available: http://decsai.ugr.es /cvg/dbimagenes /g 512 .php

ICITER-2016