ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

Reversible Data Hiding in Encrypted Images

Prajakta Jagtap[1], Atharva Joshi[2], Shamsundar Vyas[3]

Student, Computer Department, NBN Sinhgad School of Engineering, Pune, India[1,2,3]

Abstract: The following paper proposes a novel scheme of data hiding in encrypted images based on lossless compression of encrypted data. In encryption phase, the original content is encrypted into images. As majority of the encrypted data is kept unchanged, the quality of the decrypted image is satisfactory. In the receiver phase, the data is successfully extracted from the image with the help of a public key. The receiver can further recover the original plaintext image without any error.

Keywords**:** Encryption, Decryption, lossless data

I. INTRODUCTION

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption denies the message content to the interceptor. Usually encryption is used when one needs to keep his/her data private. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Such an algorithm is necessary for the decryption of the message because without it, any party will be able to crack the code and access the data. Although for a well-designed encryption scheme, large computational resources and skill are required. An authorised recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors. The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are certain approaches like cryptography and steganography. Let us understand what cryptography and steganography means.

Cryptography is the study of techniques for secure communication in the presence of third parties also called as adversaries. More generally, it is about constructing and analyzing protocols that block these third parties with the help of various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography exists at the intersection of the rules and regulations of maths, computer science, image processing etc. There are many applications of cryptography which include computer passwords and e-commerce.

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier (in our case the Image) such that the changes so occurred in the carrier are not observable. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

II. PROBLEM DEFINITION

There are existing systems having the key tool for information hiding which is *Vacating the room after encryption*. It consists of problems such as, the extracted data may contain errors. If there is no availability of sufficient space then some data may be lost & that is why the data is missing at the receiver side which can be termed as data with error. Again the un-availability of memory space is a big problem. Some space is created at the time of data embedding which is a time consuming process.

After data extraction the image recovered does not contain the qualities of the original cover. Some distortions are introduced into the image. But it is possible in future that the quality may be improved as compared to existing system.

III. THE PROCESSING

Data is hidden in the encrypted images by allocating memory before encryption. It is used to recover the original data without any loss or errors. It is basically used in the medical institutes, military institutes and law forensics, where the distortion of the original image is not permitted.

In this process, the first step is to reserve the memory space in the image for embedding of data. This sort of reservation is beneficial because it saves time for creating space for data on time. The next step is image encryption in which the image is encrypted. There are a number of methods for encryption of images such as image partition in which image is divided into two parts. Then part A is reversibly embedded into the part B. That is least significant bits are embedded first in part B.

Then the process of data hiding is done using the separable reversible data hiding. 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. This additional data is restored back in image to get image with original quality at the receiver's end.

DOI 10.17148/IARJSET.2015.2209

At the receiver end, two tasks are carried out viz. data extraction & image recovery. But, to extract the original cover from the encrypted image, an additional task known as image restoration needs to be carried out. In this additional step, the original key contents are restored in the image.

With an encrypted image containing extra data, if a user at the receiver's end has the key for decryption, he can extract the data even if he does not know the image content to extract the additional data. If the receiver has the key for encryption, he can decrypt the received data to get an image similar to the original image, but cannot extract the extra data.

If the user at the receiver's end has both the encryption as well as the decryption key then he/she can extract the extra data as well as the original image error-free by using the spatial correlation in normal image when the amount of additional data is not large.

IV. THEORY

A. Reversible data hiding techniques

The quality of the image gets disturbed when the data is embedded into the image. So it is expected that after the data extraction the image quality should be maintained just like the original image. But the image which is obtained contains some distortions. With regards to distortion in image, Kalker and Williams established a rate-distortion copy for RDH, through which they showed the rate-distortion bounds of RDH for without memory covers and proposed a recursive code development which, however, does not move towards the bound .

Another promising strategy for RDH is histogram shift (HS), in which the space is saved where data can be embedded by shifting the bins of histogram of gray values. In this process, the embedding of data is done in three steps. Step 1. The histogram is drawn. Step2. The peak point is taken into consideration. Step3. The whole image is scanned row by row. After these steps, the image is scanned again. If the grayscale value 154 is encountered, then the embedded data sequence is checked & we get the marked image. Finally, the data extraction is done. To get the original quality of the cover, the process of histogram shift is applied again. The original cover is then obtained back. Basically, data hiding is the process to hide the data into some covering media i.e. it is the concatenation of two blocks of data, first is the embedding data & second is the covering media. But in most of the cases the covering media gets distorted after the data is embedded & the covering media is not inverted back to its original form after data is removed from it [2].

Some reversible data hiding methods use the concept of differential expansion transform which is based on *haar wavelet* transform. Another concept used is the histogram shift. The differential expansion is the difference between two neighboring pixels for hiding one bit of data. In this process, the histograms are drawn first. Then the peak values are taken into consideration. Then two peak values are considered & difference is calculated. Then according to the result the bit by bit data is embedded into the image. In this way the distortion analysis is done & it is helpful to remove the distortion in the covering media & to get the original cover back [3].

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a eversible way so that the novel cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy fortification, encryption changes 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 supplier, the ability to influence the encrypted data when maintaining the plain content secret is needed. When the secret data to be broadcasted are encrypted, a supplier without any information of the cryptographic key may compress the encrypted data due to the limited channel resource.

Some attempts on RDH in encrypted images have been made. Zhang divided the encrypted image into numerous blocks. By spinning 3 LSBs of the half of pixels in every block, space can be created for the embedded bit. The data extraction and image recovery proceed by finding which part has been spinned in one block. This process can be grasped with the help of spatial correlation in decrypted image [4].

Hong et al. ameliorated Zhang’s method at the decryption side by further making use of the spatial correlation using a different estimation equation and side match method to gain much lower error rate. These two methods explained above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction [5].

Zhang et al. recovered the recursive code development for binary covers and proved that this development can gain the rate-distortion bound as long as the compacting algorithm reaches entropy, which launches the correspondence between data compression and RDH for binary covers [6].

A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. So in this way the additional data can be embedded into the covering media which is an improvement to the existing methods [7].

DOI 10.17148/IARJSET.2015.2209

Digital watermarking is a method of embedding useful information into a digital work (especially, thus, audio, image, or video) for the purpose of copy control, content authentication, distribution tracking, broadcast monitoring, etc. The distortion introduced by embedding the watermark is often constrained so that the host and the watermarked work are perceptually equivalent. However, in some applications, especially in the medical, military, and legal domains, even the imperceptible distortion introduced in the watermarking process is unacceptable. This has led to an interest in reversible watermarking, where the embedding is done in such a way that the information content of the host is preserved. This enables the decoder to not only extract the watermark, but also perfectly reconstruct the original host signal from the watermarked work[8].

B. Performance analysis of a reversible data- embedding algorithm

Data embedding in the reversible manner which is the data embedding without any loss embeds the data or payload into digital image in reversible manner. After data embedding the quality of original image may be degraded which is to be avoided. The attractive property of data embedding in reversible manner is reversibility that is after data extraction the original quality image is restored back.

Reversible data embedding hides some information in a digital image in such a way that an approved party could decode the hidden information and also restore the image to its original state. The presentation of a reversible data-embedding algorithm can be measured using following,

- ❖ Data embedding capacity limit
- ❖ Visual quality
- ❖ Complexity

The data without any distortion embedding is the attractive feature of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be pleasing, particularly in military data and medical data. In such circumstances, every small part of information is important.

From the application point of view, Since the differentiation between the implanted image and original image is almost discernible from human eyes, reversible data implanting could be thought as a top secret communication channel since reversible data implanting can be used as an information transporter.

C. Image compression Techniques

When the data is embedded into the image then the required memory is created into the covering media. But if some additional data is required, it is embedded into image then the process of image compression is done.

When it is desired to transmit repeated data over bandwidth-constrained channel, it is important to first compress the data and then encode it. Mark Johnson investigated the innovation of reversing the order of these steps, i.e., first encoding and then compressing. He showed that in certain scenarios his scheme requires no more arbitrariness in the encryption key than the conservative system where compression precedes encryption. Mark Johnson and et.al has examined the possibility of first encrypting a data and then compressing it, such that the compressor does not have knowledge of the key for encryption. The encrypted data can be compacted using dispersed source coding ethics, as the key will be available at the decoder [10].

V. OBJECTIVES

The extracted data may contain errors because if there is no availability of sufficient space then some data may lost & that's why there is data missing at the receiver side which may called as data with error. Again the un-availability of memory space is the big problem, as some space is created at the time of data embedding which is the time consuming process.

After data extraction the image recovered does not contain the qualities as was the original cover. Some distortions are there into that image.

VI. CONCLUSION AND FUTURE SCOPE

Data hiding is gaining the area of interest due to its provision for secured environment. Data hiding in reversible manner in encrypted images is providing double security for confidential data by using techniques such as image encryption.

The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner i.e. data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back. In future it may be possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery.

REFERENCES

[1] 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.

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

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

[4] 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.

[5] 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.

[6] W. 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.

DOI 10.17148/IARJSET.2015.2209

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

[8] 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.

[9] 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.

[10] 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.

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

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