A Review On Data Hiding Techniques In Encrypted Images

Ms. Anagha Markandey[#1], Prof. Pragati Patil[*2]

[#1]*M.Tech. IIIrd Sem, CSE Department*

[*2]*Assistant Professor, M.Tech,CSE Department*

Abha Gaikwad-Patil College of Engineering,Nagpur,India

Abstract **- Now a days there is very big problem of data hacking into the networking era. There are number of techniques available in the industry to overcome this problem. So, data hiding in the encrypted image is one of the solution, but the problem is the original cover cannot be losslessly recovered by this technique. That's why Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it offers the excellent property that the original cover can be recovered without any los after embedded data is extracted while protecting the image content's confidentiality. This paper enlists the various methods of data hiding in the image like differential expansion, histogram shift or the combination of both the techniques. This is useful in the way that these methods recovers the image with its original quality with improved PSNR ratio.**

Keywords **– Reversible data hiding, Image encoding, Image decoding, Image compression.**

I. INTRODUCTION

Data hiding in the encrypted images by allocating memory before encryption is used to recover the original cover without any loss & errors. It is basically used in the medical metaphors, military metaphors and law forensics, where no distortion of the original image is allowed.

In this, the very first step applied is to reserve the memory space into the image for data embedding. It is beneficial because it saves the time for creating space for data on time. Then the image encryption is stepped in which the data is embedding. There are number of methods for the image encryption 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 may include the data, some that at receiver side these contents are restored back in image to get image with original quality.

Then at the receiver side the two tasks are done as data extraction & image recovery. But to get original cover the additional task is done called as image restoration in which the original key contents are restored to the image.

With an encrypted image containing extra data, if a receiver has the key for data-hiding, he can extract the extra data though he does not know the image content. 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 receiver has both the key for data-hiding and the key for encryption, he can extract the extra data and recover the original content which is error-free by using the spatial correlation in normal image when the amount of additional data is not much large.

In this paper, in section II some earlier related work is explained which is divided into 3 parts as RDH techniques, performance analysis, image compression techniques. In section III, the disadvantages of the existing systems are enlisted named as problem definition. In section IV, the objectives are given which may be satisfied in future. Finally in section V, the conclusion with some future work is given.

II. RELATED WORK

A. Reversible data hiding techniques

As when data is embedded into the image then the quality of image get disturbed. So it is expected that after the data extraction the image quality should be maintained just like the original image. But that image contains some distortions. With regard of distortion in image, Kalker and Willems 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 [1].In this they used the encoding and decoding as,

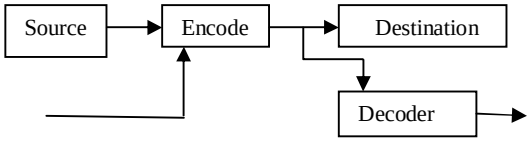

Figure 1. Reversible data hiding: Encoding & Decoding

Another promising strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. In this process the data embedding process is done in three steps as, first the histogram is drawn then the peak point is taken into consideration then whole image is scanned row by row. Then once again the image is scanned & the greyscale value 154 is encountered then the embedded data sequence is checked & we get the marked image. Then the data extraction is done. To get the original cover quality the process of histogram shift is applied again. Then the original cover is retained back. Basically data hiding is the process to hide the data into some covering media. That is it is the concatenation of two blocks of data, first is embedding data & second is 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 uses 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 neighbouring pixels for hiding one bit of data. In this 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 reversible 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.

Encryption is an effective means of privacy protection. To share a secret image with strange person, a content owner may encode the image before broadcast. In some cases, a channel administrator needs to add some extra message, such as the source data, image information 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 extra message at receiver end. That means a reversible data hiding method for encrypted image is advantageous.

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].

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 a 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].

Wei Liu et.al recommended a lossless compression method for encrypted gray image using progressive decay and rate-compatible punctured turbo codes. In this method they developed resolution progressive compression, which has been shown to have much better coding efficiency and less computational complexity than existing approaches [12]. Wei Liu and et.al observed that lossless compression of encoded sources can be achieved through Slepian-Wolf coding. For encrypted sources such as images, they are trying to improve the compression efficiency. In this paper [12], he proposed a resolution progressive compression scheme which compresses an encrypted image progressively in oath such that the decoder can monitor a low-resolution report of the image[12].

.

III. PROBLEM DEFINITION

Existing system is having the key tool as "vacating the room after encryption" consists of the problems that, 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. But it is possible in future that the quality may be improved as compared to existing system.

IV. OBJECTIVES

The lot of work in this research area is done but there are number of problems in existing systems. So the objectives to be recovered in the future may be,

- The extracted data contains the errors as there may be data loss.
- The problem of availability of memory space can occur.
- It is time consuming process.
- The key contents of original image are not restored back, so image quality may hamper.

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.

V. CONCLUSIONS & FUTURE SCOPE

Reversible data hiding in encrypted images is a new topic getting attention because of the secured-environmental requirements. Data hiding in reversible manner in encrypted images is providing double security for the data such as image encryption as well as data hiding in encrypted images both are done here.

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

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

[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.

[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] 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.

[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] 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.

[13] 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.