ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9513-9518

A Survey on Secure Reversible Data Hiding Techniques in Encrypted Images by Reserving Space In Advance

[1]Anjaly Mohanachandran, [2]Mary Linda P.A

[1]Department Of Computer Science and Engineering
KMCT College of Engineering and Technology
Calicut, Kerala, India
anjaly.m99@gmail.com

[2]Department Of Computer Science and Engineering
KMCT College of Engineering and Technology
Calicut, Kerala, India
mary.linta@gmail.com

Abstract: ***In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. There are many research processing techniques related to internet security, cryptography and steganography etc. One of these is data-hiding, using this concept we can provide security, authentication to the system. Data hiding cannot recover original cover. While Reversible data hiding is a novel concept, which can recover original cover without any loss of image. With Reversible Data Hiding (RDH) we can perform embedding operation after encryption. In this technology initially a content-owner creates space for embedding additional data and then encrypts the original image after that data hider module embed additional data in the space created in the encrypted image. At the receiver side, host can extract the data and additional data and recover original message. This concept improves payload & security of the system. This is the basic theme of this concept. Basically this work describes the survey of the reversible data hiding techniques, related methods and procedures that have been developed with the subject.***

Keywords: Data Hiding, Reversible data hiding, Image encryption, Image decryption.

1. Introduction

Now days in an entire range of everyday life digital media is stored efficiently and with a very high quality but by using computer systems it can be manipulated very easily. Consequently we know that digital data can also be transmitted through data communication networks without losing quality in a fast and inexpensive way. With digital multimedia, distribution over World Wide Web Intellectual Property Right (IPR) is more threatened than ever due to the possibility of unlimited copying. So by using some encryption techniques this easily copying of the data need to be restricted. However encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. This problem can be solved by hiding some ownership data into the multimedia data which can be extracted later to prove the ownership. This technique mostly used in bank currency where a watermark is embedded which is used to check the originality of the note. The same concept called watermarking may be used in multimedia digital contents for checking the authenticity of the original content.

Data hiding is one of the solutions of security that keep the data secure in host media while transferring the information but there exists some distortion .Data hiding in encrypted images by allocating memory before encryption. There are some applications where we use the Data-hiding concept;

1. Secret communication.
2. Image authentication.
3. Finger printing.
4. Fraud detection.
5. Copy control.

A large volume of data transmitted over internet is private and confidential. Encryption is the desired to transmit the information correctly and safely. The security provided by stegenography is more than the security provided by cryptography alone. Thus due to various similar reasons these concepts are widely used in data transfer through internet now a days. These two concepts are used in the system along with authentication which provides the authorization to the user to use the system with all correct functionalities.

Cryptography can protect the data while transmission but when it is decrypted, there is no more protection left. To provide more protection and safety information hiding techniques are used now a days and steganography is one of them which allows the user to store a large amount of data behind any image. Cryptography aims at creating data unintelligible for the third person who is not authorized to get the information. Steganography deals with hiding the data from the third person behind any image.

As the growth of information technology more data available on the internet so it faces lots of security problems. These security problems solved by many techniques such as cryptography, steganography, reversible data-hiding etc. the RDH technique establishes on steganography & security. While transferring the message from sender to receiver, exist the intruder that steals the information between of them. This type of transmission restricted by some applications such as military imagery, law forensic etc. The water marking is most favorable technique for providing the security to the system. With the use of this technique, we can watermark the information and protect the information from intruders. We can find out where the image or data modified or performed the changes by intruder or third party so that we can easily detect the modification by using the watermarking concept. The watermarking concept make the system more secure by encryption the watermark image.

2. Existing Techniques

2.1 Reversible Data Hiding

Data hiding is the way of hiding information into a cover media. It requires two set of data that are embedded data and set of cover media data. In some case cover media distorted due to perform hiding operation but this type of changes are not acceptable by some applications such as medical imagery, military imagery and law-forensic etc. so that a novel method become more popular among the researches i.e. known as Reversible data hiding (RDH).It is the technique that perform lossless embedding operation and recover the origin after the extraction. If cover medium distorted permanently when hidden message have been removed. Original Image encrypted into image encryption by using the encryption-key algorithm at the side of image owner. After that in the data hider module we can embed some additional data with the use of data-hiding key, finally gets the encrypted image that containing additional data and that image require to decryption at the receiver side. This concept describe by following figure.

Reversible data hiding techniques can be generally classified into two frameworks

1. Vacate room after encryption
2. Reserve room before encryption

In the first framework, vacate room after encryption (VRAE), a content owner first encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

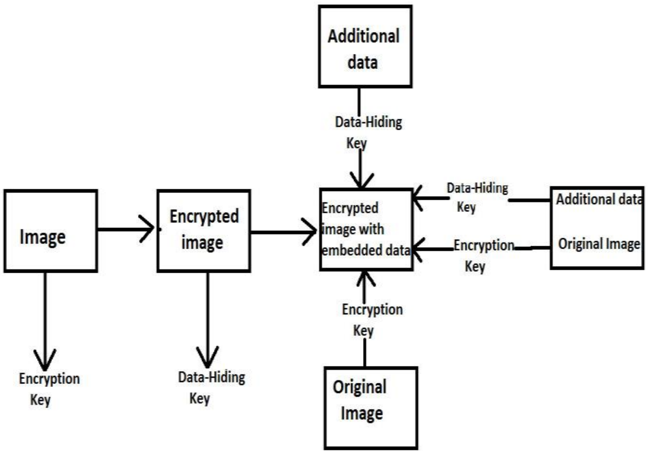

Figure 1: Reversible data- hiding in encrypted image.

In the second framework, reserve room before encryption (RRBE), the content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embed ding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy.

3. Literature Survey

Most of the work of reversible data hiding emphases on the data embedding/extracting on the plain spatial domain . But, in some scenarios, an media assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content (payload) should be recovered without any error after image decryption and message extraction at receiver side.

Xinpeng Zhang presented a practical scheme satisfying the above-mentioned requirements. A content owner encrypts the original image using an encryption key, and a data-hider embeds additional data into the encrypted image using a data-hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data [1].

Wei Zhang and Xianfeng Zhao [2] have proposed the system that maintains the reversibility. This paper defines the reversible data-hiding in encrypted image by using spare space as reserving room before encryption. Here more attention on RDH technique which maintains the reversibility that means original cover recovered after embedding additional data. It provides the security and confidentiality to user. It is new topic for cloud data management because of privacy preserving requirements. The Existing System implemented by the use of the concept of RDH in encrypted images by vacant room before encryption, but proposed system was opposite of it in this we use the reserving concept before encryption. The advantages of this proposed system is to maintain the extra space for embedding data in data hider module. This system achieves excellent performance without any loss of data.

W. Zhang, B. Chen, and N. Yu [3] have proposed a system which uses a decompression algorithm for embedding the data .It approaching the codes for reversible data hiding and improve the recursive code construction for binary bounds and this type of construction achieve the result that is rate-distortion bound that uses the concept of compression algorithm. This system checks the equivalency between data compression and RDH for binary bounds. This system defines many benefits such as reduces the distortion, improve the RDH schemes for spatial. This system also has some drawback such as not consider grey scale for designing recursive codes.

J.Tian [4] has proposed a system which uses difference expansion method for embedding data in reversible manner for digital images. Reversible data embedding means lossless embedding. Here quality degradation was very low after embedding the data. This paper describes how to measure the performance of the system by using the concept of reversible data embedding. This can be measure through various factors such as the payload capacity limit, visual quality and complexity. This system uses the differences between two neighboring pixels. The LSB's of the differences are all zero and this embedded to the message. The benefits of the system are no loss of data while performing compression and decompression. This system is useful for audio and video data. The drawbacks of the system are achieving error because of division by 2 and due to bit replacement visual quality degrade.

Z. Ni, Y. Shi, N. Ansari, and S. Wei ,[5] have proposed a system that perform the Reversible Data hiding by using the histogram shift operation for RDH. In this system used the spare space for embedding the data by shifting the bins of gray scale values. The embedding capacity measured by the use of number of pixels in peak point. This system has some benefits such as it is simple and has constant PSNR ratio, capacity is high and distortion is very low. This system has some disadvantages such as more time consuming while searching the image number of times.

X. L. Li, B. Yang, and T. Y. Zeng [6] have used a hybrid algorithm. It is basically uses three algorithms adaptive embedding, Predictive –Error Expansion (PEE) and Pixel selection. Predictive Error expansion is important for embedding the data and used for reversible watermarking. It provides authentication and integrity to the user. It also improves the payload with low distortion. Where distortion free data required we use the concept of watermarking. PEE is an improvement of the Difference Expansion (DE). The proposed system described the threshold value for pixel of image and it divides the image pixels into two parts. Afterward select the pixel on the basis of capacity parameter and threshold. Adaptive embedding and pixel selection performed simultaneously. This system reduces the embedding impact with the use of decreasing the modification and improves the visual quality.

L. Luo et al. [7] have used an interpolation technique for reversible image watermarking. Reversible image watermarking restores the original image without any distortion after performing the extraction of hidden data. In this system we can embed large amount of covert data for imperceptible modification. Digital watermarking is the form of data hiding that are used to embed the covert information into digital signal. This paper based on adaptive interpolation-error expansion, which provides very low distortion rate and lager capacity. It also improves the image quality.

Compression of encrypted data has become considerable research interest in recent years. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. There are Several techniques for compressing/decompressing encrypted data have been developed.

When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it. Mark Johnson investigated the novelty of reversing the order of these steps, i.e., first encrypting and then compressing. He showed that in certain scenarios his scheme requires no more randomness in the encryption key than the conventional 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 encryption key. The encrypted data can be compressed using distributed source coding principles, because the key will be available at the decoder. They showed that under some conditions the encrypted data can be compressed to the same rate as the original, unencrypted data could have been compressed [8].

Wei Liu et.al suggested a lossless compression method for encrypted gray image using progressive decomposition 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 [9].Wei

Liu and et.al observed that lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, they are trying to improve the compression efficiency. In this paper [9], he proposed a resolution progressive compression scheme which 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. He focused on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression. Resolution progressive compression is used for this problem, which has much better coding efficiency and less computational complexity than existing approaches [9].

Wien Hong et.al [10] proposes an improved version of Zhang's reversible data hiding method in encrypted images. The original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness. Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work. For example, when the block size is set to 8x8, the error rate of the Lena image of the proposed method is 0.34%, which is significantly lower than 1.21% of Zhang's work.

Reversible watermarking enables the embedding of useful information in a host signal without any loss of host information. Tian's difference-expansion technique is a high-capacity, reversible method for data embedding. However, the method suffers from undesirable distortion at low embedding capacities and lack of capacity control due to the need for embedding a location map. Diljith M. Thodi et.al [11] proposes a histogram shifting technique as an alternative to embedding the location map. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem. We also propose a reversible data-embedding technique called prediction-error expansion. This new technique better exploits the correlation inherent in the neighborhood of a pixel than the difference-expansion scheme. Prediction-error expansion and histogram shifting combine to form an effective method for data embedding. The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity when compared to difference expansion. There is also a significant improvement in the quality of the watermarked image, especially at moderate embedding capacities.

4. Overview of Proposed Method

The existing system describe with concept of "vacating the room after encryption (VRAE)". With the use of this concept system may has some error because of there is not sufficient space exist for performing the embedded operation and lost the data at receiver side. Here un-arability of space is biggest problem and some space created at the time of embedding. So this is also time consuming process. After extracting the data we cannot achieve the originality. Some distortion exists in the system. So our aim is to remove this type of distortion form the system.

There are lots of problems in the existing system. So objective is to recover the problems in future, which are described below:

- The extracted data may contain error.
- Time-consuming process.
- Availability of memory space.
- The key contents are not store of original image.

These entire problem recovered by using the concept of "Reserving Room Before encryption (RRBE)". With the use of VRAE concept with cannot achieve original data after encryption. So that new concept used for achieve this property i.e. RRBE. The proposed system extracted data losslessly after encryption.

5. Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption

In this framework, a customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy. RRBE primarily consists of four stages:

- Generation of encrypted image.
- Data hiding in encrypted image.
- Data extraction.
- Image recovery

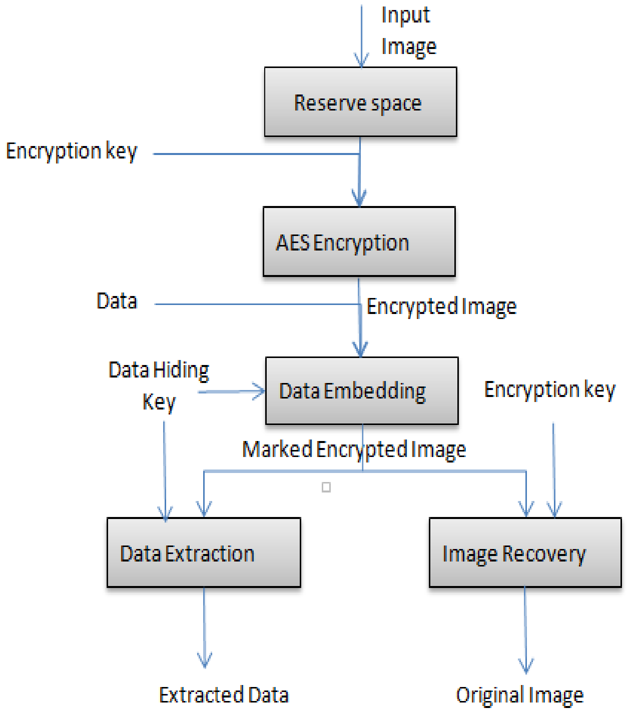

Figure 2: Framework: Reserving Room before Encryption (RRBE)

5.1 Generation of Encrypted Images

Actually, to construct the encrypted image, the first stage can be divided into three steps:

- Image partition
- Self-reversible embedding
- Image encryption

At the beginning, image partition step divides original image into two parts A and B ; then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

5.2 Data hiding in encrypted image

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of A, denoted by AE. Since AE has been rearranged to the top of E, it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by E'. Anyone who does not possess the data hiding key could not extract the additional data.

5.3 Data extraction and image recovery

1) *Case 1: Extracting Data from Encrypted Images:* To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of this work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

2) *Case 2: Extracting Data from Decrypted Images:* In Case 1, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case.

6. Conclusion

Secure reversible data hiding in encrypted images by reserving room before encryption can enhance the data security while transmitting the secret data and secret image through the networks. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which is proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effort- less. After the studying of various papers, we conclude that proposed system provides more authentication, confidentiality and security in compare to the existing system. The existing system has some drawbacks that were overcome with proposed system. The proposed method will take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

References

[1] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255258, Apr. 2011.

[2] Kede Ma, Wei. Zhang, Xianfeng Zhao, “Reversible data Hiding in Encrypted Images by reserving Room before encryption”, IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.

[3] W. Zhang, B. Chen, and N. Yu, “Improving various reversible data hiding schemes via optimal codes for binary covers” vol. 21, no. 6, pp. 2991–3003, June. 2012.

[4] J. Tian, “Reversible data embedding using a difference expansion” Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890 2003.

[5] 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.

[6] X. L. Li, B. Yang, and T. Y. Zeng, “on adaptive prediction-error expansion and pixel selection Image Process., vol. 20, no. 12, pp. 3524.

[7] L. Luo et al., “Reversible image watermarking using interpolation ,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, “Lossless Data hiding.

[8] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonbergand K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

[9] Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao “Efficient Compression of Encrypted Grayscale Images”,

Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102.

[10] 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.

[11] 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.

[12] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. watermarking algorithm using sorting and prediction Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989.

Author Profile

Anjaly Mohanachandran is P.G. student, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. She obtained her B.Tech degree in Computer Science & Engineering from Indira Gandhi Institute of Engineering & Technology in 2013. She is currently pursuing the M.Tech .degree in Computer Engineering from Calicut University.

Mary Linda P.A. is Assistant Professor, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. Her research focuses on Image processing, Internet security. She obtained her B.Tech degree in Computer Science & Engineering from KMCT College of Engineering in 2007. And she completed her M.Tech degree in Image processing from Model Engineering college, CUSAT in 2012.