Survey on a Novel approach for Reversible Data Hiding: Principles, Techniques and Recent studies

Arti yadav
PG Student, Dept. of Computer Engg.,
G.H. Raisoni College Of Engineering & Management,
Pune, India

Mrs. Minaxi Doorwar
Assistant Professor Dept. of Information Technology.
G.H. Raisoni College Of Engineering & Management,
Pune, India

Abstract— Today data hacking is a very big problem in networking field. There are many security techniques are available for solving the problem. One of these data-hiding, using this concept we can provide security, authentication to the system. Data-hiding technique has un-able to recover original message. A novel concept known to be reversible data hiding (RDH).Reversible data hiding recover the original message without any loss of information. We perform the embedding operation after encryption. With the use of this technique we can improve the payload and security to system.

Keywords - Data–hacking, Data-hiding, Reversible data hiding (RDH), payload etc.

I. INTRO DUCTION

In Recent year data security is the biggest problem because of data are growing on the internet very rapidly.so that it faces many problems related to security. Image –processing in encrypted domain has attracted by many researcher. In recent year signal-processing is most favourable field because it produces many new applications such as health monitoring products, confidential transmission product, surveillance and military product. All these applications concern with the security, confidentiality and authentication. As increasing the digital techniques for storing and transmitting the information it faces many issues related to security. Now a days information security is more important for transferring the information from one end to another end over network. Data hiding one of the solution for 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;

- Secret communication
- Image authentication
- Finger printing
- Fraud detection
- Copy control

Properties of data-hiding schemes

- *Robustness*: To extract the hidden information after apply the same operation such as linear, non-linear filter, lossy compression etc.
- *Un-Detestability*: To prove the presence of hidden message impossible. This concept is inherently tied with statistical model of carrier image.
- *Invisibility*: It is most important tool for securely transfer the information In this human perception based on the human visual system.
- *Security*: This is performed by various security algorithms.

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 favourable 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.

There are various techniques which provide security that are defined following:

A. *Cryptography**:*** Cryptography is an art of securely transferring the message from sender to receiver.it use the key concept for encryption the message. Information known as cryptography. It is used when communicating over the untrusted media such as internet. Cryptography is the technique that used in securely transfers the information with the use of algorithm which is un-reable by the third-party.

1) *Categories of cryptography*

   a) *Symmetric-key cryptography*: Symmetric-key cryptography is the technique that performed encryption and decryption by using single key. It is also known as secret key encryption.

   b) *Asymmetric-key cryptography*: It is also known as the public –key cryptography. In this we use two keys.one for encryption i.e. public and another for decryption i.e. decryption.

   c) *Hash Encryption*: Hash encryption performed by using the hash function. It provides security to user by using this concept. It produces fixed length signature for a message.

Here our concern with image encryption. Image encryption technique is different from simple encryption. The data hiding in image takes place following four steps that are:

- Select the medium or carrier.
- Message which needed protection.
- A function that will be used to hide data in the cover media.
- Alternative key which provide authentication.

2) *Types of Image cryptography/Encryption*

   a) *Generation of encryption-key*: It is generated by randomly by using random function. It uses 128-bit of value.

   b) *Generation of pseudo-random sequence*: It is generated by using encryption-key. For example RC-4 algorithm used to generate the pseudo random sequence using 128-bit encryption key.

B. Steganography: Steganography word takes from Greek word that is made up of two words such as "stegan" and "graphy", it means cover or secret writing. It deals with composing hidden messages. It is the way of hiding information without the knowledge of third-party. Steganography provides the security to the message as well as content of the information. It is an art of hiding information by embedding messages within other, seemingly harmless messages.

Steganography perform using three media:

- Hiding a message inside "text".
- Hiding a message inside "images".
- Hiding a message inside "audio" & "video".

It is the process of hiding a secret message within the carrier such as image, text, and audio.

1) *Steganography perform under two types of domains:*

   a) *Spatial Domain*: Processing is directly applicable to the pixels of image. For example of spatial domain is Least Significant bits (LSB) technique. With the use of this technique we can transfer pixels of image into binary value of pixel.

   b) *Frequency Domain*: It is applied when transferred the pixel value after that processing applicable on the transformed co-efficient. For Example of frequency domain are DCT & DWT technique. In this we implement the mathematical function which transform digital image from the spatial to the frequency domain.

These two techniques are complementary and mutually commutative.

There are various applications where we use the digital steganography of images that includes following properties:

- *Copy-right protection*: With the use of watermarking we can protect the copy-right of the product. We can embed inside an image to identify it as intellectual property.
- *Feature tagging*: This feature use by embedding caption, annotations, time-stamps etc. inside an image.
- *Secret communication*: In some cases cryptography not accepted, where we use the concept of steganography for covert communication.

II. EXISTING TECHNIQUES

A .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 [1]. This concept recovers the original image by using the encryption technique after performing the extraction. Encryption is the effective tool for providing the security to the system. It is useful for sharing the secret image from content owner to another person.

1).Reversible Data embedding algorithm used for measuring the performance:

Reversible data embedding is also known as lossless data embedding. It embeds the invisible data into digital image in a reversible manner. An authorized user can decode the hidden message and restore the original state. The performance can be measured by the following:

- Payload capacity limit.
- Visual quality.
- Complexity.

It is the motivation of distortion free embedding. With the use of this concept we can increase the capacity that means we can improve the embedding capacity limit.

B. Separable Reversible data hiding

Reversible data hiding technique uses the concept of separation. It means to able to separate the techniques as the requirement of some activities under some circumstances. The separation of activities means to extract the original cover image and extraction of payload. This type of separation performed with the use of keys.

C. Compression method for encrypted data

Compression of encrypted data is most interesting topic towards researcher. It is the traditional method that is used for removing redundancy from data after that perform the encryption. At the receiver side we perform the decryption and decompression orderly. A sender wish to keep the data confidential when sending the data to receiver then sender should use the encryption key and decryption key similarly for transmission over the channel. There are various encryption/ decryption techniques that are used for security purpose. When we transmit redundant data over untrusted medium then firstly we can compress the data after that perform the encryption algoithm.

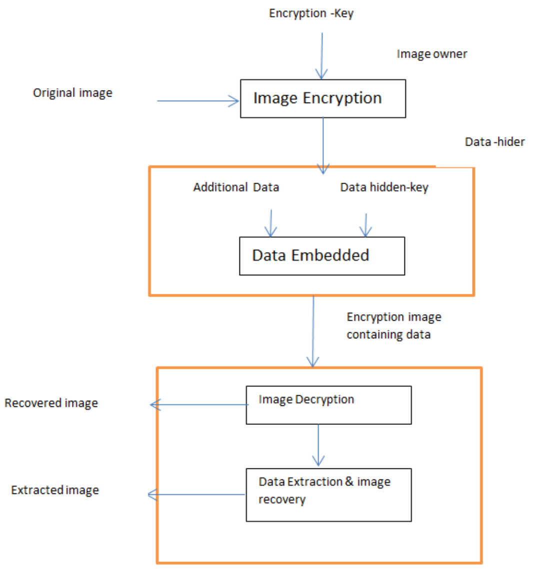

Figure 1: Reversible data- hiding in encrypted image.

III. LITERATURE SURVEY

A .Title: "Reversible data Hiding in Encrypted Images by reserving Room before encryption".

Author: Kede Ma, Wei. Zhang, Xianfeng Zhao.

Summary:

Wei Zhang and Xianfeng Zhao 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.

B. Title: "Improving various reversible data hiding schemes via optimal codes for binary covers".

Author: "W. Zhang, B. Chen, and N. Yu".

Summary:

W. Zhang, B. Chen, and N. Yu[2] 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.

C.Title:"Reversible data embedding using a difference expansion".

Author: "J. Tian"

Summary:

J. Tian 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 neighbouring 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.

D. Title: "Reversible data hiding".

Author: "Z. Ni, Y. Shi, N. Ansari, and S. Wei".

Summary:

Z. Ni, Y. Shi, N. Ansari, and S. Wei , 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.

E. Title: "Efficient reversible watermarking based error expansion and pixel selection".

Author: "X. L. Li, B. Yang, and T. Y. Zeng"

Summary:

X. L. Li, B. Yang, and T. Y. Zeng 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.

F. Title: “Reversible image watermarking using interpolation”

Author: “L. Luo et al.”.

Summary:

L. Luo et al. 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.

IV. OVERVIEW OF PROPOSED IDEA

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 lot of problems in the existing system. So objective is to recover the problems in future, which are described following:

- 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 future 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. The proposed system follows the following steps that are:

- *Reserving Room for data hiding*: Here concern with empty room means to create spare space for performing embedding operation before encryption. It hides data and achieves real reversibility.
- *Image Encryption*: Firstly content owner reserve the space for performing the hiding operation with the use of encryption-key. In this case firstly reserves the space in original image after that use the encryption algorithm. Finally gets the encrypted image and handover to the third party.
- *Data–hiding in encrypted image:* This key is used for hiding the content of the message. It is used both module such as data-hider and receiver side.
- *Data extraction and image recovery*: The content owner sends image to the receiver by the use of encryption and steganography. After that at the receiver side perform the decryption with the use of encryption-key. If receiver has the encryption-key then extract the original message and additional message.

The proposed system improves the payload capacity as compared to existing system. The reserving room concept achieves real reversibility that means without any loss of information we extract the original image and addition data. This technique is useful where any modification or loss of data not acceptable. It provides confidentiality, authentication to the user. It improves PSNR ratio.

It also improves the visual quality.

V. COMPARISION WITH EXISTING TECHNIQUES

The existing system describe on the basis of “vacating the room after encryption (VRAE)”. There are few techniques are based on it.

- Fridich et all [7] describe the practical aspect and general framework for RDH. In this we firstly extract the compressed features of original cover after that performing the compression technique losslessly. With the use of this technique we can achieve spare space for embedding the information.
- J. Tian [3] describes the concept of difference expansion (DE). It is also based on the VRAE concept. Here difference of each pixel of image expanded by multiplied by 2 etc.
- Another method is also based on this technology i.e. histogram shifting. Embedding perform by the use of shifting the bins in the form of histogram of gray-value.

All these three techniques are described with the use of VRAE .these technique achieve small payload and cannot recover without loss of information.

All these problems overcome with the proposed system that is uses the concept of RRBE.

VI. CONCLUSION

Reversible Data hiding is new topic for providing privacy to the cloud data management. 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. RDH technique achieves real reversibility. This is used by many fields.

REFERNCES

[1] 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.

[2] 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.

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

[4] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding” Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354 [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.

[5] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, December.2011.

[6] 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.

[7] J. Fridrich, M. Goljan, and D. Rui, “SPIE Photonics West, Security and Watermarking of Multimedia Contents III, San Jose, California, USA, Vol. 3971, pp. 197.