ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 7, July 2017

A REVIEW: VARIOUS TECHNIQUES FOR DATA HIDING AND CRYPTOSYSTEM USING IMAGE PROCESSING

Punisha Rajput[1]
Email I'd- punisha6335@gmail.com
AmitAsthana [2]
Computer Science engineering
Subharti Institute of Technology and Engineering (Meerut, India)

ABSTRACT

A system for lossless and reversible data hiding in encrypted images proposes a lossless, a reversible, and a combined data hiding schemes. To add one more level of security the scheme is applied for cipher text images. The third and final scheme is the combined scheme i.e. combination of lossless and reversible scheme. With the combined technique, there are two possible outcomes. A receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption. In recent study do not differentiate between the two system I.e. reversible and lossless system. It is also noticed that if data embedding capacity increases then the image quality decreases. The existing system tries to overcome all these flaws.

Keyword: - Reversible data hiding, lossless data hiding, image encryption, cryptosystem etc.

I. INTRODUCTION

Data hiding is a system for inserting data into spreads, for example, picture, sound, and video documents, which can be utilized for media documentation, copyright security, trustworthiness verification, secretive correspondence, and so forth. Most information concealing techniques install messages into the cover media to produce the checked media by just changing the minimum critical piece of the cover and, in this way, guarantee perceptual straightforwardness. The inserting procedure will more often than not acquaint perpetual twisting with the cover, that is, the first cover can never be recreated from the stamped cover. In any case, in a few applications, for example, restorative symbolism, military symbolism, and law crime scene investigation, no corruption of the first cover is permitted. In these cases, we require an exceptional sort of information concealing strategy, which is alluded to as reversible data hiding (RDH) or lossless information stowing away, by which the first cover can be lossless reestablished after the implanted message is extricated. The square graph of RDH is appeared in figure 1.1. Reversible steganography or watermarking can reestablish the first bearer with no bending or with insignificant mutilation after the extraction of concealed information. So reversible information covering up is presently getting mainstream.

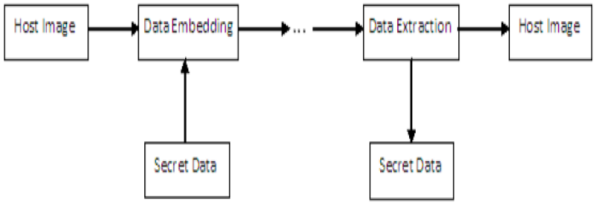

Fig 1.1 Reversible data hiding flow

As an essential necessity, the quality debasement on the picture after information implanting ought to be low. A fascinating component of reversible information implanting is the reversibility, that is, one can evacuate the inserted information to reestablish the first picture. From the data concealing perspective, reversible information installing shrouds some data in an advanced picture such that an approved gathering could translate the shrouded data and furthermore reestablish the picture to its unique, unblemished state. The inspiration of reversible information implanting is sans mutilation information installing. In spite of the fact that intangible, installing a few information will unavoidably change the first substance. Indeed, even an exceptionally slight change in pixel esteems may not be alluring, particularly in delicate symbolism, for example, military information and restorative information. In such a situation, all of data is imperative. Any change will influence the knowledge of the picture, and the entrance to the first, crude information is constantly required. From the application perspective, reversible information installing can be utilized as a data transporter. Since the contrast between the installed picture and unique picture is practically indistinct from human eyes, reversible information implanting could be thought as an incognito correspondence channel. By installing its message validation code, reversible information implanting gives a genuine self verification plot, without the utilization of metadata.

1.1. Lossless Data Hiding Scheme:

A lossless data hiding scheme for public-key encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver. With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the ciphertext pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same. When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property.

II. LITRATURE REVIEW

In related research , author proposed own studies with various technique are as below:

X Zhang [1]displayed a lossless reversible information concealing method which gives the correct recuperation of the first flag and furthermore gives correct extraction of the inserted data. Also, this correct recuperation with lossless information is only the reversible information covering up. Generally the wellknown LSB technique is utilized as the information implanting strategy. Reversible information stowing away is a method that is essentially utilized for the confirmation of information like pictures, recordings, electronic archives and so on. The primary use of reversible information concealing procedure in Intellectual Property Rights is security and validation. In some application it is imperative to give security and protection amid exchanging information. That is the reason it is important to shroud the information or to give the information security we require new approach in web correspondence.

VinitAgham [2], presented Pseudo random sequence consists of random bits generated using the encryption key. The additional data embedded to encrypted image using the parameters. With an encryptedimage containing additional data, the receiver may extractthe additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered. Compared with the other algorithms, this system demonstrated successful accuracy in recovering the original images.

Rengarajaswamy [3], presented to summarize this paper, at the transmitter side an encryption is carried. Then the DFT compression is performed to the encrypted image to create the space needed to hide the secret image. In the free space provided the additional secret data is embedded using the data-hiding key. DFT thus provides efficient compression in the frequency domain. Then at the receiver side, either of the key is used independently to recover the cover image and the secret data separately. Among other compression techniques DFT operates well in the frequency domain which is best suited for audio and images. Concluding that DFT provided best compression rate and loss is a least part.

X. Zhang [4] offered a practical scheme having an encrypted image containing additional data a receiver first decrypts it according to the encryption key, and then extracts the embedded data and recovers the original image according to the data-hiding key. In this scheme the procedure of data extraction is not separable. In other words, the content of original image is revealed before payload extraction, and, if someone has the data-hiding key only but not the encryption key he is unable to extract any information from the encrypted image containing additional data.

Z. Ni, Y. Shi, N. Ansari, and S. Wei [5] 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 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 itis the concatenation of two blocks of data, first isembedding 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.

V. Sachnev, H. J. Kim, J. Nam, S. Suresh[6] 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.

X. Zhang [7]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.

W. Hong, T. Chen, and H.Wu[8]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.

W. Zhang, B. Chen, and N. Yu [9]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.

D.M. Thodi and J. J. Rodriguez [10]Digital watermarking is a method of embeddinguseful information into a digital work (especially, thus, audio, image, or video) for the purpose of copy control, content authentication, distribution tracking, broadcast monitoring, etc. 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.

III. CHALLENGES

1. This causes the security problem of exposing transmitted digital data on the network with the risk of being copied or intercepted illegally.
2. A problem occurs here when too many of such pairs are selected for data hiding.

3. Communication over the internet is facing some problem such as data security, copyright control, data size capacity, authentication etc.

IV. IMPORTANCE

1. The planned method can acquire advantage of all traditional RDH techniques for direct images and succeed superior performance without loss of perfect secracy.
2. In some applications, such as medical image processing and military image processing, retrieval of the original cover image without any damage is a must, since these images have too process further.
3. Data hiding is a method of overlapping information into the original information. it is a valuable tool as itsfound in a various number of applications access control, annotation and authentication, multimedia, etc.
4. In most day to day application we all like the comforts of privacy and security during data transfers.

5. The reversibility benefits many practical applications such as medical image processing and multimedia archive management.

V. DISSCUSSION

In beyond numerous works in literature survey accessible by numerous Authors, we examine about various or many present research idea in terms of concept of the reversible data hiding, lossless data hiding and image encryptionwhich are given us to Data security and data integrity are the two challenging areas for research. There are so many research isprogressing on the field like internet security, steganography, cryptography. Data hiding are a group of techniques usedto put a secure data in a host media with small deterioration in host and the means to extract the secure data afterwards.Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, suchas military or medical images, with a reversible manner so that the original cover content can be perfectly restored afterextraction of the hidden message. The reversibility means not only embedding data but also original image can beprecisely recovered in the extracting stage. Most hiding techniques perform data embedding by altering the contents ofa host media. These types of data hiding techniques are thus irreversible. However, in a number of domains such asmilitary, legal and medical imaging although some embedding distortion is admissible, permanent loss of signal fidelityis undesirable. This highlights the need for Reversible (Lossless) data embedding techniques. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. a novel reversible data hidingscheme for encrypted image. After encrypting the entire data ofan uncompressed image by a stream cipher, the additional datacan be embedded into the image by modifying a small proportionof encrypted data.With an encrypted image containing additionaldata, one may firstly decrypt it using the encryption key, and thedecrypted version is similar to the original image.

VI. CONCLUSION

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. Thus such proposed scheme provides a completely new framework for reversible data hiding. Here in this approach we have used a new technique for reserving room before encryption of image. Thus the data hider can benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In author proposed approach we analyze advantage of visual cryptography approach for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. The employed technique involves the three main steps that are sieving, division and shuffling the images. Thus random shares are so generated from shuffled shares of image are transmitted.

In future, such approach does not involve any use of keys is keyless approach for image encryption with the complete lossless image recovery and data extraction.

REFRERENCES

[1] X Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826-832, April. 2012.

[2] VinitAgham Department of Computer Engineering R C Patel Institute of Technology, Shirpur.Dist. Dhule, Maharashtra, India.TareekPattewar Department of Information Technology R C Patel Institute of Technology, Shirpur.Dist. Dhule, Maharashtra, India “A Novel Approach towards Separable Reversible Data Hiding Technique” 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

[3] Rengarajaswamy1 Assistant Professor, Department of Electronics and Communication Engineering, M.A.M School of Engineering, Trichy, Tamil Nadu “DFT Based Individual Extraction Of SteganographicCompression Of Images”, IJRET February 14.

[4] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255-258, April 2011.

[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] 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.

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

[8] 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.

[9] 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.

[10] 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.