Design of Improved Reversible Data Hiding In Encrypted Images

M.RamaRao & P.Kumaraswamy

[1]M.Tech., Department of CSE., SR Engineering College,Warangal,Telangana, India.

[2]Assistant Professor, Department of CSE, SR Engineering College, Warangal, Telangana, India.

ABSTRACT:*Recently, different techniques are available for data hiding. When to send some confidential data overinsecure channel it is mandatory to embed data in some host or cover media. While sending secure data using covermedia it necessary to encrypt as well as compress the cover media after compression embed confidential data.Reversible data hiding techniques are deployed in order to achieve the lossless and high quality embedding of very large images. It also ensures that the extraction of embedded information isdone the received images matches the original one. There are two sides to Reversible data hiding method. Separable Reversible data hiding and Non-Separable Reversible data hiding. This paper deals with the conceptof Reversible data hiding ,classification of Reversible data hiding, performance parameters to check the quality of Reversible data hiding methods and survey on various techniques developed by many researchers.*

KEYWORDS-Reversible data hiding, Encryption, Decryption.

I. INTRODUCTION

Data hiding has gotten very much attention from the research group in the past for more than 2 years. By this particular method, it could embed secret dataright into a cover medium, and afterwards enable the intendeduser to draw out the embedded data from the marked medium for different uses. However, for the majority of datahiding techniques, the cover medium continues to be distortedduring the data embedding operation and hence can't be restored into its first form after data extraction.In some very sensitive scenarios, such everlasting distortionis absolutely forbidden and the precise recovery of the first coverage medium is needed. To solved thisproblem, reversible data hiding (RDH) also known as losslessor perhaps invertible data hiding, is actually suggested losslessly recover the embeddeddata as well as the cover medium. Thatis actually, with the RDH, aside from the embedded data, thecover medium could be really recovered from the marked data too. The very first RDH algorithm is theone suggested by Barton in a US patent in 1997. Heproposes to embed the authentication data intoa digital medium, as well as allow primary users to extractthe embedded authentication details for confirming the authenticity of the received data.

II. RELATED WORKS

Additionally, there are a selection of works on data hiding in the encrypted url. In a buyer-sellerwatermarking protocol [6], the seller of digitalmultimedia item encrypts the original information usinga public key, and then permutes and embeds anencrypted fingerprint supplied by the customer in the encrypted url. After decryption with a privatekey, the customer will attain a watermarked product.

This protocol guarantees that the seller can't knowthe buyer 's watermarked model while the customer can't understand the first version. An anonymousfingerprinting scheme which improves the encipheringprice by exploiting the Okamoto-Uchiyama encryption technique has been recommended in [7]. Byintroducing the composite signal representationmechanism, the computational overhead andthe larger communication bandwidth because of thehomomorphic public-key encryption are usually substantially reduced [8]. In another sort of jointdata-hiding as well as encryption schemes, an aspect of coverinformation can be used to carry the extra email and themajority of the information are actually encrypted, to ensure that both the copyright and the privacy could be protected. Forexample [9], the intraprediction mode, motionvector difference and symptoms of DCT coefficients areencrypted, while a watermark is actually embedded into the amplitudes of DCT coefficients. In [10], the coverdata in high as well as lower bit-planes of transform

domain are respectively encrypted as well as watermarked. In [11], the content material proprietor encryptsthe symptoms of host DCT coefficients as well as each contentuser uses a completely different element to decrypt just a subset ofthe coefficients, so that a number of versionscontaining different fingerprints are produced for the users.

The reversible datahiding in encrypted impression is actually examined in [12]. The majority of the job on reversibledata hiding concentrates on the information embedding/extracting on the simple spatial url [13]-[17]. But, in several apps, an inferiorassistant or perhaps a channel administrator hopes to appendsome additional email, like the origininformation, image notation or perhaps authentication data,within the encrypted picture though he doesn't understand the first picture content. And it's alsooptimistic that the first content ought to berecovered with no error after picture decryption as well as sales message extraction at receiver side.

In recent years, signal processing in theencrypted domain has attracted considerableresearch interest. As an effective and popular meansfor privacy protection, encryption converts theordinary signal into unintelligible data, so that thetraditional signal processing usually takes placebefore encryption or after decryption. However, insome scenarios that a content owner does not trustthe processing service provider, the ability tomanipulate the encrypted data when keeping theplain content unrevealed is desired. For instance,when the secret data to be transmitted areencrypted, a channel provider without anyknowledge of the cryptographic key may tend tocompress the encrypted data due to the limitedchannel resource.

In some existing joint data-hiding andencryption schemes, a part of cover data is used tocarry the additional message and the rest data areencrypted. For example, the intra-prediction mode,motion vector difference and signs of DCTcoefficients are encrypted, while a watermark isembedded into the amplitudes of DCT coefficients.In the cover data in higher and lower bit-planes oftransform domain are respectively encrypted andwatermarked. In the content owner encrypts thesigns of host DCT coefficients and each contentuser uses a different key to decrypt only a subset ofthe coefficients, so that a series of versionscontaining different fingerprints are generated forthe users. In these joint schemes, however, only apartial encryption is involved, leading to a leakageof partial information of the cover. Furthermore, theseparation of original cover and embedded datafrom a watermarked version is not considered. Ineach sample of a cover signal is encrypted by apublic-key mechanism and a homomorphic propertyof encryption is exploited to embed some additionaldata into the encrypted signal. But the data amountof encrypted signal is significantly expanded andthe computation complexity is high. Also, the dataembedding is not reversible.

In the existing Reversible techniques one can hidethe secret data in one or two bits of an image. Whenthe secret data is hided in three or more bits of theimage its quality becomes low and the human eyecan detect the changes in the image. Hence, its datacarrying capacity and the tamper resistance orsecurity is low. Due to the disadvantages above, thesecret data is embedded in two or more bits of theimage using LSB and this increases the capacity i.e)large amount of information can be embedded in thecover medium. Also, secret data is embedded usingincrement and decrement technique and thisincreases the security i.e) hacker’s inability to detectthe secret data. Also the quality of the stego imageis much better when compared to the existingtechniques.

Also In LSB, the least significant bit of each pixelfor a specific color channel or for all color channelsis replaced with a bit from the secret data. Althoughit is a simple techniques, but the probability ofdetecting the hidden data is high. SCC technique isan enhancement. The color channel, where thesecret data will be hidden in, is cycling frequentlyfor every bit according to a specific pattern. Forexample, the first bit of the secret data is stored inthe LSB of red channel, the second bit in the greenchannel, the third bit in the blue channel and so on.This technique is more secure than the LSB but stillit is suffers detecting the cycling pattern that willreveal the secret data. Also it has less capacity thanthe LSB.

Obviously, most of the existing data hidingtechniques are not reversible. For instance, thewidely utilized spread-spectrum based data hidingmethods are not invertible owing to truncation (forthe purpose to prevent over/underflow) error andround-off error. The well-known least significant bit(LSB) plane based schemes are not lossless owingto bit replacement without “memory.” Anothercategory of data hiding techniques, quantizationindex-modulation (QIM)based schemes are notdistortion-free owing to quantization error.

III. REVERSIBLE DATA HIDING

Reversible data hiding is actually the method of concealing the essential details behind the pictures for secret data reception. the strategy to conceal the excess email into the cover press by an it's an it'sreversible fashion, i.e. after extraction of received picture we might create the picture exact same as the genuine (original) reputation and certainly will read through the idea hide behind it. Initially we encrypt the messagefrom the sender aspect and after that at the receiver aspect the real (original) note may be recovered [3].

In this particular strategy first the content material proprietor encrypts the first content before passing it to the information hider for further transmission. The information hider then add some additional details in the picture byapplying several data hiding techniques and pass it to the receiver aspect. The receiver aspect then extractthe encoded email and certainly will recoup the image exact same as the real (original) picture. Thefunctionality of a reversible information hiding algorithm may be driven on the foundation of followingtolls:-

1) Payload capability limit
2) Visual quality
3) Complexity

A. Separable Reversible Data Hiding

The type of reversible data hiding is actually the separable reversible details hiding. Here the separable means to distinct i.e. individual in other words we may separate something. The primary strategy ofseparable reversible data hiding is the fact that we are able to extract the real picture by utilizing the encryption element as well as the extraction of the payload by utilizing the information hiding key.One and some other i.e. both the areas are actually separated from one another. It means if we've the datahiding crucial then we could extract the unseen i.e. secret data but can't reassemble the originalpicture of course, if we've the encryption key then we could create the image exact same as the real image but can't read through the secret information. We need to have both of the secrets to check out the entire receiveddata[4].

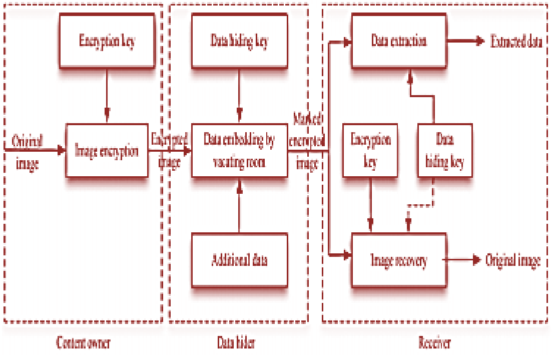

Fig.1. separable Reversible Data hiding

B. Non-Separable Reversible Data Hiding

Another approach of reversible data hiding is non-separable Reversible Data hiding. In thismethod first the content legatee encrypts the image using encryption key then passes it to the datahider. The data hider then embedded some supplementary i.e. additional data in the image usingthe data hiding key. Here, the main characteristic of Non-Separable Reversible Data hiding isdifferent from Separable

Reversible data hiding. At the receiver point we need both the keys i.e.encryption key and the data hiding key to extract the genuine data and the genuine image [5].

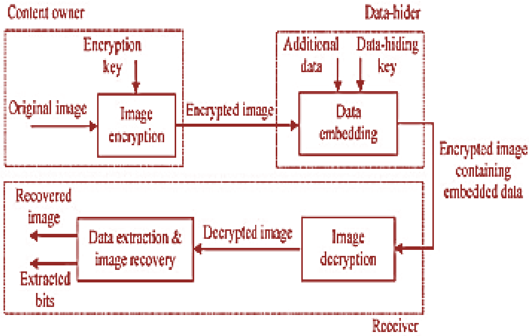

Fig.2. Non-separable reversible data hiding in encrypted Image

A. Image Encryption

The sender selects the file and applies his encryption algorithm to encrypt the image. Encryptionis the method of applying or altering some of the attributes of the genuine (original) image to forma very different image. Nobody can read the accurate (exact) image if he is unknown of thechanged done by the content owner [6].

B. Data Embedding

After encrypting the image the sender embed some supplementary i.e. additional data behind theselected part of the image before transmission. Any kind of image can be selected for theencryption like JPEG, PNG or BMP.

C. Data Extraction

This is the action implemented at the receiver side. After receiving the data, the main work of thereceiver is to extract the original data hide behind the image. This approach is known as dataextraction.

D. Image Recovery

Image recovery is the technique of decrypting the received image. The main action is to generatethe image same as the original image. And this is done by the reversibly perform the encryptionaction i.e. by using the decryption key.

The quality of the encrypted image is measured by calculation of certain evaluation measurementmetrics. These metrics gives the comparison ratio between the original image and the modifiedimage. The quality may be assessed on the basis of these values. The metrics used in this paperare as follows: Mean Square error (MSE), peak signal- to-noise ratio (PSNR), Number Of PixelChange Rate (NPCR) and Embedding ratio in BPP.[7] [8]

A. Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. TheMSE can be defined as the measurement of average of the squares of the difference between theintensities of the Encrypted image and the original image. It is popularly used because of themathematical tractability it offers. A large value for MSEmeans that the image is of poor quality.

B. Peak signal to noise ratio (PSNR)

The PSNR [5] depicts the measure of reconstruction of the encrypted image. This metric is usedfor discriminating between the cover and encrypted image. The advantage of this measure is easycomputation.

C. Number of Pixel Change Rate(NPCR)

Attacker tries to find out a correlation between the plain image and the cipher-image, by studyinghow differences in an input can affect the resultant difference at the output in an attempt todetermine the key. Trying to make a slight change such as modifying one pixel of the encryptedimage, aggressor (attacker) observes the change of the plain-image.

D. Payload

We use the different techniques to hide the data behind the image. The data which we want tohide behind the image is known as the payload. If we want to hide more data behind the imagewe need more space for. There are many methods which provides the high payload capacity.

IV. CONCLUSION

With this paper, we offered the initiatives of different researchers in the area of reversible data hiding. RDH is actually on the list of main methods of datahiding in image processing. Reversible datahiding schemes consists of image encryption, data and data hiding extraction/ picture recovery phases. Since the sturdiness of the RDH method hinges primarily on 3 elements - robustness,imperceptibility amount in the stegoimage, and embedding data. The RDH system leavesspecial patterns on the cover pictures and the patterns feats the steganalyst.

When the dimensions of thesecret message is actually tiny, the transform domain name grounded methods like DCT, DWT and adaptiveRDH are not less susceptible to steganalysis. In this particular strategy the distortion is going to be also less becauseembedding is carried out in transform domain. All the above mentioned issues have to be resolved whiledesigning a RDH method that ought to be powerful to attacks. We have to build up RDHtechniques exactly where we are able to embed data equal or even much more than existing strategies and without a distortion in stegoimage so that the security of the note could be increased.

REFERENCES

[1] Nosrati,RonakKarimi Mehdi Hariri,” Reversible Data Hiding:Principles, Techniques, and Recent Studies”.World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222-2510©2011 WAP journal.www.waprogramming.com.

[2] Mr P. S. Nalwade ,MsPoojaPrabhakarPetkar ,” A Survey on Reversible Data Hiding Techniques “, IJCTA May-June 2014.

[3] Kede Ma, Weiming Zhang, XianfengZhao,”Reversible Data Hiding in Encrypted Images by Reserving RoomBefore Encryption”, IEEE transactions on information forensics and security, vol. 8, no. 3, march 2013.

[4] V. Suresh, C. Saraswathy,” Separable Reversible Data Hiding Using Rc4 Algorithm” IEEE InternationalConference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 2013.

[5] San Diego, California, USA “Applications of Digital Image Processing”, Part of the SPIE InternationalSymposium on Optical Engineering and Applications, 10-14 August 2008.

[6] ZaidoonKh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi,” Overview: Main Fundamentals forSteganography “, journal of computing, volume 2, issue 3, March 2010.

[7] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans.Circuits Syst. VideoTechnol,vol. 16, no. 3, pp. 354–362, Mar.2006.

[8] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding-new paradigm in digital watermarking,” Eur.Assoc. Signal Process. J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.

[9] J. Tian, Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol,vol. 13, no. 8, Aug 2003, pp. 890-896.

[10] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,"IEEE Trans. Circuits Syst. Video Technol, vol. 17, no. 6, Jun 2007, pp.774-778.

[11] D. Kundur and K. Karthik, “Video fingerprinting and encryption principles for digital rightsmanagement,” Proceedings IEEE, vol. 92, no.6, pp. 918–932, Jun. 2004.

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

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

[14] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su,“Reversible data hiding,” IEEE Trans. Circuits Syst.Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E.Saber, "Lossless generalizedLSB data embedding," IEEE Trans. ImageProcess., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[16] W. Hong, T.-S.Chen, Y.-P.Chang, and C.-W.Shiu, "A high capacity reversible data hidingscheme using orthogonal projection and predictionerror modification," Signal Process., vol. 90, pp.2911–2922, 2010.

[17] C.-C. Chang, C.-C.Lin, and Y.-H. Chen,"Reversible data-embedding scheme usingdifferences between original and predicted pixelvalues," IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[18] A. Mayache, T. Eude, and H. Cherifi, "Acomparison of image quality models and metricsbased on human visual sensitivity," in Proc. Int.Conf. Image Processing (ICIP'98), Chicago, IL,1998, vol. 3, pp.

Authors:

M.RamaRao pursing M.Tech in Computer Science in Department of Computer Science and Engineering at S.R. Engineering College.

P.Kumaraswamy is an Assistant professor in Department of Computer Science and Engineering at S.R. Engineering College and has 11 years of experience in Academics. His research activities are in the area of data mining, Cloud Computing etc.