An Extensive Survey of Literature on Secure Reversible Image Data Hiding Over Encrypted Domain

Pallavi Dixit[1], Prof. Bhupendra Sen[2], Prof. K K Nayak[3]

[1]Mtech. Scholar, [2]Research Guide, [3]HOD

Department of Electronics and Communication Engineering, BIST, Bhopal

Abstract- This is the digital information revolution era. It has heralded connectivity, i.e. connectivity over the Internet and connectivity through the wireless network. The development of high speed computer networks and that of internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities in the form of electronic publishing and advertising, real-time information delivery. Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The intended message to be sent is called plain text message and the disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. In order to avoid raising the suspicions of eaves-droppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically. This work presents an extensive review of literature on secure reversible image data hiding.

Keywords- Data Hiding, Cryptography,Reversible Image Data Hiding,Encrypted Domain,Feature extraction,steganography, Watermarking.

I. INTRODUCTION

Now a day's digital media is being immensely used in various type of applications such as medical, military, law enforcement, fine art work protection and so on. Security is the main concern which is to be taken care of while transferring confidential data on the Internet. Since text, images, audio, video are the part of digital data that are transferred over open public network so there is need to protect this digital data. From the last few decades, various methods have been developed to enforce security in various types of applications. Generally, two methods are used to secure the data i.e. cryptography and data hiding.

The boom in the information age is not without its adverse effects though. Copying is simple with no loss of fidelity. A copy of a digital media is identical to the original. This has in many instances, led to the use of digital content with malicious intent. One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called digital signature or copyright label or watermark that authenticates the owner of the data. With the ease of editing and perfect reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) have become important concerns. Data hiding, schemes to embed secondary data in digital media, have made considerable progress in recent years and attracted attention from both academia and industry. Techniques have been proposed for a variety of applications, including ownership protection, authentication and access control. Imperceptibility, robustness against moderate processing such as compression, and the ability to hide many bits are the basic but rather conflicting requirements for many data hiding applications.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. A message in cipher text might arouse suspicion on the part of the recipient while an ”invisible” message created with steganographic methods will not. Anyone engaging in secret communication can always apply a cryptographic algorithm to the data before embedding it to achieve additional security. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered.

Data hiding technique s used for copyright protection, temper detection, covert communication, data integrity etc. It is generally accepted that a data hiding technique must possess following two important properties:

- Imperceptibility
- Embedding capacity

Embedding process and extracting process are the two main processes of data hiding. In embedding process, secret data is embedded into cover media. Cover media is modified after embedding the secret data. This modified

cover media which contain secret data is known as marked data. Secret data is extracted from the marked data and recovers the original cover media.

A traditional data hiding system, shown in Fig. 1.1, includes embedder and extractor. The input to the embedder is multimedia data and secret data, which is to be embedded into original multimedia data. The output of embedder is marked data.

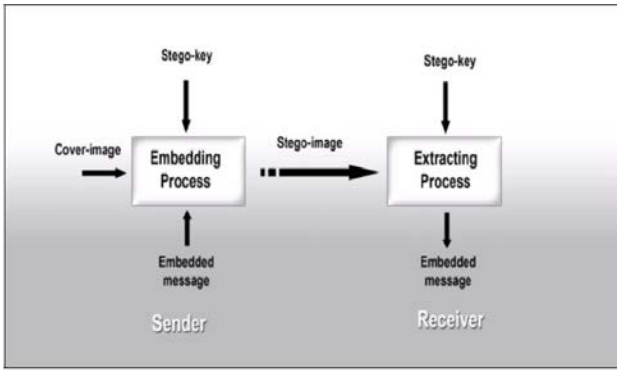

Figure 1.1Generelized data hiding System.

II. REVERSIBLE DATA HIDING

Digital watermarking often referred to as data hiding. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as lossy data hiding. Here, let us examine three major classes of data hiding algorithms. With the most popularly utilized spread-spectrum watermarking techniques, either in DCT domain or in block 8x8 DCT domain, round-off error and/or truncation error may take place during data embedding. As a result, there is no way to reverse the stego-media back to the original without distortion. For the least significant bit-plane (LSB) embedding methods, the bits in the LSB are substituted by the data to be embedded and the bit-replacement is not memorized.

Reversible watermark is a special subset of fragile watermark. Like all fragile watermarks, it can be used for digital content authentication. But reversible watermark is much more than content authentication. It has an additional advantage that when watermarked content has been detected to be authentic, one can remove the watermark to retrieve the original un-watermarked content.

Reversible watermarking can be classified into SSR (strict sense reversible) and WSR (wide sense reversible). A watermark is SSR if once it has been decoded/detected it can also be removed from the host asset, thus making it possible the exact recovery of the original asset. A watermark is WSR if once it has been decoded /detected it can be made undecodable/undetectable without producing any perceptible distortion of the host asset.

In reversible watermarking, a watermark is embedded in a digital image I. This results in a watermarked image I'. This image might or might not have been tampered by some intentional or unintentional attack. The watermark can be removed from I' to restore the original image, which results in a new image I"([provided no tampering has taken place). By definition of Reversible watermark the restored image I" will be exactly same as the original image I, pixel-by-pixel, bit-by-bit. Fig. 2.1 illustrates Reversible Watermarking Scheme.

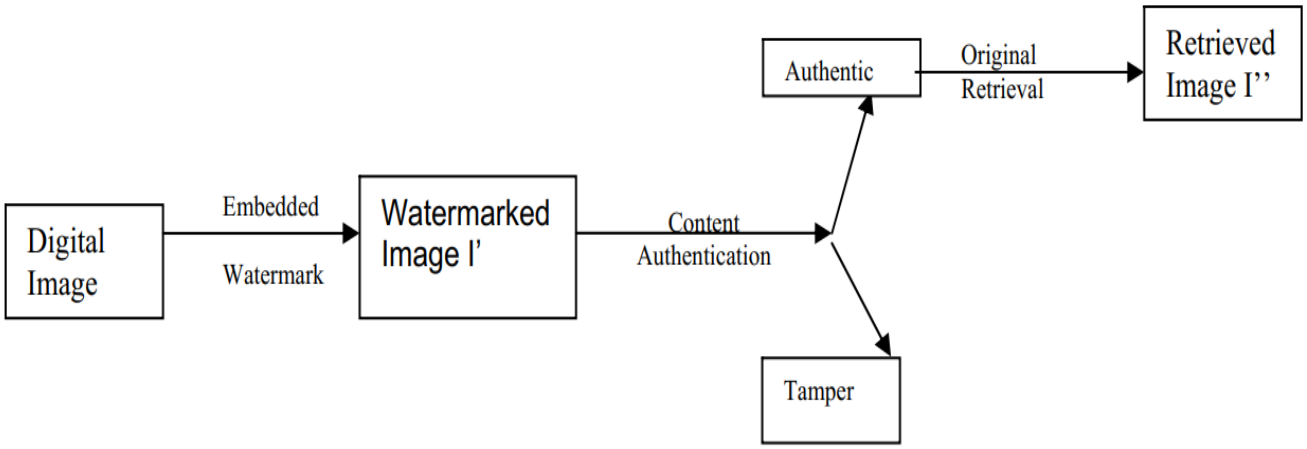

Figure 2.1 A Reversible Data Hiding Scheme.

One basic requirement of digital watermarking is its imperceptibility, embedding a watermark inevitably changes the original content. Even a very slight change in pixel values may not be desirable in sensitive imagery, such as military data, medical data and data used in crime detection. In such scenario, every bit of information is important. Any change will affect the intelligence of the digital content, and the access to the original, raw data is always required. Reversible watermarks will provide the original, raw data for digital content authentication.

III. RELATED WORK

SR. NO.	TITLE	AUTHOR	YEAR	APPROACH
1	Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation,	J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au and Y. Y. Tang,	2016	Anovel reversible image data hiding scheme over encrypted domain.
2	Reversible data hiding with image bit-plane slicing,	H. Nyeem,	2017	Instead of directly embedding in an input image, to embed in a pair of bit-plane sliced images of the input image
3	Secure data transmission through reversible data hiding,	L. Tomy and Namitha T N,	2016	XOR ciphering technique used for encryption and decryption process
4	Reversible Data Hiding in Cloud Based Applications,	N. N. Chendulkar and P. S. Mahajani,	2015	A novel technique is proposed termed as reversible data hiding (RDH) by which can hide data
5	Data Compression and Hiding Using Advanced SMVQ and Image Inpainting,	Y. Y. Satpute and B. A. Tidke,	2015	Side-match vector quantization and image in painting is used for an integrated data-hiding and compression scheme that is used for digital images.
6	Data hiding technique by using RGB-LSB mechanism	V. Agham and T. Pattewar,	2014	A novel scheme for separable reversible data hiding in encrypted domain in which we use image as a cover medium and image as a data to be hid.
7	Reserve Room based Reversible Data Hiding in digital images,	T. S. K. Shripriyadharshini, S. yohalakshmi and S. Deepa,	2014	Novel method of Reserving Room before Encryption with traditional RDH algorithm

J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au and Y. Y. Tang,[1] This exploration proposes a novel reversible image data hiding scheme over encrypted domain. Data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and nonencrypted image patches, allowing us to jointly decode the embedded message and the original image signal. Compared with the state-of-the-art methods, the proposed approach provides higher embedding capacity and is able to perfectly reconstruct the original image as well as the embedded message. Extensive experimental results are provided to validate the superior performance of our scheme.

H. Nyeem,[2]Utilizing bit-plane slicing, a novel approach for reversible data hiding (RDH) is introduced in this exploration. Instead of directly embedding in an input image, we propose to embed in a pair of bit-plane sliced images of the input image. Specifically, an (m + n)-bit input image is subdivided in two lower intensity images, i.e., n-bit image using n-LSB planes and m-bit image using m MSB planes. Embedding in a lower intensity image would offer relatively higher embedding rate, since the pixel-counts of the highest bin in the image histogram would be much higher than that of the original image. Moreover, embedding in the n-bit image would cause lower embedding distortion, while that in the m-bit image

should contribute to a higher contrast enhancement. After embedding, histogram shifting (HS)-based embedding, those two images can be combined to get the (m+n)-bit embedded image. Comparing with a prominent HS-based RDH scheme, the proposed scheme has demonstrated significantly higher embedding rate and better contrast-enhancement.

L. Tomy and Namitha T N,[3]Data hacking is very difficult to deal with today's electronic world. There are large numbers of technique used, for the secure

communication of data. Images are widely used in different-different processes. So data hiding is used in the encrypted image, but the main problem is that distortion at the time of data extraction. Reversible data hiding in encrypted image is used to solve this problem. SDS Algorithm gives more security to secret data. RDH recovers the original image after the extraction of the embedded data. In this work, XOR ciphering technique used for encryption and decryption process. All existing mechanisms embed data by reversibly vacating room after the encrypted images. However, this may result in some errors on data extraction and/or image restoration. In this work, we suggest a method by holding a space before encryption with a RDH algorithm. Thus, the data hider can embed data in the encrypted image. The embedded data can be data or image. Both data extraction and image recovery will be formed without any error. The transmission and exchange of image also demands high security. Cryptography is used to maintain security.

N. N. Chendulkar and P. S. Mahajani, [4]Now-a-days many unauthorized users try to get the protected information and therefore it is necessary to secure our data. Besides, there are also scenarios that data hiding needs to be done in the encrypted domain or combined with the encryption, especially in the age of big data and cloud computing. In previous method first encryption was done and then the room was vacated to hide the data. But there were some errors in data extraction and image recovery. In this exploration a novel technique is proposed termed as reversible data hiding (RDH) by which we can hide our data. RDH is applied to encrypted images by which we can properly recover our data and the cover image. The hidden data can be in the form of text or image. In the proposed method we first vacate room to hide data and after encrypting image using certain encryption key the data hider reversibly hides the data whether text or image using data hiding key. In previous method only text was hidden. But the proposed work is extended to hide the image also in the same reserved space which was used to hide text. The hidden image is also recovered without any errors. The results given in the workproves that we can exactly recover the hidden data, hidden image and the cover image as and when needed by the receiver. The traditional RDH algorithm used is histogram shifting. By this method we can properly recover hidden data and cover image without any errors. Large amount of data can be hidden as compared to previous method.

Y. Y. Satpute and B. A. Tidke, [5] Data hiding is a process that includes converting the secret data like a video file, an audio file, an image, etc. Into cover data. It is popularly used in various applications like medical fields, military applications, etc. The reversible data hiding is nowadays the most used research area in the field of secret data hiding. In this project, side-match vector quantization and image in painting is used for an integrated data-hiding and compression scheme that is used for digital images. A combined data hiding and compression technique which is based on SMVQ (side-match vector quantization) and image in painting is proposed. Two functions, data hiding and image compression can be integrated into one single code to secure the private data more efficiently.

V. Agham and T. Pattewar, [6]Internet is the most popular communication medium now a days but communication over the internet is facing some problem such as data security, copyright control, data size capacity, authentication etc. Separable reversible data hiding technique means separating two major activities in the scheme. These two activities are getting the exact recovery of the secure hidden data and exact recovery of cover data. Here we introduce a novel scheme for separable reversible data hiding in encrypted domain in which we use image as a cover medium and image as a data to be hid. The scheme's main feature is the way of data embedding into the encrypted cover image. Here we are concentrating on using RGB-LSB method for data embedding and finally verifies the performance of using RGB-LSB method in terms of Quality index Q, PSNR etc.

T. S. K. Shripriyadharshini, S. yohalakshmi and S. Deepa, [7] In Reversible Data Hiding (RDH), original cover can be losslessly restored after the embedded data has been extracted. This work proposes the novel method of Reserving Room before Encryption with traditional RDH algorithm. In the first phase, the content owner embeds the secured data in the reserved room using data hiding key. This modified stegoimage is encrypted using an Encryption key. Both Data hiding key and encryption key are used at the receiver section to restore the original image and data embedded in it. Experimental results show that this proposed method achieves real reversibility, better image quality.

IV. PROBLEM IDENTIFICATION

Secret information is embedded in cover media and at the time of extraction, secret information is extracted along with cover media exactly same as before embedding. Reversible techniques are used to recover the cover media from marked media by extracting secret media. Cover media is as important as secret media in many areas such as medical, military etc.A basic approach of reversible watermarking algorithms is to select an embedding area in an image, and embed both the payload and the original values in this area. As the amount of information needed to be embedded (payload and original values in the original area) is larger than that of the embedding area,most reversible watermarking techniques rely on loss less data compression on the original values in the embedding area,

and the space saved from compression is used for embedding the payload.

V. CONCLUSION

In the information era, multimedia content (e.g, audio, image, video and 3D computer graphics models) in digital form is being used in a wide range of application areas. However, at the same time, an increasing number of security problems have been revealed.For instance, the proliferation of intelligent editing tools can also facilitate misuse, illegal copying and distribution, plagiarism and misappropriation, which could seriously ruin the interests of the creator or owner of the multimedia work.This work presents a survey of literature on data hiding. In addition, a few other important problems encountered in practice, such as the requirement for reversibility of the original data after the watermark has been extracted, have been also discussed in brief.Steganography and watermarking differ in a number of ways including purpose, specification and detection/extraction methods. The most fundamental difference is that the object of communication in watermarking is the host signal, with the embedded data providing copyright protection. In steganography the object to be transmitted is the embedded message, and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability.

REFERENCES

[1]. J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au and Y. Y. Tang, "Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, March 2016.

[2]. H. Nyeem, "Reversible data hiding with image bit-plane slicing," 2017 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, 2017, pp. 1-6.

[3]. L. Tomy and Namitha T N, "Secure data transmission through reversible data hiding," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-4.

[4]. N. N. Chendulkar and P. S. Mahajani, "Reversible Data Hiding in Cloud Based Applications," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 1141-1146.

[5]. Y. Y. Satpute and B. A. Tidke, "Data Compression and Hiding Using Advanced SMVQ and Image Inpainting," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 1074-1077.

[6]. Agham and T. Pattewar, "Data hiding technique by using RGB-LSB mechanism," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-5.

[7]. T. S. K. Shripriyadharshini, S. yohalakshmi and S. Deepa, "Reserve Room based Reversible Data Hiding in digital images," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, 2014, pp. 1452-1456.

[8]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[9]. M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042–1049, Apr. 2006.

[10]. 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.

[11]. X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091–1100, Jul. 2013.

[12]. C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao, "An inpainting- assisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109–1118, Jul. 2013.

[13]. W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906–910, Jun. 2009.