2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS)

Comparative Study on Different Reversible Image Data Hiding Techniques

Anisha Jose
M.Tech, Computer Science and Engineering
Nehru College of Engineering and Research Centre
Thrissur, Kerala, India
anisha.153@hotmail.com

Mary Mareena
Assistant Professor, Computer Science and Engineering
Nehru College of Engineering and Research Centre
Thrissur, Kerala, India
pvmareena@gmail.com

Saritha K
Assistant Professor, Computer Science and Engineering
Nehru College of Engineering and Research Centre
Thrissur, Kerala, India
saritha.cse@ncerc.ac.in

Abstract— Reversible steganography, also called reversible data hiding in digital images has been studied extensively in recent years. Reversible Image Data Hiding (RIDH) is a category of data hiding technique that ensures perfect reconstruction of cover image upon the extraction of the embedded message. The property of reversibility means that the original image can be recovered completely after the embedded bits are extracted. The main focus is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. This paper compare and analyses the different methods which has been used for reversible image data hiding over several years. Also, proposes a novel Reversible Image Data Hiding (RIDH) scheme over encrypted domain. A public key modulation mechanism is applied to achieve data embedding, in which access to the secret encryption key is not needed. A powerful two-class SVM classifier is designed at the decoder side to distinguish encrypted and non-encrypted image blocks, which allows to decode the embedded message and the original image signal jointly. Compared with the state-of-the-arts, the proposed technique provides higher embedding capacity, and is able to reconstruct the original image as well as the embedded message perfectly.

Keywords— Reversible image data hiding, public key modulation, SVM classifier.

I. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes important for many applications especially in confidential transmission, video surveillance, military and medical applications. The protection of multi-media data can be done with encryption or data hiding algorithms. Data hiding is a technique to embed additional data into digital multimedia by altering the cover signals slightly. When the data hiding is performed in a reversible manner, the original cover content can be restored perfectly after data extraction at receiver side. Reversible data hiding method embeds a piece of information into the host images and generate the marked one. After extracting the embedded data, the original image can be exactly recovered. Reversible data hiding can be used in many fields such as medical, military, and legal applications, which do not allow modifications in the digital representation of the cover image due to confidentiality issues.

The reversible data hiding methods can be classified into three types: the difference expansion methods, histogram modification methods, and lossless compression based methods. In the difference expansion methods, the differences between two adjacent pixels are doubled which generates a new least significant bit (LSB) plane for embedding the additional information. The histogram modification methods shift the histogram of cover data from its peak point towards its zero points, and utilize the cover data at the peak point of histogram to carry the additional data. The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression to spare space for accommodating the additional.

Most data hiding methods embed messages into the cover media to generate marked image by modifying only the LSB of the cover image. The embedding process will usually have low embedding capacity and also introduce permanent distortion of original image. That is, the original cover can never be reconstructed image from the marked cover. In the medical imagery, military imagery, and law forensics, these type of degradation in original cover is not allowed. Therefore a special kind of data hiding method is needed, which is Reversible Data Hiding (RDH) or lossless data hiding. The original cover can be restored reversibly after the extraction of embedded message.

Figure 1 shows the overall block diagram of reversible data hiding process. At the sender side, a secret data which is shared between the sender and receiver, is embedded into the

978-1-5090-3294-5/17/$31.00 ©2017 IEEE

host image. This image with secret data is now transmitted to the receiver side, where the data extraction is taken place and the host image is reconstructed.

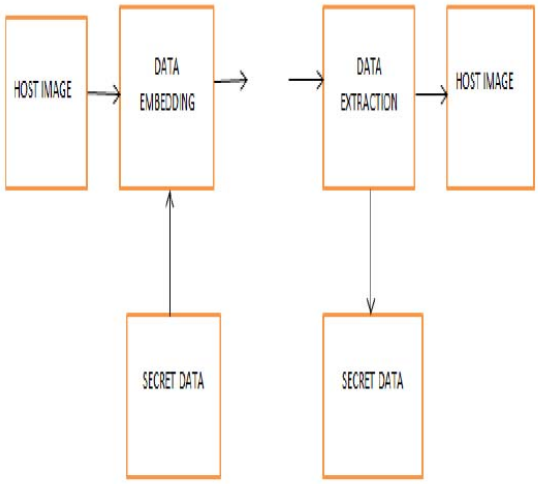

Fig. 1. Reversible Data Hiding Process

Most of works on reversible data hiding is applied on unencrypted domain. In some practical scenarios, a content owner encrypts the original images as unintelligible data for privacy protection. In the field of secure remote sensing and Cloud computing, the parties who process the image data are un-trusted. All images will be encrypted before forwarding to an un-trusted third party for further processing so as to protect the privacy and security.

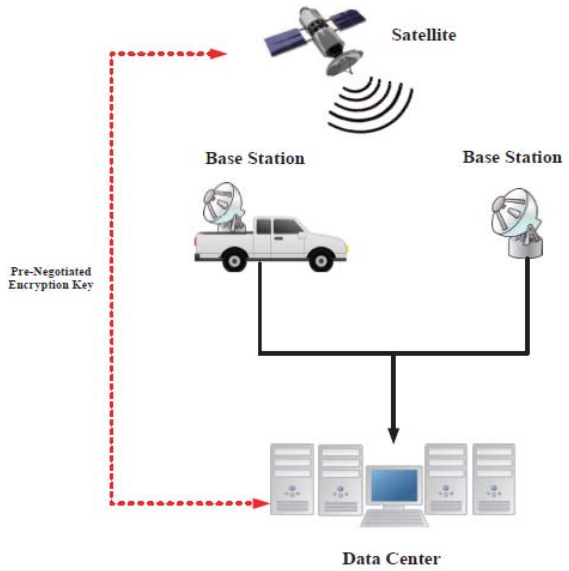

Fig. 2. Image data hiding in the scenario of secure remote sensing.

In secure remote sensing, the satellite images captured by on-board cameras, are encrypted and then sent to the base station, as illustrated in Fig 2. The base station embeds a confidential message, such as the base station ID, location information, time of arrival (TOA), local temperature, wind speed, etc., into the encrypted images. Now, the encrypted image which contains the additional message is transmitted to a data center over a public network for further investigation and storage. Any base station, for security reasons, has no privilege of accessing the secret encryption key pre-negotiated between the satellite and the data center. Therefore, it is clear that the message embedding operations have to be conducted entirely over the encrypted domain.

II. LITERATURE SURVEY

Mehmet Utku Celik *et. al.* [1] presents a lossless (reversible) data-embedding technique, which enables the recovery of original host signal after the extraction of embedded information. Here the work proposes a generalization of the well-known least significant bit (LSB) modification as the data-embedding method that introduces additional operating points on the capacity-distortion curve. It compresses a portions of the signal that are susceptible to embedding distortion and transmits these compressed descriptions as a part of the embedded payload. In this way, lossless recovery of the original is achieved. A prediction-based conditional entropy coder utilizes unaltered portions of the host signal as side-information which improves the compression efficiency. The lossless embedding step produces a watermarked signal in which the message data is embedded by taking the host signal and the message data as the input. The watermarked signal is used for data extraction and recovery process, to exactly extract the embedded data and to recover the original host signal. The LSB of each signal sample is replaced by a payload data bit. Two or more LSBs may be over written if additional capacity is required. During extraction, these bits are read in the same scanning order so that the payload data can be reconstructed. LSB modification is a simple and non robust embedding technique. It provides a high-embedding capacity and small bounded embedding distortion. However, the method is irreversible, i.e., it results in a permanent distortion of host signal when its lowest levels containing the residual signal are replaced with the watermark signal.

Work by Chuan Qin *et. al.* [2] proposes a prediction-based reversible steganographic scheme based on image inpainting. According to the distribution characteristics of the image content, reference pixels are chosen adaptively. Then, the image inpainting technique is introduced to generate a prediction image which has similar structural and geometric information as that of cover image. Finally, the histogram of the prediction error is shifted to embed the secret bits reversibly. The embedded secret bits can be extracted from the stego image correctly, since the same reference pixels can be

exploited in the extraction procedure. Also, the cover image can be restored losslessly. A prediction process is conducted first to estimate the cover image pixels, and the prediction error, i.e., the difference between the cover image and the prediction result, is used to embed the secret data. The accuracy of the prediction result depends on choosing the reference pixels and how it is utilized for prediction. Here, the reference pixels are adaptively selected according to the distribution characteristics of the image. Fewer reference pixels are chosen in the smooth regions of the cover images, while more reference pixels are chosen in the complex regions. The PDE-based inpainting algorithm can effectively generate the prediction image that has the similar structural and geometric information as the cover image according to the chosen reference pixels.

In the paper proposed by William Puech *et. al*. [3], a reversible data hiding algorithm on encrypted images is applied which remove the embedded data before the image decryption. Reversible data hiding methods discussed so far are not applicable on encrypted images. In this paper, local standard deviation of the marked encrypted images is analyzed in order to remove the embedded data during the decryption step. If block encryption methods are applied to images, one can face three inconveniences. The first one is when there exist a homogeneous zones (regions with the same color), then all blocks in these zones are encrypted in same manner. The second problem is that block encryption methods are not robust to noise. The third problem is data integrity. However, the combination of encryption and data-hiding can solve these problems. The Advanced Encryption Standard (AES) algorithm consists of a set of processing steps repeated iterations called rounds which is dependent on the size of the key and the size of the data block. AES first perform an XORing of subkey with the block which is called the AddRoundKey step. Afterwards, the round operation is followed. Each regular round operation consist of four steps. In the SubBytes step, every byte of the block is replaced by a substitute in a substitution box (S-Box). The next is the ShiftRows step where the rows are shifted over different offsets in a circular manner. The next step is the MixColumns, where every column is multiplied with a matrix over the Gallois Field. Another AddRoundKey step is performed as the last step. In the proposed method, coding algorithm involves two steps which are the encryption and the data hiding step. For each block composed of n pixels, here apply the AES encryption algorithm by block. Same secret key is used for data encryption and data hiding. The decoding algorithm also involves two steps which are the message extraction and the decryption. The extraction of the message is just enough to read the bits of the pixels which are marked by using the secret key k and the same PRNG. But after the extraction, each marked cipher-text will remain marked. The problem is to decrypt the marked encrypted image. The removal of decryption is done by analyzing the local standard deviation during the decryption of the marked images.

The next paper proposed by Wien Hong *et. al.* [4], adopts a better scheme to measure the block smoothness. Then it uses the side-match scheme to decrease the error rate of extracted-bits. The evaluation of block smoothness favors a correct data extraction. The four borders of each block do not take part in the calculation of block smoothness. Therefore the correctness of data extraction may get decreased, especially when the block size is too small. Smoothness evaluation employs the summation of absolute of two neighboring pixels. Moreover, the message extraction and image recovery are performed starting from the noticeable change in smoothness to the least ones. It also adopts the side-match technique by concatenating the border of recovered blocks to the unrecovered blocks for the evaluation of block smoothness.

Xinpeng Zhang *et. al.* [5] proposes reversible data hiding scheme in encrypted images based on lossless compression of encrypted data. A stream cipher is used in the encryption phase to mask the original content. Then, a part of encrypted data in the cipher-text image is compressed using LDPC code, and then inserts the compressed data and the additional data into a part of encrypted data itself. Quality of decrypted image is satisfactory, since majority of the encrypted data are unchanged. A receiver who has the data-hiding key can extract the additional data and the compressed data successfully. The original image is encrypted by the content owner by using a stream cipher. Data hider may compress half of the 4th LSB of the encrypted image using LDPC code, even though he does not know the original content and the cryptographic key. Then insert the compressed data and the additional data into the encrypted image. The receiver can extract the additional data using the data-hiding key, also decrypt it using the cryptographic key to reconstruct the original version. If the receiver has both the data-hiding and cryptographic keys, he can further recover the original image without any errors.

III. PROPOSED SYSTEM

This work proposes a novel Reversible Image Data Hiding (RIDH) scheme[6] in encrypted domain. A public key modulation mechanism is performed to achieve data embedding, in which access of secret encryption key is not needed. A powerful two-class SVM classifier is used at the decoder side which is designed to distinguish encrypted and non-encrypted image blocks. This allows us to jointly decode the embedded message and as well as the original image signal. Compared with the state-of-the-arts, the proposed method provides higher embedding capacity. Also it ensures perfect reconstruction of original image and the embedded message.

Data embedding is done via public key modulation mechanism and data extraction is performed by exploiting the distinguishability of encrypted and non-encrypted image blocks. Since the decoding of the message bits and the original image is bind together, the proposed technique belongs to non-separable category of RIDH solutions. There uses the conventional stream cipher applied in the standard format as

the encryption algorithm. That is, the ciphertext is generated by bitwise XORing of the plaintext and the key stream. When stream cipher is used, the encrypted image is generated by,

$$[[f]] = Enc(f, K) = f \oplus K \quad \text{----- (1)}$$

where f and [[f]] denote the original and the encrypted images, respectively. Here, K is the key stream generated by using the secret encryption key. The original image is obtained by performing the following decryption function,

$$f = Dec([[f]], K) = [[f]] \oplus K \quad \text{----- (2)}$$

The encrypted image [[f]] serves as the cover to hold the message to be hidden. First step is to divide encrypted cover image into a series of non-overlapping blocks of size M×N. Each block is designed in such a way to carry n bits of message. If the number of blocks in the image is B, the embedding capacity becomes n * B bits. To enable efficient embedding, here generates $S = 2^n$ binary public keys Q_0, Q_1, …… ,Q_{S-1}, each having length L = M × N × 8 bits. These public keys are selected prior to the message embedding, according to the criterion of maximizing the minimum Hamming distance[7] among all keys.

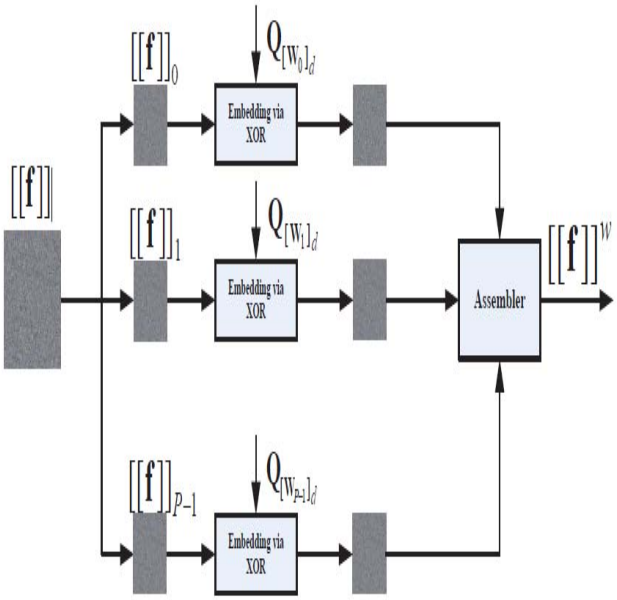

Fig. 3. Schematic diagram of data hiding over encrypted domain.

The decoder has the decryption key K, and tries to recover both the embedded message and the original image simultaneously without any distortions.

More specifically, S decoding candidates are created by XORing each block with all the S possible public keys Q_0, Q_1,…… ,Q_{S-1}.

$$\begin{aligned} \mathbf{f}_i^{(0)} &= \mathbf{f}_i^w \oplus \mathbf{Q}_0 = \mathbf{f}_i \oplus \mathbf{Q}_{[\mathbf{W}_i]_d} \oplus \mathbf{Q}_0 \\ \mathbf{f}_i^{(1)} &= \mathbf{f}_i^w \oplus \mathbf{Q}_1 = \mathbf{f}_i \oplus \mathbf{Q}_{[\mathbf{W}_i]_d} \oplus \mathbf{Q}_1 \\ &\vdots \\ \mathbf{f}_i^{(S-1)} &= \mathbf{f}_i^w \oplus \mathbf{Q}_{S-1} = \mathbf{f}_i \oplus \mathbf{Q}_{[\mathbf{W}_i]_d} \oplus \mathbf{Q}_{S-1} \end{aligned}$$

A two-class SVM classifier is used to identify the candidate corresponding to each block. SVM classifier classifies the encrypted and non-encrypted image patches. At the extraction phase, all the S possibilities are tried, and identify the one which generated structured image patches. Based on the index of the identified public key, the embedded message extraction is performed by converting the index i to its binary representation. Thus, the n bits of the message can be obtained. Finally, n bits from each block is combined to construct the original message.

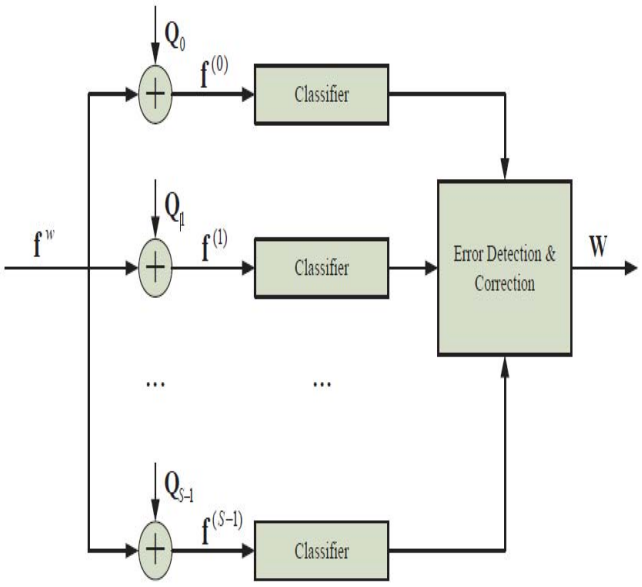

Fig. 4. Schematic diagram of the data extraction.

The proposed RIDH scheme designed over encrypted domain may also be extended to handle compressed and encrypted images. Also, this approach provides higher embedding capacity, and is able to reconstruct the original image and the embedded message perfectly.

The table below shows the comparison between various existing RIDH techniques and the proposed method.

TABLE I
COMPARISON OF DIFFERENT REVERSIBLE IMAGE DATA HIDING TECHNIQUES

Title	Method	Advantages	Disadvantages
Lossless Generalized-LSB Data Embedding	Compress certain image features in order to vacate room for message embedding. LSB of each signal sample is replaced by a data bit embedding one bit of data per input sample.During extraction, these bits are read in the same scanning order, and payload data is reconstructed.	Simple embedding technique	High distortion of host signal. Designed over plain text domain. Less secure.
An Inpainting-Assisted Reversible Steganographic Scheme using a Histogram Shifting Mechanism	Generate the prediction image effectively that has the similar structural and geometric information as the cover image. Reference pixels are chosen adaptively according to the distribution characteristics of the image content.The histogram of the prediction error is shifted to embed the secret bits reversibly.	Less distortion, Improves image quality	As the hiding capacity becomes greater, the visual quality of images degrades
A Reversible Data Hiding Method for Encrypted Images	Apply reversible data hiding algorithms on encrypted images. Data is embedded by flipping 3 LSB of half of the pixel in a block. Encryption and data hiding is done using a secret key.	Applicable on encrypted images	High computational complexity, Security of the system depends only on the secret key used
An Improved Reversible Data Hiding in Encrypted Images Using Side Match	Summation of the absolute of two neighbouring pixel is employed. Side match technique is employed to concatenate the border of recovered blocks to the unrecovered blocks and perform the smoothness evaluation of the concatenated blocks. Extraction and recovery are performed starting from the most noticeable changes in smoothness to the least ones.	Better performance for data extraction and image recovery	Error rate is high for larger blocks. Data extraction errors since local smoothness does not always hold for natural images.
Efficient Reversible Data Hiding in Encrypted Images	In encryption phase, content owner uses a stream cipher to mask the original content. Data hider compresses half of the 4^{th} LSB of encrypted image and inserts the compressed data as well as the additional data into the part of encrypted image itself. A receiver with the data-hiding key and the cryptographic-key can successfully extract the additional data and the compressed image.	Since the majority of encrypted data are kept unchanged, the quality of directly decrypted image is satisfactory	Makes the key management functions difficult in distributed infrastructure. Decoder requires a feedback channel which is very costly.
Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation	The 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 non-encrypted image patches, allowing us to jointly decode the embedded message and the original image signal.	Provides higher embedding capacity, able to perfectly reconstruct the original image as well as embedded message.	Time complexity is high

IV. CONCLUSION

In this paper, different reversible data hiding techniques are compared and a secure RIDH scheme operated over the encrypted domain is proposed. Even though some of the methods provides high embedding capacity, they incurs permanent distortion of host images. Also, the use of more secret keys makes the key management functions such as key generation, activation, de-activation, suspension and expiration, difficult in large distributed infrastructure. A public key modulation mechanism is proposed, which allows us to embed the message via simple XOR operations, which does not need the access to secret encryption key. A powerful two-class SVM classifier is used at the decoder side to discriminate between encrypted and non-encrypted image patches. This enables to jointly decode the embedded message and the original image signal perfectly. The proposed method is more efficient than the traditional RDH techniques for plain images and achieve excellent performance without any loss of secrecy.

REFERENCES

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

[2] 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, 2013.

[3] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding Method for encrypted images," in *Proc. of SPIE 6819*, 2008, pp. 1-9.

[4] T. Hong, W. Chen and H. Wu, "An improved reversible data hiding in encrypted images using side match, " *IEEE Signal Processing Lett.*, vol.19, no. 4, pp. 199-202, 2012.

[5] X. Zhang, Z. Qian, G. Feng, and Y. Ren,"Efficient reversible data hiding in encrypted images," *J. Vis. Commun. Image R.*, vol. 25, no. 2, pp. 322-328, 2014.

[6] Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au Yuan Yan Tang,"Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation," *IEEE Trans. On* Circuits and Systems for Video Technology, vol. 26, issue 3, pp.441-452,2015.

[7] J. MacDonald, "Design methods for maximum minimum-distance error correcting codes," *IBM J.*, pp. 43-57, 1960..