IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation

J. Malathi, T. Sathya Priya

M.Phil, Computer Science, Shri Sakthikailassh Women's College, Salem[1]

Asst. Professor, Computer Science, Shri Sakthikailassh Women's College, Salem[2]

Abstract: This work proposes a novel Reversible Image Data Hiding (RIDH) scheme over encrypted domain. The data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. Support Vector Machine (SVM) has been widely used in machine learning for data classification. It has high generalization ability which provides high reliability in real-world applications such as image processing, computer vision, text mining, natural language processing, bio-informatics and many more. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the signal or to show the identity of its owners. 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. Compared with the state-of-the-arts, 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.

Keywords: SVM, RIDH, Water marking

I. INTRODUCTION

Reversible Image Data Hiding (RIDH) is a special category of data hiding technique, which ensures perfect reconstruction of the cover image upon the extraction of the embedded message. The reversibility makes such image data hiding approach particularly attractive in the critical scenarios, e.g., military and remote sensing, medical images sharing, law forensics and copyright authentication, where high fidelity of the reconstructed cover image is required. The majority of the existing RIDH algorithms are designed over the plaintext domain, namely, the message bits are embedded into the original, un-encrypted images. The early works mainly utilized the lossless compression algorithm to compress certain image features, in order to vacate room for message embedding. However, the embedding capacity of this type of method is rather limited and the incurred distortion on the watermarked image is severe. Histogram shifting (HS)-based technique, initially designed by Ni et al. Is another class of approach achieving better embedding performance through shifting the histogram of some image features. The latest difference expansion (DE)-based schemes and the improved prediction error expansion (PEE)-based strategies were shown to be able to offer the state-of-the-art capacity distortion performance. Recently, the research on signal processing over encrypted domain has gained increasing attention, primarily driven by the needs from Cloud computing platforms and various privacy preserving applications.

This has triggered the investigation of embedding additional data in the encrypted images in a reversible fashion. In many practical scenarios, e.g., secure remote sensing and Cloud computing, the parties who process the image data are un-trusted. To protect the privacy and security, all images will be encrypted before being forwarded to an un-trusted third party for further processing. For instance, in secure remote sensing, the satellite images, upon being captured by on-board cameras, are encrypted and then sent to the base station(s), as illustrated in Fig. 1. After receiving the encrypted images, the base station embeds a confidential message, e.g., base station ID, location information, time of arrival (TOA), local temperature, wind speed, etc., into the encrypted images. Eventually, the encrypted image carrying the additional message is transmitted over a public network to a data center for further investigation and storage. For security reasons, any base station has no privilege of accessing the secret encryption key K pre-negotiated between the satellite and the data center. This implies that the message embedding operations have to be conducted entirely over the encrypted domain. In addition, similar to the case of Cloud computing, it is practically very costly to implement a reliable key management system (KMS) in such multi-party environment over insecure public networks, due to the differences in ownership and control of underlying infrastructures on which the KMS and the protected resources are located. It is therefore much desired if secure data hiding could be achieved without an additional secret data hiding key

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

shared between the base station and the data center. Also, we appreciate simple embedding algorithm as the base station usually is constrained by limited computing capabilities and/or power. Finally, the data center, which has abundant computing resources, extracts the embedded message and recovers the original image by using the encryption key K.

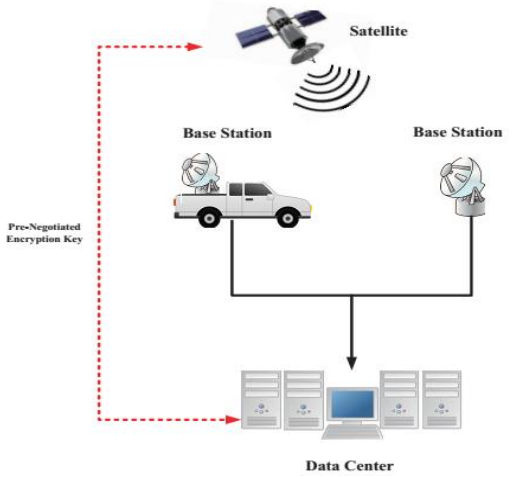

Fig. 1. Image data hiding in the scenario of secure remote sensing

In this thesis, we propose an encrypted-domain RIDH scheme by specifically taking the above-mentioned design preferences into consideration. The proposed technique embeds message through a public key modulation mechanism, and performs data extraction by exploiting the statistical distinguish ability of encrypted and non-encrypted image blocks. Since the decoding of the message bits and the original image is tied together, our proposed technique belongs to the category of non-separable RIDH solutions. Compared with the state-of-the-arts, the proposed approach provides higher embedding capacity, and is able to achieve perfect reconstruction of the original image as well as the embedded message bits. Extensive experimental results on 100 test images validate the superior performance of our scheme. The rest of this paper is organized as follows. Overviews the related work on RIDH over the encrypted domain. The proposed data hiding technique in encrypted images. The schematic diagram of the proposed message embedding algorithm over encrypted domain is depicted in following figure. In this work, we do not consider the case of embedding multiple watermarks for one single block, meaning that each block is processed once at most. For simplicity, we assume that the number of message bits to be embedded is $n \cdot A$, where $A \leq B$ and B is the number of blocks within the image. The steps of performing the message embedding are summarized as follows:

Step 1: Initialize block index i = 1.
Step 2: Extract n bits of message to be embedded, denoted by Wi.
Step 3: Find the public key Q[Wi]d associated with Wi, where the index [Wi]d is the decimal representation of Wi. For instance, when n = 3 and Wi = 010, the corresponding public key is Q2.
Step 4: Embed the length-n message bits Wi into the ith block via

$$[[\mathbf{f}]]_i^w = [[\mathbf{f}]]_i \oplus \mathbf{Q}_{[\mathbf{W}_i]_d}$$

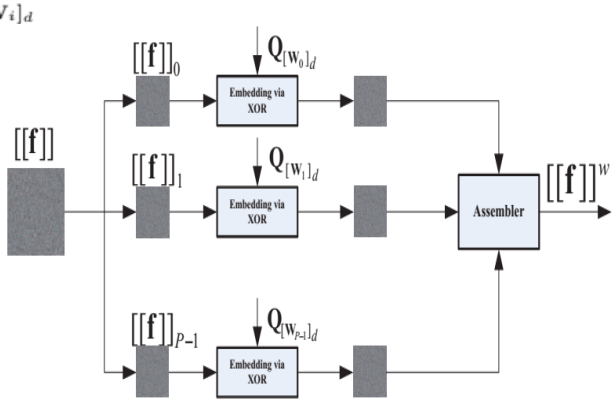

Fig. 2.schematic diagram of data hiding over encrypted domain

Step 5: Increment i = i + 1 and repeat ***Steps 2-4*** until all the message bits are inserted. The watermark length parameter A needs to be transmitted alone with the embedded message bits. There are many ways to solve this problem. For instance, we can reserve some blocks

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

to embed A. Or, we can append an end-of-file symbol to the message to be embedded, such that the decoder can implicitly determine A. Both strategies can be readily implemented in practice with negligible affect to the actual embedding rate. For the sake of simpler presentation, we exclude the discussion of embedding A in the sequel. From the above steps, it can be seen that the message embedding is performed without the aid of a secret data hiding key. As will be proved, high level of embedding security can still be guaranteed, thanks to the protection offered by the encryption key K.

In addition, the computations involved in message embedding are rather small (simple XOR operations), and all the block-by-block processing can be readily made parallel, achieving high-throughput. It is emphasized that the possibility of eliminating the data hiding key is not unique to our proposed method, but rather arguably applicable for all non-separable RIDH schemes over encrypted domain. For instance, the existing non-separable RIDH schemes, upon trivial modifications, can still ensure embedding security even if the data hiding key is eliminated. If we fix the way of partitioning a block into S0 and S1 (namely, do not use data hiding key to randomize the block partitioning), then an attacker still cannot compute the fluctuation function. So as to decode the embedded message. This is because an attacker does not access to the secret encryption key K.

In other words, the protection mechanism in the encrypted domain can be naturally extended to provide security for message embedding, eliminating the necessity of introducing an extra data hiding key. This could lead to significant reduction of the computational cost and potential risk of building up a secure KMS, which has been proved to be very challenging in the multi-party environment. Though the possibility of removing the data hiding key holds for all non-separable RIDH schemes over encrypted domain, it has never been pointed out in the existing work. It can be witnessed by the fact that all the existing RIDH schemes, including separable and non-separable ones, involve a data hiding key that has to be shared and managed between the data hider and the recipient. In addition to identifying this property, we, in the following Section VI, will exploit the message indistinguishability to prove that the removal of data hiding key will not hurt the embedding security. Before presenting the data extraction and image decryption methods, let us first investigate the features that can be used to discriminate encrypted and non-encrypted image blocks. The classifier designed according to these features will be shown to be crucial in the proposed joint data extraction and image decryption approach.

II. LITERATURE SURVEY

2.1 OVERVIEW:

Reversible image data hiding (RIDH) is a special category of data hiding technique, which ensures perfect reconstruction of the cover image upon the extraction of the embedded message. The reversibility makes such image data hiding approach particularly attractive in the critical scenarios, e.g., military and remote sensing, medical images sharing, law forensics and copyright authentication, where high fidelity of the reconstructed cover image is required.
The majority of the existing RIDH algorithms are designed over the plaintext domain, namely, the message bits are embedded into the original, un-encrypted images. The early works mainly utilized the lossless compression algorithm to compress certain image features, in order to vacate room for message embedding

2.2 A NOVEL REVERSIBLE DATA HIDING SCHEME BASED ON TWO-DIMENSIONAL DIFFERENCE-HISTOGRAM MODIFICATION

Author Name: Swapna Kumari And B Dasari Subbarao

Problem Definition

In this thesis, based on two-dimensional difference histogram modification, a novel reversible data hiding (RDH) scheme is proposed by using difference-pair-mapping (DPM). First, by considering each pixel-pair and its context, a sequence consisting of pairs of difference values is computed. Then, a two-dimensional difference-histogram is generated by counting the frequency of the resulting difference-pairs. Finally, reversible data embedding is implemented according to a specifically designed DPM. Here, the DPM is an injective mapping defined on difference-pairs.

Findings

It is a natural extension of expansion embedding and shifting techniques used in current histogram-based RDH methods. By the proposed approach, compared with the conventional one-dimensional difference-histogram and one-dimensional prediction-error-histogram-based RDH methods, the image redundancy can be better exploited and an improved embedding performance is achieved. Moreover, a pixel-pair-selection strategy is also adopted to priority use the pixel-pairs located in smooth image regions to embed data. This can further enhance the embedding performance.

Conclusion

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

Experimental results demonstrate that the proposed scheme outperforms some state-of-the-art RDH works.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

2.3 AN INPAINTING-ASSISTED REVERSIBLE STEGANOGRAPHIC SCHEME USING A HISTOGRAM SHIFTING MECHANISM
Author Name: Chuan Qin

Problem Definition
In this thesis, we propose a novel prediction-based reversible steganographic scheme based on image in painting. First, reference pixels are chosen adaptively according to the distribution characteristics of the image content. Then, the image in painting technique based on partial differential equations is introduced to generate a prediction image that has similar structural and geometric information as the cover image.

Finding
Through the use of the adaptive strategy for choosing reference pixels and the in painting predictor, the prediction accuracy is high, and more embeddable pixels are acquired. Finally, by using the two selected groups of peak points and zero points, the histogram of the prediction error is shifted to embed the secret bits reversibly. Since the same reference pixels can be exploited in the extraction procedure, the embedded secret bits can be extracted from the stego image correctly, and the cover image can be restored lossless.

Conclusion
The proposed scheme provides a greater embedding rate and better visual quality compared with recently reported methods.

2.4 REVERSIBLE DATA HIDING WITH OPTIMAL VALUE TRANSFER
Author Name : Mrs. A. Niranjana devi

Problem Definition
In reversible data hiding techniques, the values of host data are modified according to some particular rules and the original host content can be perfectly restored after extraction of the hidden data on receiver side. In this paper, the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed.

Finding
The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors. Here, the estimation errors are modified according to the optimal value transfer rule. Also, the host image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset.

Conclusion
A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. This way, a good reversible data hiding performance is achieved.

2.5 SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE
Author Name : Jiantao Zhou

Problem Definition
This work proposes a novel scheme to reversibly hide data into encrypted grayscale image in a separable manner. During the first phase, the content owner encrypts the image by permuting the pixels using the encryption key. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key. At the receiver side, if the receiver has only encryption key, he can generate an image similar to the original one, but cannot read the hidden data.

Finding
Peak Signal to Noise Ratio (PSNR) of this decrypted image is much higher than the existing methods. If the receiver has only data hiding key, he can extract the data, but cannot read the content of the image. If the receiver has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key.

Conclusion
The method also has a higher data hiding capacity than the existing reversible data hiding techniques in encrypted image.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

2.6 AN IMPROVED REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING SIDE MATCH
Author Name: T. MARGARET

Problem Definition
The proposes an improved version of Zhang's reversible data hiding method in encrypted images. The original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness.

Finding
Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits.

Conclusion
The experimental results reveal that the proposed method offers better performance over Zhang's work. For example, when the block size is set to 8 8, the error rate of the Lena image of the proposed method is 0. 34%, which is significantly lower than 1.21% of Zhang's work.

III. METHODOLOGY

Encryption Method:
Encryption is the process of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers.

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message.

Watermark Method:
A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.
It is prominently used for tracing copyright infringements and or banknote authentication. Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm. If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

Embedded Method:
An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today.
When compared with general-purpose counterparts are low power consumption, small size, rugged operating ranges, and low per-unit cost. This comes at the price of limited processing resources, which make them significantly more difficult to program and to interact with. However, by building intelligence mechanisms on top of the hardware, taking advantage of possible existing sensors and the existence of a network of embedded units, one can both optimally manage available resources at the unit and network levels as well as provide augmented functions, well beyond those available. For example, intelligent techniques can be designed to manage power consumption of embedded systems.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. According to the context of the attack, the attacker may have access to different amount of information. Clearly, the attacker at least can access to watermarked signal. In some occasions the embedded message or the cover signal can also be a available to the attacker. Therefore, the security level of the encrypted-domain RIDH scheme should be assessed for different contexts,. Similar to the problem of evaluating the security for encryption primitives, defined three types of attacks:

- The Watermarked Only Attack (WOA), in which the attacker only has access to watermarked images.
- The Known Message Attack (KMA), in which the attacker has access to several pairs of previously watermarked images and the associated messages. Certainly, the currently transmitted message bits are not known to the attacker.
- As explained, the purposes of the last two attacks are mainly to recover the data hiding key, so as to extract the future embedded messages or hack different pieces of content watermarked with the same key. In our proposed RIDH scheme, the data hiding key has been eliminated, and hence, these two attack models are not applicable. Under the WOA, the only attack type relevant to our scheme, the attacker attempts to extract the embedded message and/or recover the original image from the watermarked and encrypted image. Before evaluating the security under WOA, let us first give the definition of message indistinguishability, which should hold for any secure encryption method.

V. RESULTS AND DISCUSSION

Results and Evaluation

In this thesis, we experimentally evaluate the embedding performance of our proposed encrypted-domain RIDH scheme. The test set is composed of 100 images of size 512 × 512 with various characteristics, including natural images, synthetic images, and highly textured images. All the test images can be downloaded from https://dl.dropboxusercontent.com/u/ 103270026/TestImage.zip. Obviously, the test set is different from the training set used to derive the two-class SVM classifier. As mentioned in Section III, we stick to standardized encryption method, and all the images are encrypted using the stream cipher AES-CTR. We would like to compare our scheme with three state-of-the-art algorithms, where standardized encryption methods were also used. It tabulates the embedding capacity and data extraction accuracy τ of our method, and for different settings of block size. Here, τ is defined by

$$\tau = \frac{\text{\# of correctly extracted bits}}{\text{\# of embedded bits}}$$

and the values given are averaged over all the blocks in the 100 test images. In this table, we fix n = 3 in our method, i.e., each block accommodate 3 bits. As the scheme of [18] only works on blocks no less than 3×3, the results for smaller block configurations are marked with '–'. For fair comparison with [18] and [19], we try different numbers of flipped LSBs, instead of fixing to flip 3 LSBs, and only record the best extraction accuracy. This is equivalent to remove the constraint on direct decryption. It can be seen that, for all the three methods, the embedding capacity increases as the block size drops. Our method can embed 21675 message bits for each 512 × 512 image when the block size is 6 × 6, while ensuring 100% accuracy of data extraction. As the block size decreases further, small number of extraction errors appears. Even when the block size shrinks to 2 × 2, the accuracy is still as high as 99.2356%.

In contrast, the values of τ and its improved version are consistently lower than 100%, even when the block size is as big as 8 × 8. Also, for the same block size, the extraction accuracy of our method is significantly higher than those of [18] and [19], while the embedding capacity is 3 times higher. In addition to the comparison of the averaged extraction accuracy, we also show the results of these three methods for six representative images illustrated. Images with large portion of textural regions, e.g., Texture mosaic 1 and Cactus, give much degraded results, especially when the block size is small. For instance, the extraction accuracy is only 72.1252%, for the image Cactus when the block size is 4 × 4. In contrast, our method offers much better extraction accuracy for all settings of block size. In fact, extraction errors are only detected in three images Texture mosaic 1, Cactus, and Baboon in the case that the block size is 4 × 4, while for all the other cases with bigger block sizes, 100% extraction accuracy is retained.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

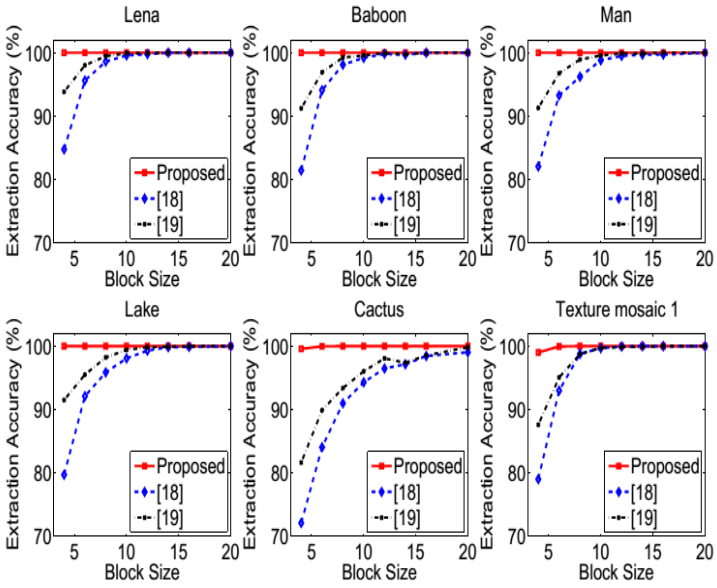

Fig. 3.Six Test Images For Fine-Grained Comparison

TABLE I. EMBEDDING PERFORMANCE COMPARISON WITH [18] AND [19].

	proposed		[18]		[19]	
Block Size	Capacity	Accuracy	Capacity	Accuracy	Capacity	Accuracy
8 × 8	12288 bits	100%	4096 bits	89.4468%	4096 bits	92.0461%
8 × 7	14016 bits	100%	4672 bits	88.4133%	4672 bits	91.4372%
7 × 7	15987 bits	100%	5329 bits	87.2088%	5329 bits	90.6550%
7 × 6	18615 bits	100%	6205 bits	85.7437%	6205 bits	89.6938%
6 × 6	21675 bits	100%	7225 bits	84.1943%	7225 bits	88.8833%
6 × 5	26010 bits	99.9973%	8670 bits	82.1644%	8670 bits	87.6347%
5 × 5	31212 bits	99.9930%	10404 bits	79.9319%	10404 bits	86.1932%
5 × 4	39168 bits	99.9903%	13056 bits	77.1022%	13056 bits	84.3227%
4 × 4	49152 bits	99.9761%	16384 bits	73.9654%	16384 bits	82.3897%
3 × 3	86700 bits	99.8224%	28900 bits	64.0132%	28900 bits	76.8219%
2 × 2	196608 bits	99.2356%	--	--	65536 bits	69.1936%

Fig. 4.comparison of the extraction accuracy for six representative test images

When comparing, our method also achieves better embedding performance. For a 512 × 512 image, the embedding capacity of 16384 bits, as it can only work with 4 × 4 blocks, and each block accommodates one message bit. As a comparison, our scheme can embed 49152 message bits with the same block size, assuming n = 3. Under the above settings, the averaged accuracy of recovering the original image block in our method is 99.9761%, which outperforms the result 97.3062% given by encrypted images. The performance gap becomes even more significant if we focus on the texture-rich images. For Texture mosaic 1, our method leads to the extraction accuracy 99.02%, while the counterpart of encrypted images is dramatically reduced to 74.83%.

Furthermore, we investigate the effect brought by increasing n, i.e., embed more bits into one single block. Obviously, the number of public keys Qj's exponentially increases as we make n larger. This will enlarge the complexity of data extraction as we need to examine all the S = 2n decoding candidates. Also, the maximized minimum Hamming distance among all the public keys Qj's decreases for bigger n, which in turn could result in more extraction errors. Thanks to the powerful error correction mechanism based on image selfsimilarities, these increased errors can still be corrected to a large extent. As illustrated in Table II, when n ≤ 5, we still can ensure 100% success rate of data extraction for all 100 test images. As we further increase n from 6 to 10, some extraction errors gradually appear only in two test images Texture mosaic 1 and Cactus, which contain highly textured areas. The data extraction in the remaining 98 images can still be perfectly performed. In Fig. 8, we highlight the blocks in which extraction errors occur in the two problematic images when n = 8. It can be observed that the incorrectly decoded blocks are untypically homogenous in textural characteristics to their context, which explains the difficulty in discretion by the proposed error correction mechanism. To tackle this challenge, an error-correcting code (ECC) such as Hamming code can be used to further correct those unsolvable errors, at the cost of significantly reduced embedding rate. Here, we do not discuss the employment of ECC in details because 1) the ECC is a relatively independent component, and 2) the performance of ECC highly depends on the decoding error rate, on which we focus in this work. Upon knowing the characteristics and behavior of the decoding error, the task of designing and implementing an ECC becomes a trivial issue.

Finally, we evaluate the time complexity of performing the joint decryption and data extraction, with respect to different settings of n, where n is the number of bits embedded into one single block. As can be seen from Section V, the computational complexity mainly comes from applying SVM classifier to the S = 2n decoding candidates. Since the SVM training is conducted off-line, the associated complexity will not be counted into the evaluation of joint decryption and data extraction. In Fig. 9, the results are averaged over all the 100 test images of size 512 × 512. The measurement of the time complexity is carried out over an un-optimized, unparalleled dotnet implementation by using the built-in tic and functions in a personal PC with Intel i7@3.40 GHz CPU and 32 GB RAM. When n = 1, namely, each block carries 1bit message, it takes around 0.66 seconds on average to process one 512 × 512 sized image. As n becomes larger, the time complexity increases, because there are S = 2n public keys that need to be examined. Noticing that the joint decryption and data extraction of different blocks are largely independent, except the error correction stage where image self-similarity is exploited, significant time saving can be retained by using a parallel computing platform. We also would like to point out that the complexity of performing the joint decryption and data extraction may not be crucial in many applications, e.g. secure remote sensing, where the recipient has abundant computing resources.

VI. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

In this thesis, design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. It suggests a public key modulation mechanism, which allows us to embed the data via simple XOR operations, without the need of accessing the secret encryption key. At the decoder side, a propose to use a powerful two-class SVM classifier to discriminate encrypted and non-encrypted image patches, enabling us to jointly decode the embedded message and the original image signal perfectly.

FUTURE ENHANCEMENT

Performed extensive experiments to validate the superior embedding performance of our proposed RIDH method over encrypted domain. And also would like to point out that the complexity of performing the joint decryption and data extraction may not be crucial in many applications, e.g. secure remote sensing, where the recipient has abundant computing resources.

BOOKS REFERENCES

1. Alistair Mc Monnies, "Digital Image Processing 3rd Edition". Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.
2. Poonam Yadav, "Digital Image Processing" Edition 2002, Tata McGraw-Hill, Publishing Company Limited, New Delhi.
3. Roger S. Pressman "Software Engineering" Tata McGraw-Hill, Publishing Company Limited (1987).
4. Munesh Chandra Trivedi, "Digital Image Processing", Second Edition, Pearson Education Asia, ISBN: 981-4035-20-3 (2000).

5. Tamal Bose, "Digital Signal and Image Processing (WSE series)", Microsoft Press.
6. B. Chanda & D.Dutta Majumder, "Digital Image Processing And Analysis", Prentice Hall.

JOURNAL 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] 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, 2006.
[3] Z. Ni, Y. Shi, N. Ansari, and W. Su,"Reversible data hiding" IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.
[4] 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 Secur, vol. 8, no. 7, pp. 1091-1100, 2013.
[5] 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.
[6] 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, 2009.
[7] J. Tian,"Reversible data embedding using a difference expansion" IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003.
[8] Y. Hu, H. K. Lee, and J. Li,"De-based reversible data hiding with improved overflow location map" IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250-260, 2009.
[9] X. Li, B. Yang, and T. Zeng,"Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection" IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524-3533, 2011.
[10] X. Zhang,"Reversible data hiding with optimal value transfer" IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316-325, 2013.
[11] T. Bianchi, A. Piva, and M. Barni,"On the implementation of the discrete fourier transform in the encrypted domain" IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, pp. 86-97, 2009.