International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

Reversible Image Data Hiding in an Encrypted Domain with High Level of Security

Pooja. G[1], Rohini. J[2]

[1,2]*Students Dept of Computer Science and Engineering, Arasu Engineering College, Tamilnadu, India*

Abstract - *This paper proposes a reversible image data hiding (RIDH) scheme over encrypted domain. The public key modulation mechanism is used 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 patches, to jointly decode the embedded message and the original image signal. The proposed system provides higher embedding capacity and also it is able to reconstruct the original image as well as the embedded message*.

Key Words: (Size 10 & Bold) SVM classifier, Reversible Image Data Hiding (RIDH), Public key modulation, Secret encryption key, Data embedding etc.

1. INTRODUCTION

Reversible image data hiding (RIDH) is a 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 some of the 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. 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 a un-trusted third party for further processing.

Most of the existing systems are developed over plaintext and the message bits are embedded into original.

1.1Introduction to image processing

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions digital image processing may be modeled in the form of multidimensional systems.

There are two types of methods used for image processing namely, analogue and digital image processing. Analogue image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. Digital image processing techniques help in manipulation of the digital images by using computers. The three general phases that all types of data have to undergo while using digital technique are pre-processing, enhancement, and display, information extraction.

1.1 Image data hiding

Data security over the networks is an important challenge for researchers and computer engineers for decades. Internet is a great convenience which offers secure data communication of important messages, secret information, variety of images and documents. In order to prevent the unauthorized access of important messages and images from malicious fraudsters, one need to make it more secure by sending the encrypted messages over the networks. To accomplish and build such secure systems, many data hiding and encryption techniques have been proposed in the last few decades. Both the data hiding and encryption techniques are found to be the main mechanisms in data security. However, use of former mechanism has been increasing recently due to some demerits have been found in the later mechanism.

Data hiding techniques could play a major role to embed important data into multimedia files such as images, videos or sounds. Because digital images are insensitive to human visual system, therefore images could be good cover carriers. Data hiding has two major applications [5] – watermarking and steganography. Watermarking merely extends the cover source with extra information. Steganographic techniques are used to store watermarks in data.

1.2 Stegnography

Steganography provides better security than cryptography because cryptography hides the contents of the message but not the existence of the message. So no one apart from the

authorized sender and receiver will be aware of the existence of the secret data. Steganographic messages are often first encrypted by some traditional means and then a cover image is modified in some way to contain the encrypted message. The detection of steganographically encoded packages is called steganalysis. In this paper, we propose three efficient Steganography techniques that are used for hiding secret messages. They are LSB based Steganography, Steganography using the last two significant bits and Steganography using diagonal pixels of the image. Symmetric and asymmetric key cryptography has been used to encrypt the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

1.3 Existing System

The majority of the existing RIDH algorithms are designed over the plaintext domain, such as the message bits are embedded into the original unencrypted 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 based technique, 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.

1.4 Drawbacks

The drawbacks of the existing approaches are: Low secure reversible image data hiding and there is no Discriminate encrypted and non-encrypted image patches.

2. LITERATURE SURVEY:

(i) M. U. Celik, G. Sharma, A. Tekalp, and E. Saber,"Lossless generalizedlsb data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp.253- 266, 2018. In this paper the data embedding is done with lossless compression.

(ii) 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, 2017. In this paper the watermarking is also included to eliminate the errors.

(iii) 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.

(iv) 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.

(v)Y. Hu, H. K. Lee, and J. Li,"De-based reversible data hiding with improved overflow location map," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 19, no. 2, pp. 250-260, 2009.

3. PROPOSED SYSTEM:

In this paper, 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 distinguishability 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. 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.

3.1 Feature selection for discriminating Encrypted AND Non-Encrypted Image Blocks

To differentiate encrypted and original, un-encrypted image blocks, we here design a feature vector $\rho = (H, \sigma, V)'$ integrating the characteristics from multiple perspectives. Here, H is a tailored entropy indicator, σ is the SD of the block. Compared with the original, un-encrypted block, the pixels in the encrypted block tend to have a much more uniform distribution.

To reduce the negative effect of insufficient number of samples relative to the large range of each sample, we propose to compute the entropy quantity based on quantized samples, where the quantization step size is designed in accordance with the block size. Specifically, we first apply uniform scalar quantization to each pixel of the block $f = MN \cdot f / 256 k$

Instead of considering dedicated encryption algorithms tailored to the scenario of encrypted domain data hiding, we here stick to the conventional stream cipher applied in the standard format. That is, the ciphertext is generated by bitwise XORing the plaintext with the key stream. If not otherwise specified, the widely used stream cipher AES in the

CTR mode (AESCTR) is assumed. The resulting data hiding paradigm over encrypted domain could be more practically useful because of two reasons: 1) stream cipher used in the standard format (e.g., AES-CTR), is still one of the most popular and reliable encryption tools, due to its provable security and high software/hardware implementation efficiency [26]. It may not be easy, or even infeasible, to persuade customers to adopt new encryption algorithms that have not been thoroughly evaluated; 2) large number of data have already been encrypted using stream cipher in a standard way. When stream cipher is employed, the encrypted image is generated by

$$[[f]] = Enc(f, K) = f \oplus K$$

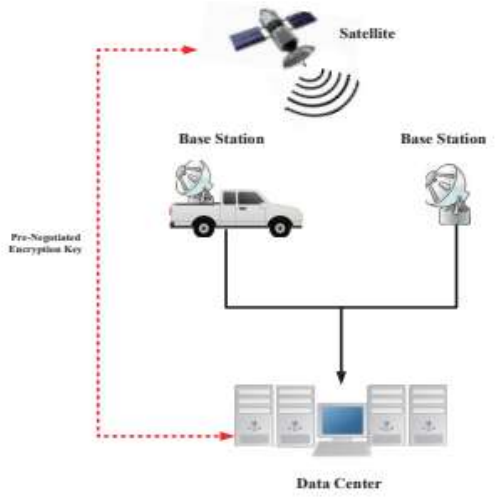


Fig 1: Image data hiding by secure remote sensing

The schematic diagram of the proposed message embedding algorithm over encrypted domain is depicted in Fig. 2. 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.

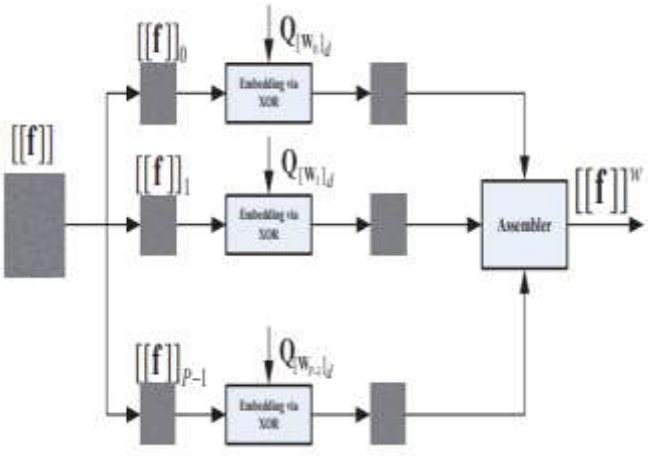


Fig -2: Data hiding over encrypted domain

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.

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 in the Section VI, high level of embedding security can still be guaranteed, thanks to the protection offered by the encryption key K.

4. JOINT DATA EXTRACTION AND IMAGE DECRYPTION

The decoder in the data center has the decryption key K, and attempts to recover both the embedded message and the original image simultaneously from [[f]]w, which is assumed to be perfectly received without any distortions. Note that this assumption is made in almost all the existing RIDH methods. Due to the interchangeable property of XOR operations, the decoder first XORs [[f]]w with the encryption key stream K and obtains

$$fw = [[f\,]]w \oplus K$$

The resulting fw is then partitioned into a series of nonoverlapping blocks fw i 's of size M×N, similar to the operation conducted at the embedding stage. We have

$$fwi = fi \oplus Q[Wi]d$$

The joint data extraction and image decryption now becomes a blind signal separation problem as both Wi and fi are unknowns. Our strategy of solving this problem is based on the following observation: fi, as the original image block, very likely exhibits certain image structure, conveying sematic information. When classification errors are detected for some blocks, we need a mechanism to correct them. Though the classifier is carefully designed, it is still difficult to distinguish those highly textured original blocks from the encrypted ones, especially when the block size is small. To solve this challenging problem, we propose to exploit the self-similarity property inherent to natural images. Even for those highly textured images, it is observed that similar blocks could be found in a non-local window. According to this phenomenon, the proposed error correction approach is based on the following key observation: if a block is correctly decoded, then with very high probability, there are some similar patches around it.

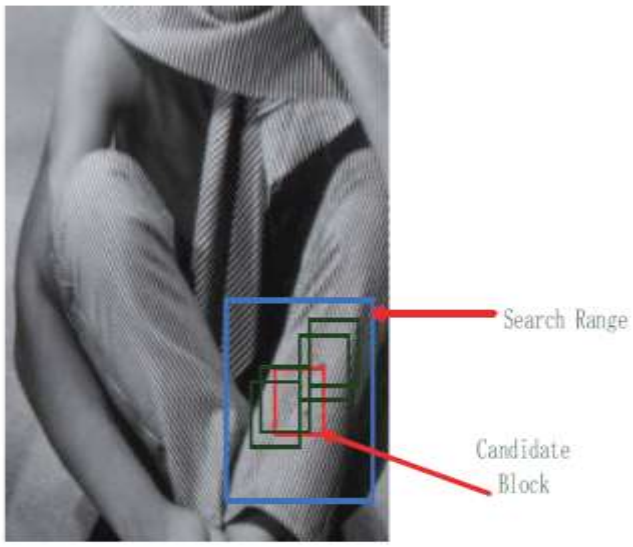


Fig -3: Error correction mechanism based on image self-similarity

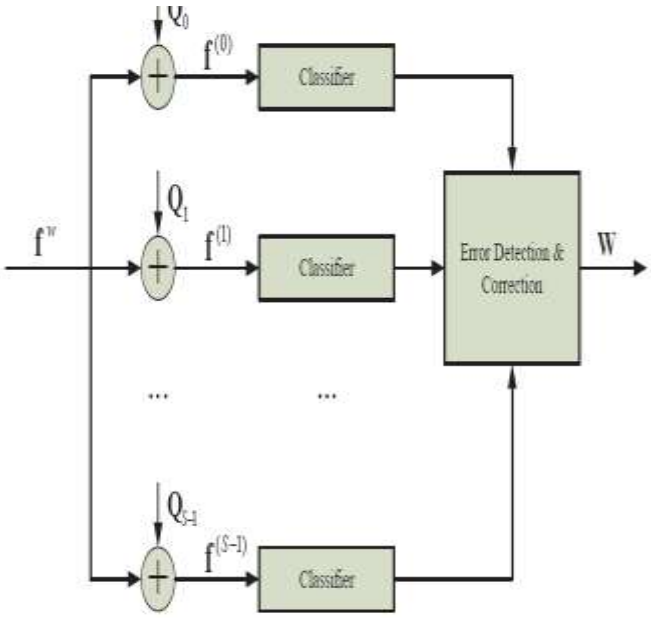


Fig-5: Schematic diagram for data extraction

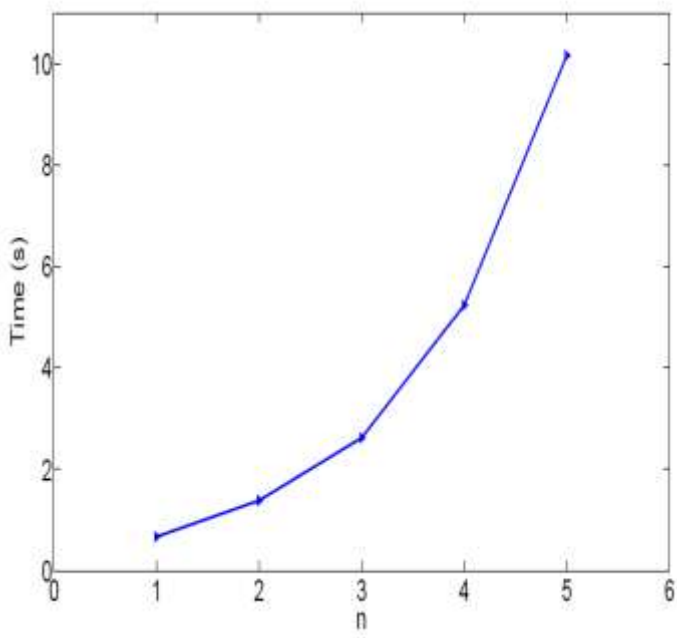
5. SECURITY ANALYSIS

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, namely, [[f]]w. In some occasions, the embedded message or the cover signal can also be available to the attacker [31]. Therefore, the security level of the encrypted-domain RIDH scheme should be assessed for different contexts. As explained in [31], 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 [[f]]w. Before evaluating the security under WOA, let us first give the definition of message indistinguishability, which should hold for any secure encryption method. There are three kinds of attacks, namely, 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; the Known Original Attack (KOA), in which the attacker has access to several pairs of *previously* watermarked images and the corresponding cover image. Certainly, the current cover image is not known to the attacker.

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 self similarities, 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) theperformance of ECC highly depends on the decoding error rate, on which we focus in this work. Upon knowing thecharacteristics 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. 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 Matlab implementation by using the built-in tic and toc functions in a personal PC with Intel i7@3.40 GHz CPU and 32 GB RAM. When n = 1, namely, each block carries 1 bit 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. we try different numbers of flipped LSBs, instead of fixing to flip 3 LSBs, and only record the best extraction accuracy in Table I. 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.



6. CONCLUSION

In this paper, we design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. We suggest 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, we 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.

7. REFERENCES

[1] M. U. Celik, G. Sharma, A. Tekalp, and E. Saber,"Lossless generalizedlsb data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp.253-266, 2018

[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, 2017.

[3] C.-C. Chang and C.-J. Lin,"Libsvm: A library for support vector machines," *ACM Trans. Intelligent Syst. and Technol.*, vol. 2, no. 3, pp. 27-53, 2016

[4] 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.

[5] X. Zhang,"Reversible data hiding with optimal value transfer," *IEEE Trans. Multimedia*, vol. 15, no. 2, pp. 316-325, 2013.

8. BIOGRAPHIES

Pooja. G received B.Tech(IT) from Annai college of Engineering and Technology and pursuing M.E (CSE) in Arasu Engineering college, Kumbakonam.

Rohini. J received B.E (CSE) from Arasu Engineering College and Pursuing M.E(CSE) in Arasu Engineering College, Kumbakonam.