International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Reversible Data Hiding in Encrypted Images Based on Progressive Recovery

Nagendra Prasad V, H. L. Shilpa

MCA Department, P.E.S. College of Engineering, Mandya, Karnataka , India

ABSTRACT

This paper proposes a method of reversible data hiding in encrypted images (RDH-EI) based on progressive recovery. Three parties are involved in the framework, including the content owner, the data-hider, and the recipient. The content owner encrypts the original image using a stream cipher algorithm and uploads a ciphertext to the server. The data-hider on the server divides the encrypted image into three channels and, respectively, embeds different amount of additional bits into each one to generate a marked encrypted image. On the recipient side, additional message can be extracted from the marked encrypted image, and the original image can be recovered without any errors. While most of the traditional methods use one criterion to recover the whole image, we propose to do the recovery by a progressive mechanism. Rate-distortion of the proposed method outperforms state-of-the-art RDH-EI methods.

Keywords : RDH-EI, LSB-planes, Image Recovery, Image Encryption, RDH

I. INTRODUCTION

Lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional data into several LSB-planes of cipher text pixels. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of originalimage. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original image after decryption.

Purpose

The main purpose of this project to create a combined data hiding schemes for cipher text images encrypted by public key cryptosystem.

Scope

The scope of this project is to create an application which enhances the security of data by hiding the data inside the image by placing it as a cipher text.

II. SYSTEM MODEL

We propose a novel architecture, In this architecture three parties are involved, and they are image provider, data hider and the receiver. Image provider encrypt the original image and the encrypted images now than, Data Hider embed the specified data into the encrypted images, and encrypted images containing embed data and Receiver decrypt the image using key and receiver obtain original image and embed data.

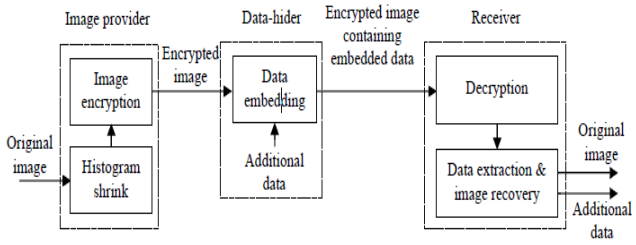

Figure 2 : System Architecture

III. PREVIOUS WORK

In some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. some parameters are embedded into a small number of encrypted pixels, and the of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

IV. PROPOSED METHODOLOGY

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted andthe original image can be perfectly recovered by exploiting the spatial correlation in natural image.

Image Encryption

The reversible data hiding in encrypted image is investigated in. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content.

Data Extraction

We will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters from the LSB of the selected encrypted pixels. Then, the receiver permutes and divides the other pixels into groups and extracts the embedded bits from the LSB planes of each group. When having the total extracted bits, the receiver can divide them into original LSB of selected encrypted pixels and additional bits. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

Image Recovery

In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

V. LITERATURE SURVEY

Every Software development requires the survey process. The Survey process is needed to get the requirement for the software. The Survey also consists of studying the present system and also studying about the tools needed for the development of the software. A proper understanding of the tools is very much essential. Following is an extract of the information of the material collected during literature survey.

Reversible data hiding into encrypted images is of increasing attention to researchers as the original content can be perfectly reconstructed after the embedded data are extracted while the content owner's privacy remains protected. The existing RDH techniques are designed for grayscale images and, therefore, cannot be directly applied to palette images. The RDH in the encrypted palette images is more challenging than that designed for normal image formats. This method adopts a color partitioning method to use the palette colors to construct a certain number of embeddable color-triples to embed the secret data. For a receiver, the embedded color-triples can be determined by verifying a self-embedded check-code that enables the receiver to retrieve the embedded data only with the data hiding key. By using the encryption key, the receiver can roughly reconstruct the image content.

Novel reversible data hiding scheme for encrypted images based on a pseudorandom sequence modulation mechanism. In the first phase, a content owner encrypts the original image for content protection. Then, a data-hider replaces a small proportion of data in LSB planes of encrypted image with the additional data and modifies the rest data in LSB planes according to the pseudorandom sequences modulated by the replaced and embedded data. With the encrypted image containing additional data, an additional-data user knowing the data-hiding key can extract the embedded additional data. And a content user with the encryption key may decrypt the encrypted image containing additional data to obtain the principal original content. If someone receives the decrypted image and has the data-hiding key, he can also successfully extract the additional data and perfectly recover the original image by exploiting the spatial correlation in natural image.

Novel reversible data hiding algorithm for encrypted images is proposed. In encryption phase, chaotic sequence is applied to encrypt the original image. Then the least significant bits (LSBs) of pixels in encrypted image are losslessly compressed to leave place for secret data. With auxiliary bit stream, the lossless compression is realized by the Hamming distance calculation between the LSB stream and auxiliary stream. At receiving terminal, the operation is flexible, that is, it meets the requirement of separation. With the decryption key, a receiver can get access to the marked decrypted image which is similar to the original one. With data-hiding key, the receiver can successfully extract secret data from the marked encrypted image. With both keys, the receiver can get secret data and the exactly original image. Compared with existing methods, experiments show the feasibility and efficiency of the proposed method, especially in aspect of embedding capacity, embedding quality and error-free recovery with increasing payload.

Reversible data hiding scheme for encrypted image with a low computation complexity is proposed, which consists of image encryption, data embedding and data extraction/ image recovery phases. The data of original image are entirely encrypted by a stream cipher. Although a data hider does not know the original content, he can embed additional data into the encrypted image by modifying a part of encrypted data. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

According to the data hiding key, with the aid of spatial correlation in natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB steganalytic methods, if he does not know the data hiding key, it is still impossible to extract the additional data and recover the original image. For ensuring the correct data extraction and the perfect image recovery, It may let the block side length be a big value or introduce error correction mechanism before data hiding to protect the additional data with a cost of payload reduction.

VI. CONCLUSION

Lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plain image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error. Due to the compatibility of the two schemes, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. So, the receiver may extract a part of embedded data in the encrypted domain, and extract another part of embedded data and recover the original image in the plaintext domain.

VII. REFERENCES

[1]. W. Hong, T.-S. Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, 19(4), pp. 199-202, 2012

[2]. X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396-1403, 2013.

[3]. J. Yu, G. Zhu, X. Li, and J. Yang, "An Improved Algorithm for Reversible Data Hiding in Encrypted Image," Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012), Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013

[4]. Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bit stream," IEEE Trans. on Multimedia, 16(5), pp. 1486-1491, 2014.

[5]. M. S. A. Karim, and K. Wong, "Universal Data Embedding in Encrypted Domain," Signal Processing, 94, pp. 174-182, 2014.

[6]. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Information Forensics & Security, 8(3), pp. 553-562, 2013.

[7]. W. Zhang, K. Ma, and N. Yu, "Reversibility Improved Data Hiding in Encrypted Images," Signal Processing, 94, pp. 118-127, 2014.

[8]. Y.-C. Chen, C.-W. Shiu, and G. Horng, "Encrypted Signal-Based Reversible Data Hiding with Public Key Cryptosystem," Journal of Visual Communication and Image Representation, 25, pp. 1164-1170, 2014.