Digital Copyright Protection for Multimedia

Rashmi Nikale A.[1], Sunita A. Gode.[2], Jamuna Adke S.[3], Rajeshri Kasture.[4],
Prof. Prof. K. N. Shedge [5]

[1,2,3,4] *BE Student, Computer Engineering Department, SVIT Chincholi, Nashik*
[5] *Professor, Computer Engineering Department, SVIT Chincholi, Nashik*

Abstract

This paper proposes a lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homo morphic 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 by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. 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 plaintext image after decryption.

Keyword : - *Reversible data hiding, data hiding , image encryption, audio encryption, image decryption, audio decryption, cryptography.*

---

1. Introduction

Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable ciphertext, the data hiding techniques embed additional data into cover media by introducing slight modifications. In some distortion-unacceptable scenarios, data hiding may be performed with a lossless or reversible manner. Although the terms “lossless” and “reversible” have a same meaning in a set of previous references, we would distinguish them in this work. We say a data hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, in, the pixels with the most used color in a palette image are assigned to some unused color indices for carrying the additional data, and these indices are redirected to the most used color. This way, although the indices of these pixels are altered, the actual colors of the pixels are kept unchanged. On the other hand, we say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure. A number of mechanisms, such as difference expansion, histogram shift and lossless compression, have been employed to develop the reversible data hiding techniques for digital images. Recently, several good prediction approaches and optimal transition probability under payload-distortion criterion have been introduced to improve the performance of reversible data hiding.Combination of data hiding and encryption has been studied in recent years. In some works, data hiding and encryption are jointed with a simple manner. For example, a part of cover data is used for carrying additional data and the rest data are encrypted for privacy protection. Alternatively, the additional data are embedded into a data space that is invariable to encryption operations. In another type of the works, data embedding is performed in encrypted domain, and an authorized receiver can recover the original plaintext cover image and extract the embedded data. This technique is termed as reversible data hiding in encrypted images (RDHEI). In some scenarios, for securely sharing secret images, a content owner may encrypt the images before transmission, and an inferior assistant or a channel administrator hopes to append some additional messages, such as the origin information, image notations or authentication data, within the encrypted images though he does not know the image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal

information into the corresponding encrypted images. Here, it may be hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. In, the original image is encrypted by an exclusive-or operation with pseudo-random bits, and then the additional data are embedded by flipping a part of least significant bits (LSB) of encrypted image. By exploiting the spatial correlation in natural images, the embedded data and the original content can be retrieved at receiver side. The performance of RDHEI can be further improved by introducing an implementation order or a flipping ratio. In, each additional bit is embedded into a block of data encrypted by the Advanced Encryption Standard (AES). When a receiver decrypts the encrypted image containing additional data, however, the quality of decrypted image is significantly degraded due to the disturbance of additional data. In, the data-hider compresses the LSB of encrypted image to generate a sparse space for carrying the additional data. Since only the LSB is changed in the data embedding phase, the quality of directly decrypted image is satisfactory. Reversible data hiding schemes for encrypted JPEG images is also presented. In, a sparse data space for accommodating additional data is directly created by compress the encrypted data. If the creation of sparse data space or the compression is implemented before encryption, a better performance can be achieved.

2. System Architecture:

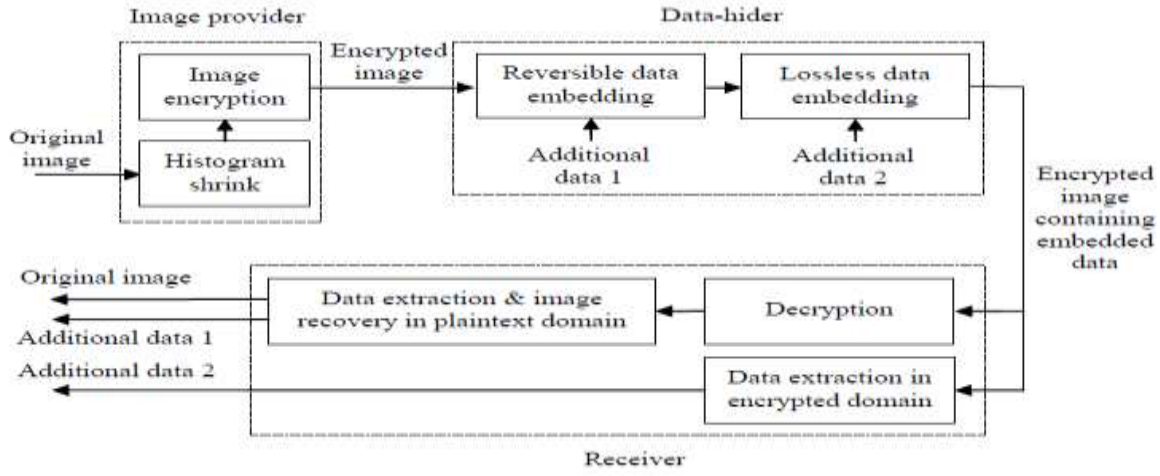

Fig: System Architecture

This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When having the encrypted image, the data-hider modifies the ciphertext pixel values to embed a bit-sequence generated from the additional data and error-correction codes. Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side. Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image. Note that the data-extraction and content-recovery of the reversible scheme are performed in plaintext domain, while the data extraction of the previous lossless scheme is performed in encrypted domain and the content recovery is needless.

3. Construction

Steganography is the art and science of writing hidden message in such way that no one, apart from the sender and intended recipient suspect the existence of the message.In that we doing image and audio steganography
Image Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden message or data
Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file.
Image / Audio Encryption & Decryption
Hidden data can be extracted from the encryption domain & the Operation Doesn't hamper the Quality of object
File Image Extension:-.BMP
File Audio Extension:-.WAV
In Your SYSTEM:-
Image:-In proposed system using high resolution for display clear images.
Audio:-Quality of audio don't change variably
Good quality of Sound
For image and audio run Process
1 Capture Secrete message
2 Choose the Audio or image
3 Provied the password and key for encryption
4 Stegnography generation
5 Capture encrypted audio or image
6 Provide Password and key
7 De-stegrography operation
8 Retriva lsecrete Message

4. Objective

1. Each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then reversed.
2. In second stage, extended hill cipher technique is applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure.
3. In third stage, the whole image _le is randomized multiple number of times using Modi_ed MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption.

5.Software,Hardware &Test Data Requirements:

5.1Hardware Requirement:

No external component required

5.2Software Requirements:

1. Operating System: Windows 7
2. Coding Language: C .Net,
3. IDE: Visual Studio2010

6. Conclusion:

This work proposes a Digital Copyright Protection for Multimedia cipher-text images encrypted by public key cryptography with probabilistic and homomorphic properties. In this 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 plaintext 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 plaintext image in the plaintext domain.

7. References:

[1]. W. Zhang, X. Hu, X. Li, and N. Yu, Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications, IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.

[2]. P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Proceeding of the Advances Cryptology, EUROCRYPT99, LNCS, 1592, pp. 223-238, 1999.

[3]. X. Zhang, Commutative Reversible Data Hiding and Encryption, Security and Communication Networks, 6, pp. 13961403, 2013.

[4]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, Lossless Generalized-LSB Data Embedding, IEEE Trans. on Image Processing, 14(2), pp. 253266, 2005.

[5]. 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.