Efficient Reversible Data Hiding based on Lossless Recovery

[1]Miss S.A. Rajgure, [2]Dr. V.M. Thakare, [3]Dr. S.S. Sherekar

[1]PG Student, SGBAU, Amravati

[2]HOD, SGBAU, Amravati

[3]Professor, SGBAU, Amravati

Abstract: This paper proposes an efficient reversible data hiding scheme based on lossless recovery. RDH in encrypted JPEG bitstream, the most popular image format, aiming at providing an RDH-EI approach with separable extraction capability, high embedding capacity, and secure encryption. This paper proposes an iterative algorithm to recover the original image. In this work, lossless recovery is required. Although JPEG encoding itself is lossy, users always hope not to introduce further degradation to a JPEG image while uploading. That is why lossless recovery is required. The proposed method also offers better security than the previous work.

Index terms: *Reversible data hiding, iterative recovery.*

I. INTRODUCTION

Reversible data hiding (RDH) aims to embed secret bits into an innocent object (e.g., digital image) by slightly altering the insignificant components of a cover signal, and, the hidden data as well as the original content should be recovered from the marked content without any loss. As a special case of information hiding, RDH can find many applications. Its reversibility is especially desirable when true fidelity is needed, *e.g.*, for medical and military image processing [1],[4]. The RIDH algorithm which already exists is 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 [2]. Some attempts on RDH-EI have been made. The original image is encrypted by the content owner using the stream enciphering, and additional bits are embedded by a data-hider into cipher text blocks by flipping three LSB of half the pixels in each block. On recipient side, the cipher text image is decrypted and two candidates for each block are generated by flipping again. As the original block is smoother than the interfered, embedded bits can be extracted and original image can be losslessly recovered [3]. While the additional data are embedded into encrypted images with symmetric cryptosystem in the above-mentioned RDHEI methods, a RDHEI method with public key cryptosystem is proposed. Although the computational complexity is higher, the establishment of secret key through a secure channel between the sender and the receiver is needless [5].

This paper, discusses five different RDH scheme i.e. SRDH scheme, RIDH scheme, RDH-EI scheme, RDH in encrypted domain, lossless, reversible, and combined data hiding schemes. There are some drawbacks in these schemes. High rates in the methods are achieved at the expenses of serious distortions and the quality of decrypted image is significantly degraded due to the disturbance of additional data; to overcome such problems improve version of RDH scheme is proposed here that is **"iterative recovery".** In iterative recovery the original image is recovered.

II. BACKGROUND

Many studies on Reversible data hiding have been done to improve the security in recent past years. Such schemes are: SRDH scheme for encrypted palette images which aims to divide the palette colors into multiple color-triples, among which the embeddable color-triples are recorded and self-embedded into the encrypted index matrix together with some other auxiliary data before the image transmission [1]. A Reversible image data hiding (RIDH) scheme over encrypted domain is proposed in which the data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed [2]. RDH-EI based on progressive recovery includes the content owner, the data-hider, and the recipient [3]. A new simple yet effective framework for RDH in encrypted domain is proposed. RDH in encrypted domain, specific RDH schemes have been designed according to the encryption algorithm utilized [4]. Cipher text images encrypted by public key cryptosystems with probabilistic and homomorphic properties of a lossless, a reversible, and a combined data hiding schemes [5].

This paper introduces five Reversible data hiding scheme i.e., SRDH scheme, RIDH scheme, RDH-EI scheme, RDH in encrypted domain, lossless, reversible, and combined data hiding schemes.

This paper is organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters **Section VI** contains proposed method **section VII** gives outcome and possible result. Finally **section VIII** Conclude this review paper. Finally **Section IX** presents future scope.

III. PREVIOUS WORK DONE

Han-Zhou Wu et al (2015) [1] has proposed SRDH scheme which adopts a color partitioning method to use the palette colors to construct a certain number of embeddable color-triples, the encrypted image indexes are self-embedded to embed the secret data so that a data hider can collect the usable color-triples. By using the encryption key, the receiver can roughly reconstruct the image content.

Jiantao Zhou et al (2015) [2] has proposes the RIDH technique which embeds the 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.

Zhenxing Qian et al (2016) [3] have proposed a new RDH-EI protocol for three parties. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based RDH-EI provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art RDH-EI methods.

Fangjun Huang et al (2016) [4] has proposed RDH in encrypted domain, the pixels in a plain image are first divided into sub-blocks with the size of m × n. Then, with an encryption key, a key stream is generated, and the pixels in the same sub-block are encrypted with the same key. After the stream encryption, the encrypted m × n sub-blocks are randomly permutated with a permutation key. Since, the correlation between the neighboring pixels in each sub block can be well preserved in the encrypted domain.

Zichi Wang et al (2015) [5] has proposed a reversible, lossless and combined data hiding schemes for cipher text images encrypted by public key cryptosystems. In 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.

IV. EXISTING METHODOLOGIES

A. Separable reversible data hiding (SRDH) :

The SRDH scheme [1], mainly consists of four phases, i.e., the encrypted image generation, data embedding, data extraction as well as image recovery. In the encrypted image generation, by employing the color partitioning algorithm, a certain number of usable color-triples are collected. After obtaining the encrypted image, a data hider can embed the secret data into the encrypted image. The idea of data hiding process is to modify the pixel values of collected color-triples. After a receiver acquires the marked and encrypted image, he should extract the auxiliary data at first. Then, he can fully retrieve the secret data if he has only the data hiding key. With only the encryption key, he can produce an approximation image of the original one. The receiver can fully reconstruct the image content and retrieve the secret data if he has both the encryption key and data hiding key.

B. Reversible image data hiding (RIDH) :

All the existing schemes in RIDH [2], include a data hiding key that has to be shared and managed between the data hider and the recipient which is separable and non-separable. The message will be exploited to identifying this property to prove that the removal of data hiding key will not hurt the embedding security.

C. Reversible data hiding in encrypted images (RDH-EI):

In RDH-EI [3], lossless recoveries in methods depend on the embedding payloads. As the payload is determined by the embedding parameters, errors may happen during recovery if inappropriate parameters are used. We analyse the error rates in each round of image recovery.

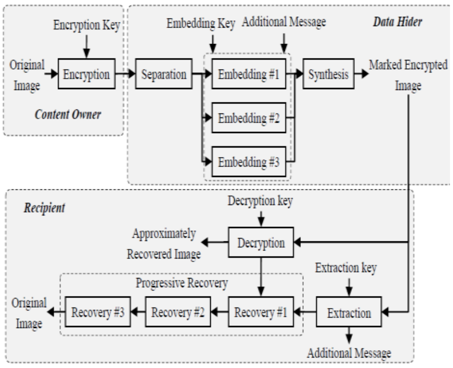

Figure 1: Framework of RDHEI based on progressive recovery

In Fig. 1, there are three parties: the content owner, the data-hider, and the recipient. The content owner encrypts the original image and uploads the encrypted image onto a remote server. The data-hider divides the encrypted image into three sets and embeds message into each set to generate a marked encrypted image. The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key.

D. Reversible data hiding in encrypted domain:

In Reversible data hiding in encrypted domain[4], the reversible data hiding algorithm is independent of the image encryption algorithm, and thus hundreds of previously proposed DHS (difference histogram shifting) and no need to design additional specific RDH scheme as the PEHS (prediction-error histogram shifting) based RDH schemes can be accomplished in encrypted domain directly . The proposed method consists of two parts. One part is image encryption and the other part is data extraction and original image recovery. The message extraction and image restoration can be described as follows.

$$b^* = \begin{cases} 0 & if\ C''_{i,j} - C''_{i,1} = 0, -1 \\ 1 & if\ C''_{i,j} - C''_{i,1} = 1, -2 \end{cases}$$

$$C'_{i,j}{}^* = \begin{cases} C''_{i,j} - 1 & if\ C''_{i,j} - C''_{i,1} > 0 \\ C''_{i,j} + 1 & if\ C''_{i,j} - C''_{i,1} < -1 \\ C''_{i,j} & otherwise \end{cases}$$

Where, $b*$ and C_'i, j ∗ represent the extracted message bit and the restored pixel value, respectively.

E. A lossless , a reversible, and a combined data hiding :

The pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels in a lossless, a reversible, and a combined data hiding schemes [5], so that the amount of encrypted data and the computational complexity are lowered. The data of encrypted image are modified in the lossless scheme, by the probabilistic property for data embedding. In the combined scheme, the image provider performs histogram shrink and image encryption. When having the encrypted image, the data-hider may embed the first part of additional data using the method. Denoting the ciphertext pixel values containing the first part of additional data as $c'(i, j)$, the data-hider calculates

$$c''(i,j) = c'(i,j) \cdot (r''(i,j))^n \bmod n^2$$

or

$$c''(i,j) = c'(i,j) \cdot (r''(i,j))^{n^s} \bmod n^{s+1}$$

Where, $r''(i, j)$ are randomly selected .On receiver side, the receiver firstly extracts the second part of additional data from the LSB-planes of encrypted domain. Then, after decryption with his private key, he extracts the first part of additional data and recovers the original plaintext image from the directly decrypted image.

V. ANALYSIS AND DISCUSSION

In the SRDH scheme [1], the encryption process can provide satisfactory confidentiality as an unauthorized decoder will hardly access the image visual content. In the proposed method, the data extraction process is independent of the image texture such that the data extraction operations are free of any error, which maintains the integrity of hidden data.

In RIDH method [2], the data extraction process is independent of the image texture such that the data extraction operations are free of any error, which maintains the integrity of hidden data.

RDH-EI methods [3], depends on the embedding payloads. As payload is determined by the embedding parameters, errors may happen during recovery if inappropriate parameters are used. A better prediction way is provided by the RDH-EI based progressive recovery for estimating the LSB-layers of the original image.

Reversible data hiding in encrypted domain in plain domain aims at developing a method that increases the embedding capacity as high as possible while keeping the distortion as low as possible. Since we consider RDH in encrypted image [4], the embedding capacity is relatively more important, and the concern over image quality degradation caused by data hiding can be neglected.

A lossless, a reversible, and a combined data hiding scheme [5], in which the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly, so that the amount of encrypted data and the computational complexity are lowered.

RDH scheme	**Advantages**	**Disadvantages**
Separable reversible data hiding scheme	Relatively high embedding payload and maintain a very good quality of the decrypted and marked image.	Our method does not produce an error rate in the data extraction and image recovery.
Reversible image data hiding scheme	This method has high embedding capacity, and reconstruct the original image as well as the embedded message.	The purposes of the last two attacks are to recover the data hiding key, the data hiding key has been eliminated, and hence, the two attack models are not applicable.
Reversible data hiding in encrypted images	This method achieves a better embedding rate	High rates in the methods are achieved at the expenses of serious distortions.
Reversible data hiding in encrypted domain	This method is independent of the image encryption algorithm. And has high payload and error-free data extraction	The permutation step can completely scramble the image, and thus the information disclosure cannot be exploited to decrypt encryption algorithm.
A lossless , a reversible, and a combined data hiding schemes	This method decreases the computational complexity..	The data embedding on encrypted domain can be slight distorted in plaintext domain due to the homomorphic property.

TABLE 1: Comparison between different RDH schemes.

VI. PROPOSED METHODOLOGY

Iterative recovery

In the progressive recovery the generated image has poor quality when directly decrypting the marked encrypted image. So to overcome this problem, this paper proposed a novel **"Iterative recovery"** framework.

In the proposed framework of iterative recovery, JPEG encryption and decryption algorithms are developed to hide the content of an original image. When the enciphered bitstream is received to the server, an additional messages is embedded by the data hider into the encrypted copy by compressing the padding bits of the bitstream. With an iterative recovery method based on blocking artifacts, the recipient can losslessly recover the original bitstream. The proposed method provides larger embedding capacity than the previous approach.

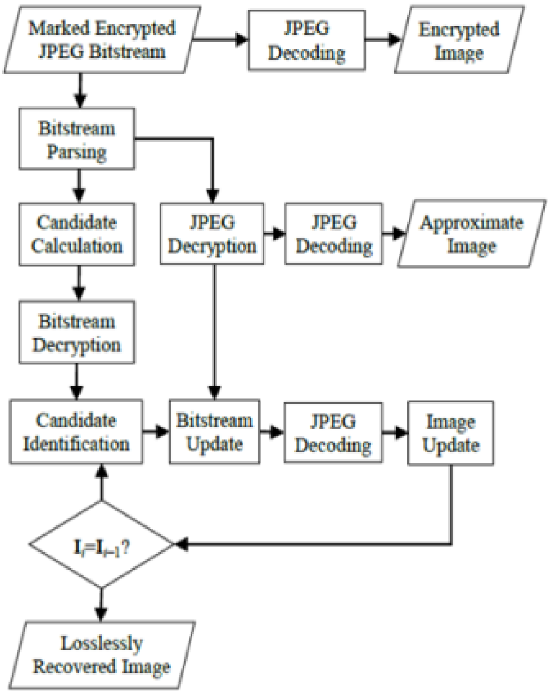

Fig 2: Flowchart of iterative recovery

The above diagram explains the working of proposed framework. The marked encrypted JPEG bitstream can be directly decoded by the JPEG decoder to construct an encrypted image of a smaller size. With the embedding key, the recipient can parse and decipher the marked encrypted JPEG bitstream using the proposed JPEG decryption algorithm. Since only the AC appended bits of the remaining entropy-coded segments were modified in data hiding, an approximate image with reduced quality can be reconstructed after decryption. With both the encryption and embedding keys, the recipient can losslessly recover the original JPEG image.

VII. OUTCOME AND POSSIBLE RESULT

The proposed method "**iterative recovery**" will losslessly recover the original image. The security is better in this method and a new JPEG bit stream corresponding to a smaller sized image is constructed. This approach has separable extraction capability, high embedding capacity, and secure encryption.

CONCLUSION

This paper focused on the study of various RDH scheme i.e. SRDH scheme, RIDH scheme, RDH-EI scheme, RDH in encrypted domain, lossless, reversible, and combined data hiding schemes. There are some drawbacks in these schemes. High rates in the methods are achieved at the expenses of serious distortions and the quality of decrypted image is significantly degraded due to the disturbance of additional data; to overcome such problems improve version of RDH scheme "**Iterative recovery**" is proposed here which losslessly recover the original image.

REFERENCES

[1] Han-Zhou Wu, Yun-Qing Shi, Hong-Xia Wang and Lin-Na Zhou, "Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification", *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 2015.

[2] Jiantao Zhou, *Member, IEEE,* Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 2015.

[3] Zhenxing Qian, Xinpeng Zhang, Guorui Feng,"Reversible Data Hiding in Encrypted Images Based on Progressive Recovery", *IEEE SIGNAL PROCESSING LETTERS*, 2016.

[4] Fangjun Huang, Jiwu Huang and Yun-Qing Shi, "New Framework for Reversible Data Hiding in Encrypted Domain", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Vol. 11, No. 12, DECEMBER 2016.

[5] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng,"Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 2015.