A Secure Method for Data Hiding in Encrypted Image using Progressive Recovery

Bhakti Narayan Patil
St. John College of Engineering and Technology
Palghar

Sanyukta Bhaskar Patil
St. John College of Engineering and Technology
Palghar

Mansi Kailash Patil
St. John College of Engineering and Technology
Palghar

Neha Mahyavanshi
St. John College of Engineering and Technology
Palghar

ABSTRACT

The existing paper explains reversible data hiding in encrypted images based on progressive recovery. Image processing is a method to convert an image into digital form and perform some operations on it, in order to yield an enhanced image or to extract some essential information from it. Three parties are involved in the framework, including the content owner, the data-hider, and the recipient. The owner encrypts the original image using an algorithm i.e. stream cipher . The method proposes stream cipher algorithm such as the AES (Advanced Encryption Standard)and uploads cipher text to the server. The data-hider on the server divides the encrypted image into three channels and respectively insert different amount of additional bits into each channel to generate a marked encrypted image. On the recipient side, additional message can be extracted from the marked encrypted image, and error free image can be recovered. Reversible data hiding is a technique used to recover original content it can be perfectly restored after extraction of the hidden message.

General Terms

Reversible data hiding, Information hiding, Cryptography, Steganography, Stream cipher

Keywords

Encryption, Decryption, Reversible Data hiding, scrambling, intrascrambling, AES algorithm

1. INTRODUCTION

In the modern era of digital communication a transfer of a secret message is a contestable one. Several methods have been proposed and investigated in the literature to provide privacy for communication. Data hiding technique conceals the secret message into cover image, where the image embedded with secret message is called stego-image. Then this stego-image is being transmitted to prevent the other party from modifying, intercepting, and tampering, thus protecting the data. There are two major research areas in data hiding techniques: irreversible data hiding and reversible data hiding. Irreversible hiding technique cannot recover images back to cover images even after the receiver retrieved the embedded secret message. Such technique holds an extremely high capacity but it destroys images. As for reversible data hiding technique, stego-images can be restored back to the original images after retrieving the embedded secret data with a lower capacity than irreversible method. From the above methods, this paper utilizes progressive reversible data hiding technique with the goal of achieving high capacity, acceptable image quality and reversibility. Traditional methods uses one criteria to recover the whole image, the progressive recovery uses three criteria as in our proposed method maximum data can be hidden as compared to the previous methods.

2. RELATED WORK

Cryptography is an art of securely transferring the message from sender to receiver. It uses the key concept for encryption the message information known as cryptography. It is used when communicating over the untrusted media such as internet. Cryptography is the technique that used in securely transfers the information with the use of algorithm which is un-readable by the third-party.

Categories of cryptography

a. Symmetric-key cryptography:

Symmetric-key cryptography is the technique that performed encryption and decryption by using single key. It is also known as secret key encryption.

b. Asymmetric-key cryptography:

It is also known as the public–key cryptography. In this two keys are used, one for encryption i.e. public and another for decryption i.e. decryption.

c. Hash Encryption:

Hash encryption performed by using the hash function. It provides security to user by using this concept. It produces fixed length signature for a message. Here our concern with image encryption. Image encryption technique is different from simple encryption. The data hiding in image takes place following four steps that are:

a) Select the medium or carrier.

b) Message which needed protection.

c) A function that will be used to hide data in the cover media.

d) Alternative key which provide authentication.

Types of Image cryptography/Encryption:

a. Generation of encryption-key: It is generated by randomly by using random function. It uses 128-bit of value.

b. Generation of random sequence: It is generated by using encryption-key. For example AES & RC4 algorithm.

Image Scrambling:

Digital image scrambling is the technique which transforms a meaningful image into a meaningless or disordered image in order to enhance the ability to confront attack and in turn improve the security.

In general, the better an image is scrambled, the better the information is hidden. Image scrambling technology is basically used in image encryption method by which the original image information can be hidden, so that the information will not be easily intercepted.

3. LITERATURE SURVEY

Currently, reversible data-hiding schemes [1]are applied in three domains i.e. the spatial domain, the transformed domain and the compression domain. In the compressed domain, the data is hidden by changing the compression code. The advantage of reversible data-hiding schemes in the compression domain is that such schemes can reduce transmission costs and simultaneously secure the information that is transmitted. The reversible data hiding schemes based on compression methods are projected in the last few years.

A. Pixel Based Algorithms

Pixel-based algorithms [3] compare the pixel which are at spatial neighborhood in order to select the pixel which is most similar in a sample texture as the output pixel. Since the pixels which are synthesized already are used to compute output pixel, any wrong computation will affect eh rest of the result causing errors.

Otori and Kuriyama [4]proposed the secret messages which are to be embedded can be encoded in the form of dotted pattern and they can be painted on to a blank workbench. The remaining pixel values can be coated using pixel based approach thus disguising the presence of colored dotted pattern. In order to extract the secret message at the receiver side before applying data-detecting mechanism printout of the stego texture image is taken. The embedding capacity provided by the method of Otori and Kuriyama is based on the number of the colored dotted patterns.

B. Patch-Based Algorithms :

Patch-based algorithms [7] use patches instead of pixels in order to synthesize the texture. Since the structure of texture inside the patches are maintained by Cohen et al. and Xu et al. approach the quality of image is improved.

Liang et al. [8] used the feathering approach for the overlapped pixel region by taking the average of the overlapped pixels.

Efros and Freeman [9] used image quilting approach by stitching the overlapped patches. He devised an approach by which the approach finds the source texture and candidate patch which has minimum error tolerance. Thus a boundary which is optimal between the synthesized and candidate patch is produced.

Honsingeret. al [11] used the spatial domain for data hiding. They used 256 modulo addition for embedding in the original image, hash function and secret key used while embedding the secret data. The reversibility is done by using of modulo addition and prevents the overflow and underflow condition It produces salt and pepper noise during modulo addition. Hiding is performed based on the histogram values [12], first find a value which no pixel called zero point and then the maximum pixel number of pixels in the image called peak point. They used peak points to insert the secret information. The maximum number of peak points leads to large data embedding.

Chuan Qin et.al used VQ the compression algorithm [15] is used in data hiding.The each overlapped partition is comprised of n2 pixels. A VQ code book, including Q code words is constructed and shared by the sender and the receiver. The length of each code word is equal to n2, During the embedding process the indices whose reference value are zero in the table is not considered in the index code book. A mapping is done based on the zero indices and the maximum occurrences in the indices. The unused indices are used to hide more data.

Wein Hong et.al [17] used pixel differencing method, in this the nearest neighboring pixels to predict the visited pixel value and calculates the variance value from those pixels. Message bits are embedded by adjusting the difference value found in the pixels. They proved the proposed algorithm with existing methods in terms of payload.

FeiPeng et al. [19] presented a reversible hiding method based on the integer transform and adaptive embedding. According to the pre-estimated distortion the image block is identified. The parameter is selected in different blocks which help to embed the secret bits in smooth block rather than sharper ones. Algorithm concentrates on a location map and auxiliary information which provides the length of the message and flag bit which identifies the embedding mechanism. This provides a good quality image with high payload capacity. Results show that the proposed method achieved an additional 2.17 bits per pixel payload than the existing schemes. A tradeoff exists between the capacities of the secret bit embedded per block and the distortion created in the image.

C. Reversible data hiding Algorithm :

Ni et al. [10] devised an algorithm which can recover the image without any distortion. Since the texture synthesis technique can control the pixel modification, it is an efficient technique among existing approaches. To the best of our knowledge, there is hardly any literature that relates reversible data hiding and patch based texture synthesis.

4. PROPOSED SYSTEM

A new Reversible Data Hiding in Encrypted Image protocol for three parties is proposed in this system. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based Reversible Data Hiding in Encrypted Image provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art Reversible Data Hiding in Encrypted Image methods. Since Reversible Data Hiding in Encrypted Image is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate. For a fair comparison, this paper limits the distortion to three LSB-layers, and accordingly improves the embedding rate.

The proposed system is illustrated in Figure including 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. When both keys are available, the original image can be losslessly recovered by progressive recovery.

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

In the proposed system there are three parties the content owner,the data hider,and the recipient.The content owner takes the original image and performs encryption over it using the encryption key.This encrypted image is sent to the data hider,the data hider separates the encrypted image into three channels and embeds additional message into each channel.After embedding additional message into it an marked encrypted image is generated.This marked encrypted image is sent to the recipient.The recipient performs extraction and decryption over the marked encrypted image using extraction key and decryption key.In extraction the additional message is obtained and in decryption the approximate recovered image is obtained.After extraction recovery is done to acquire the original image.

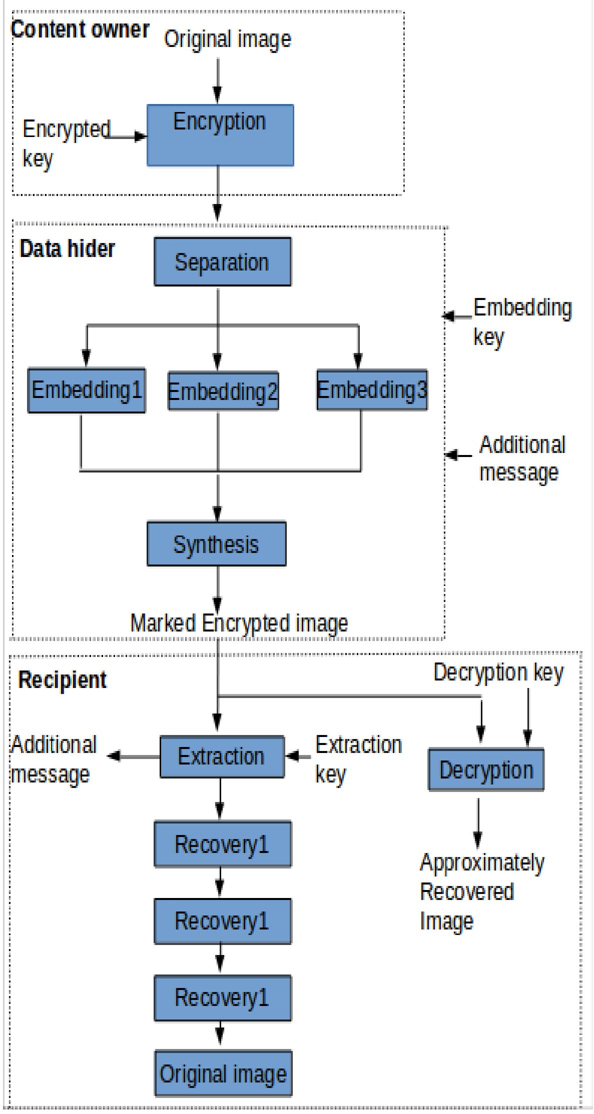
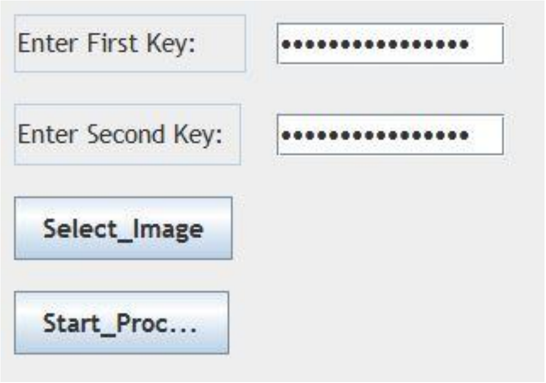


Fig 1: Architecture Diagram

[Reversible Data Hiding in Encrypted Images Based on Progressive Recovery]

5. RESULT AND ANALYSIS



Enter First Key: ••••••••••••••••

Enter Second Key: ••••••••••••••••

Fig 2: Content Owner Phase One

The content owner enters two keys which are of 16bit each,then select the image which is to be encrypted.Start the process by clicking the start button.

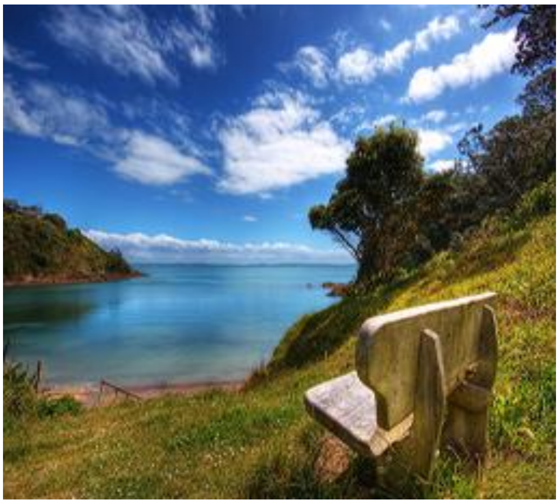
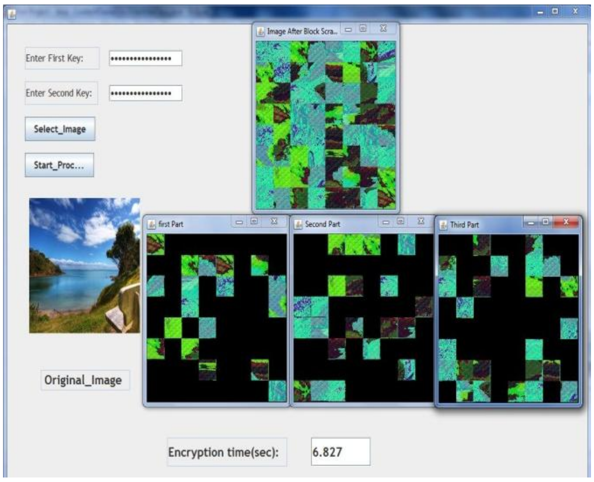


Fig 3: Original image

After selecting the image we start the process and get the block scrambling image that is shown in fig.4



Enter First Key: ••••••••••••••••

Enter Second Key: ••••••••••••••••

Encryption time(sec): 6.827

Fig 4: Image after Encryption and Block Scrambling

In block scrambling the image is divided into three parts i.e part1, part2, part3. Three blank images of the same size are created and the small parts of the top image are taken and fitted into the three blank images.

Fig 5: Image after Intra Block Scrambling

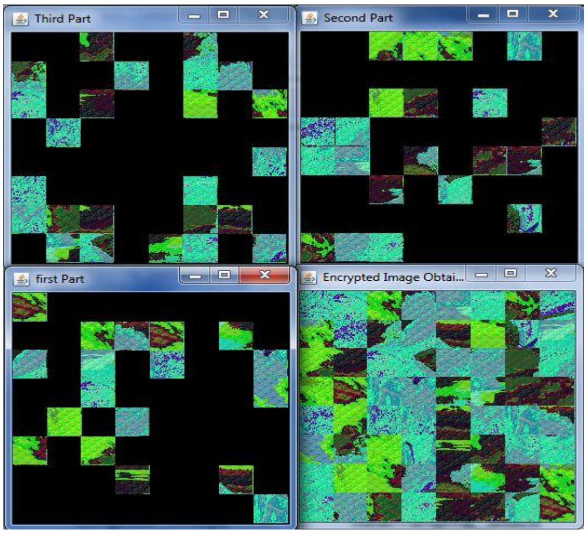


Fig 6: Image after performing block scrambling

6. CONCLUSION

Based on our previous work, a new Reversible Data Hiding in Encrypted Image protocol for three parties is proposed in this paper. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based Reversible Data Hiding in Encrypted Image provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art Reversible Data Hiding in Encrypted Image methods. This increases the payload and the imperceptibility. This is the light weight Algorithm, it does not require any transforms like DWT, DCT and FFT. This algorithm guarantees the value of the PSNR is above 50 dB. Therefore, its overall performance is better than many existing reversible data hiding algorithms. This algorithm can be applied in various fields where the original data and the cover image are entirely convalesced without loss.

7. FUTURE WORK

The Paper limits the distortion to three LSB-layers. Future researches may be directed to investigating more block division types for further improvement on the data hiding capacity. Future work will be to study the characteristics of image and data hiding methods to increase capacity, PSNR, and security & how to extend idea of Reversible data hiding to 3-D Image, audio &video. There should be research on increasing the size of the storing data and media data without any latency even if the size of the data increases without any limit.

8. REFERENCES

[1] N. F. Johnson and S. Jajodia, “Exploring steganography: theunseen,” Computer, vol. 31, no. 2, pp. 26-34, 1998.

[2] N. Provos and P. Honeyman, “Hide and seek: an introduction tosteganography,” Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062- 1078, 1999

[4] H. Otori and S. Kuriyama, “Data-embeddable texture synthesis,” in Proc. of the 8th International Symposium on Smart Graphics, Kyoto, Japan,

[5] H. Otori and S. Kuriyama, “Texture synthesis for mobile data communications,” IEEE Comput.Graph. Appl., vol. 29, no. 6, pp. 74- 81

[6] A. Efros and T. K. Leung, “Texture synthesis by non-parametric sampling”, in Proceedings of 7th IEEE International Conference on Computer Vision, pp. 1033–1038, Sep. 1999.

[7] Efros and T. K. Leung, “Texture synthesis by non-parametric sampling”, in Proceedings of 7th IEEE International Conference on Computer Vision, pp. 1033–1038, Sep. 1999.

[8] L. Liang, C. Liu, Y.-Q.Xu, B. Guo, and H.-Y. Shum, “Real-time texture synthesis by patch-based sampling”, ACM Transactions on Graph Theory, vol. 20, no. 3, pp. 127–150, May 2001.

[9] Efros and W. T. Freeman, “Image quilting for texture synthesis and transfer”, in Proceedings of 28th Annual Conference on Computer Graph. Interaction Technology, pp. 341–346, Sep. 2011.

[10] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEETrans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354- 362, 2006.

[11] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, “Lossless Recovery of an Original Image Containing Embedded Data,” U.S. Patent 6 278 791 B1, Aug. 21, 2001

[12] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su , Reversible Data Hiding , IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, No. 3, March 2006

[13] Chuan Qin , Chin-ChenChang , Yen-ChangChen , Efficient reversible datahiding for VQ-compressed images based on index mapping mechanism , Signal Processing 2687–2695 , 2013.

[14] N.M. Nasrabadi,R.King,Image coding using vector quantization a review,IEEETransactionsonCommunications 36 957–971 , 1988.

[15] C.C. Chang,W.C.Wu,Fast planar-oriented ripple search algorithm for hyperspace VQ codebook,IEEE Transactionson Image Processing 16(6) 1538–1547 ,2007.

[16] Qin, Chuan, Chin-Chen Chang, and Yen-Chang Chen. "Efficient reversible data hiding for VQ-compressed

images based on index mapping mechanism", Signal Processing, 2013.

[17] Wien Hong ,Tung-ShouChen , Mei-ChenWua , An improved human visual system based reversible data hiding method using adaptive histogram modification ,Optics Communications 291 87–97 , 2013

[18] Hong, Wien, Tung-Shou Chen, and Mei-Chen Wu. "An improved human visual system based reversible data hiding method using adaptive histogram modification", Optics Communications, 2013.

[19] FeiPeng, XiaolongLi, BinYang, Adaptive reversible data hiding scheme based on integer transform. Signal Processing (2012) 54–62.