ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Robust and Secure Data Hiding Based On Reversible Method.

R Shalini[1]*, S Sridevi[1], and G Rosline Nesa Kumari[2].

[1]UG, CSE, SSE, Saveetha University Chennai, India
[2]Professor, CSE, SSE, Saveetha University Chennai, India.

ABSTRACT

In this paper, based on two-dimensional difference histogram modification, a novel Reversible Data Hiding (RDH) scheme is proposed by using Difference-Pair-Mapping (DPM). First, by considering each pixel-pair and its context, a sequence consisting of pairs of difference values is computed. Then, a two-dimensional difference-histogram is generated by counting the frequency of the resulting difference-pairs. Finally, reversible data embedding is implemented according to a specifically designed DPM. By the proposed approach, compared with the conventional one-dimensional difference-histogram and one-dimensional prediction-error- histogram-based RDH methods, the image redundancy can be better exploited and an improved embedding performance is achieved. Moreover, a pixel-pair-selection strategy is also adopted to priorly use the pixel-pairs located in smooth image regions to embed data. This can further enhance the embedding performance.

Keywords: Reversible data hiding(RDH),Histogram,Cryptography keys.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Digitization and networking have become more and more evident characteristics in the rapid development of the economic society. The convenient and timely acquisition of on-line services through accessing the Internet is a tidal current for individuals and organizations. However, the transmission of sensitive information via an open Internet channel increases the risk of interception. Thus many techniques have been proposed to deal with this issue. Data hiding, known as information hiding, plays an important role in information security [8]. The main idea of data hiding is that the secret data is concealed into the cover medium, such as an image, audio, video or text, to avoid attracting the attention of attackers in the Internet channel, who may capture the secret data for malicious purposes. In this paper, a novel, reversible, data hiding scheme based on histogram shifting is presented to further improve embedding capacity and image quality. In our scheme [7], All pixels are classified into two types, i.e., wall pixels and non-wall pixels. To conceal secret data, the interpolation errors [19] are performed for the wall pixels. Also, calculate the difference values between the non-wall pixels and their corresponding parent pixels, which are defined according to the direction order, based on the histogram shifting. Experimental results confirm that our scheme can provide larger embedding payload while maintaining better visual quality of the stegno image[2]. The remainder of this paper is organized as follows. Section 2 will review the reversible data hiding scheme of Luo et al. [18]. Then, the proposed scheme is depicted at length inSection3.Section 4 shows the experimental results an relevant discussions.

SYSTEM ANALYSIS

Reversible data hiding in images is a technique that embeds data in digital images by altering the pixel values for secret communication, and the embedded image can be recovered to its original state after the extraction of the secret data[9]. Many reversible data hiding methods have been proposed recently embeds data bits by expanding the difference of two consecutive pixels[4]. Uses a lossless compression technique to create extra spaces for carry data bits. Shifts the bins of image histograms to leave an empty bin for data embedment. Adopts the difference expansion and histogram shifting for data embedment. Embeds data by shifting the histogram of prediction errors while considering the local activity of pixels to further enhance the quality of stego-image. Traditionally, data hiding is used for secret In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in. With the lossy compression method presented in an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied. Based on the homomorphic properties of the underlying cryptosystem, the discrete Fourier transform in the encrypted domain can be implemented. In a composite signal representation method packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data[21].

PROPOSED SYSTEM

In proposed method the image is encrypted by content owner by using the encryption key. The data hider can hide the data in the encrypted image compressing the least significant bits of the encrypted image to obtain the space to hide the data by using data hiding key. At the receiver side the data can be retrieved using the data hiding key by decrypting the image. But, the encrypted image unchanged still it is decrypted using the encryption key. The receiver who has the both the encryption and data hiding keys can access the data embedded as well as the original image.

ISSN: 0975-8585

Proposed system advantages

Two-dimensional difference-histogram is fully utilized . Image redundancy will be better exploited. More data bits can be embedded without degrading the marked image quality. PSNR is slightly improved.

SYSTEM DESIGN

ARCHITECTURE DIAGRAM FOR ENCRYPTION AND DECRYPTION

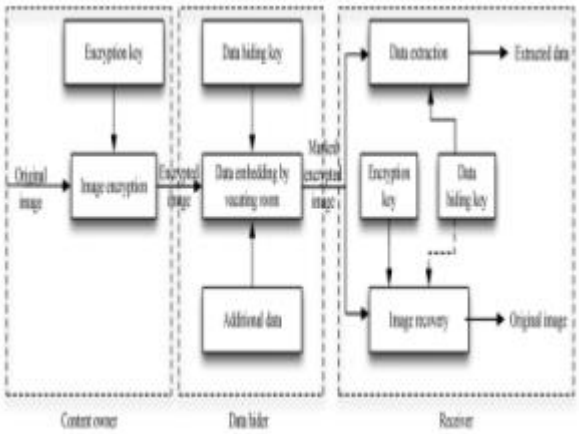

Fig 3.1 Data Encryption

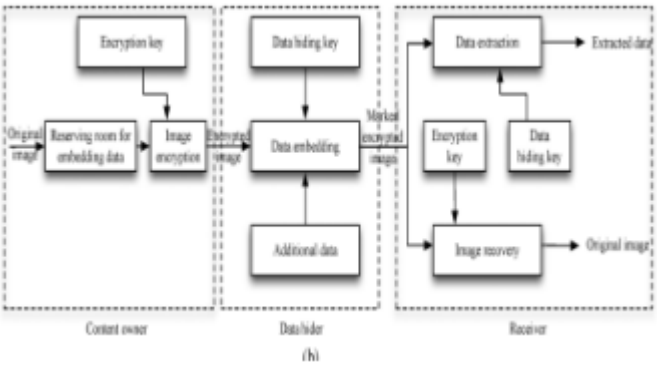

Fig 3.2 Data Decryption

SYSTEM IMPLEMENTATION

SYSTEM DESCRIPTION

The content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out[5]. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

MODULE DESCRIPTION

Module 1: Vacating room after encryption -VRAE

A content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider and the data hider can

embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

Module 2: Reserving room before encryption-RRBE

First reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out[6]. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

Module 3: Generation of Encrypted Image

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition is to construct a smoother area , on which standard RDH algorithms. The above discussion implicitly relies on the fact that only single LSB-plane A of is recorded. It is straightforward that the content owner can also embed two or more LSB-planes A of into B, which leads to half, or more than half, reduction in size. However, the performance of, in terms of PSNR, after data embedding in the second stage decreases significantly with growing bit-planes exploited[11].

Module 4: Image Encryption

Image Encryption is same with other RDH algorithms, overflow/underflow problem occurs when natural boundary pixels change from 255 to 256 or from 0 to -1. To avoid it, we only embed data into estimating error with its corresponding pixel valued from 1 to 254. However, ambiguities still arise when non boundary pixels are changed from 1 to 0 or from 254 to 255 during the embedding process. These created boundary pixels in the embedding process are defined as pseudo-boundary pixels. Hence, a boundary map is introduced to tell whether boundary pixels in marked image are natural or pseudo in extracting process. It is a binary sequence with bit “0” for natural boundary pixel, bit “1” for pseudo-boundary pixel. Since estimating errors of marginal area of B cannot be calculated via (2), to make the best use of B we choose its marginal area shown in Fig. 2 to place the boundary map, and use B LSB replacement to embed it. The original LSBs of marginal area is assembled with messages. In most cases, even with a large embedding rate, the length of boundary map is very short; thus, the marginal area of B is enough to accommodate it.

Module 5: Self-Reversible Embedding

The goal of self-reversible embedding is to embed the LSB- planes of A into B by employing traditional RDH algorithms. For illustration, we simplify the method in to demonstrate the process of self-embedding. Note that this step does not rely on any specific RDH algorithm.

Module 6: Self-Reversible Embedding

(1) Extracting Data From Encrypted Images:

To manage and update personal information of images which are encrypted for protecting clients’ privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case.

(2)Extracting Data From Decrypted Images:

Both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario

CONCLUSION

In this paper, a novel, reversible, data hiding scheme based on histogram shifting is proposed for high quality images. To achieve larger embedding capacity and higher image quality, we classify all pixels as wall pixels and non- wall pixels. The secret message are respectively embedded into wall pixels based on the interpolation errors, and into non- wall pixels according to the difference values between they and their corresponding parent pixels, which are defined by the direction order. By applying histogram shifting to these interpolation errors and difference values, we not only guarantee the high image quality but also provide the large embedding capacity. According to the experimental results, the proposed reversible scheme achieves larger payload and better visual quality than those of some schemes for single layer embedding and multilayer embedding. In addition, the performance of the proposed scheme is more stable for different images.

REFERENCES

[1] J. S. Pan, M. T. Sung, H. C. Huang, B. Y. Liao, Robust VQ-based digital watermarking for the memory less binary symmetric channel, Proceedings of 2004 International Symposium on Circuits and Systems(ISCAS04), vol. 5 ,2004, pp. V-580 - V-583.

[2] M. Iwata, K. Miyake, A. Shiozaki, Digital steganography utilizing features of JPEG images, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E87-A (4) (2004) 929–936.

[3] J. Mielikainen, LSB matching revisited, IEEE Signal Processing Letters,13 (5) (2006) 285–287.

[4] K. S. Kim, M. J Lee, H. Y. Lee, H. K. Lee, Reversible data hiding exploiting spatial correlation between sub-sampled images, Pattern Recognition, 42 (11) (2009) 3083-3096.

[5] C. C. Chanueg, T. D. Kieu, Y. C. Chou, Reversible information hiding for VQ indices based on locally adaptive coding, Journal of Visual Communication and Image Representation, 20 (1) (2009) 57–64.

[6] B. Yang, M. Schumucker, W. Funk, C. Brush, S. Sun, Integer DCT-based reversible watermarking for images using compounding technique, Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents, San Jose, CA, vol. 5306, 2004, pp. 405-415.

[7] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Q. Shi, and Z. Ni, Lossless data hiding using histogram shifting method based on integer wavelets, Proceedings of International Workshop on Digital Watermarking, Lecture Notes in Computer Science, 4283, 2006, pp. 323-332.

[8] C. C. Chang, C. Y. Lin, Y. H. Fan, Lossless data hiding for color images based on block truncation coding, Pattern Recognition, 41 (7) (2008)2347-2357.

[9] J. Tian, Reversible data hiding using difference expansion, IEEE Transactions on Circuits and Systems for Video Technology, 13 (8) (2003) 890-896.

[10] C. C. Chang and T. C. Lu, A difference expansion oriented data hiding scheme for restoring the original host images, The Journal of Systems and Software, 79 (12) (2006) 1754-1766.

[11] C. C. Chang, T. D. Kieu, W. C. Wu, A lossless data embedding technique by joint neighboring coding, Pattern Recognition, 42 (7) (2009) 1597– 1603.

[12] C. C. Lee, H. C. Wu, C. S. Tsai, Y. P. Chu, Adaptive lossless steganographic scheme with centralized difference expansion, Pattern Recognition, 41 (6) (2008) 2097-2106.

[13] C. C. Lin, N. L. Hsueh, A lossless data hiding scheme based on three- pixel block differences, Pattern Recognition, 41 (4) 2008 1415-1425.

[14] Y. C. Li, C. M. Yeh, C. C. Chang, Data hiding based on the similarity between neighboring pixels with reversibility, Digital Signal Processing, 20 (4) 2010 1116-1128.

[15] P. Tsai, Y. C. Hu, H. L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing, 89 (6) 2009 1129-1143.

[16] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Transactions on Circuits and Systems for Video Technology, 16 (3) 2006 354-362.

[17] Z. Zhao, H. Luo, Z. M. Lu, J. S. Pan, Reversible data hiding based on multilevel histogram modification and sequential recovery, International Journal of Electronics and Communications, 2011, doi: 10.1016/j.aeue.2011.01.014.

[18] H. Luo, F. X. Yu, H. chen, Z. L. Huang, H. Li, P. H. Wang, Reversible data hiding based on block median preservation, Information Sciences, 181 (2) (2011) 308-328.

[19] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong Reversible image watermarking using interpolation technique, IEEE Transactions on Information Forensics and Security, 5 (1) (2011) 187-193.

[20] G.Rosline Nesa kumari, L.Sumalatha, Dr.V.Vijayakumar "A Fuzzy Based Chaotic And Logistic Method For Digital Watermarking Systems", International Journal of Scientific & Engineering Researc Publications, Volume 3 , Issue 6, June 2012.

[21] S.Maruthuperumal, G.Rosline Nesakumari, Dr.V.Vijayakumar, "Complete Qualified Significant Wavelet Tree Quantization for Image Watermarking" in International Journal of Computer Science and Technology,Vol.3, Issue 2, April-June 2012.