ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

CONSTRUCTION OF SECURED DATA TRANSMISSION CHANNELS WITH REVERSABLE DATA HIDING SCHEME

Ms. A. Seerin Chithara, II[nd] ME (CSE),
Mrs.Vanitha.K M.E.,Ph.d., Asst. Professor/CSE
Al-Ameen Engineering College, Erode, Tamilnadu, India
seerinkvp@gmail.com

Abstract

Steganography methods are used to hide the secret text into the cover data values. Cover image and secret data are recovered with any noises and errors. Reversible Data Hiding (RDH) method produces the original images in the unhide operations. Histogram construction and histogram modification operations are carried out under the RDH method. Pixel collection and distance values are used in the histogram construction process. Data hide operations are performed in the histogram modification process.

Prediction Error Histogram (PEH) is constructed in the Prediction Error Expansion (PEE) technique. Histogram modification process does not considers the image content values. RDH process is enhanced with multiple histogram based modification mechanism. The hide operations are carried out with the Multiple Histogram Modification(MHM) mechanism. Pixel context based complexity measure is adapted to construct the PEH. Multiple histograms are prepared to cover the complete image.

Embedding capacity enhancement is the main goal of the Reversible Data Hiding (RDH) scheme. Predictor and complexity measure identification operations are upgraded in the system. Frequency variation is considered in the histogram modification process. The secret data security is ensured with the RSA algorithm.

1. Introduction

Modern steganography entered the world in 1985 with the advent of the personal computers being applied to classical steganography problems. Development following that was very slow, but has since taken off, going by the large number of steganography software available. Concealing messages within the lowest bits of noisy images or sound files. Concealing data within encrypted data or within random data. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data.

Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack. Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set. Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications can mean a delay in packets, and the delays in the packets can be used to encode data. Content-Aware Steganography hides information in the semantics a human user assigns to a

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

datagram. These systems offer security against a non-human adversary/warden. Messages are fractionalized and the pieces are added as comments of orphaned web-logs. In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced by Krzysztof Szczypiorski in 2003. Contrary to the typical steganographic methods which utilize digital media as a cover for hidden data, network steganography utilizes communication protocols' control elements and their basic intrinsic functionality. As a result, such methods are harder to detect and eliminate.

Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit), to the time relations between the exchanged PDUs, or both. It is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography. Network steganography covers a broad spectrum of techniques, which include, among others. Steganophony the concealment of messages in Voice-over-IP conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver or, alternatively, hiding information in unused header fields. WLAN Steganography the utilization of methods that may be exercised to transmit steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)

2. Related Work

In 2009, Tsai et al. proposed a reversible data hiding scheme based on prediction and histogram-shifting techniques. For a histogram-shifting based reversible data hiding technique, the payload is determined by the peak height of a histogram. Generally speaking, the higher the peak height of a histogram, the more the payload is. Tsai et al. employed a simple predictor to transform pixels in the spatial domain to error values in the prediction domain [1]. After constructing the error histogram, the histogram-shifting technique is then employed to conceal data. Since the pixels in most natural images are highly correlated, the peak height of error histogram is often higher than that of image histogram. Thus, their method achieves a significant higher payload than that of Ni et al.'s method. The detailed embedding, extraction and restoration procedures of Tsai et al.'s methods are briefly described in the following sub-suctions.

2.1. Embedding procedure

To embed data, the cover image I sizedM×Mis partitioned into N blocks $\{B_i\}^N_{i=1}$. Each block is composed of m×m pixels. In Tsai et al.'s method, setting m= 3 will achieve the best results; therefore, we set m= 3 to illustrate their method. Let c_i be the center pixel of block Bi, and $\{b_{i,j}\}^8_{j=1}$ be the pixels in Bi excluding c_i The center pixel ci is termed the basic pixel of Bi, and $\{b_{i,j}\}^8_{j=1}$ are termed the non-basic pixels of block Bi. An example of the layout of the basic pixel and non-basic pixels in a 3×3 image block. Once the basic

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

pixel and non-basic pixels in each block are determined, data embedding can be summarized.

2.2. Extraction and image recovery procedures

The data extraction and image recovery procedures are similar to that of data embedding procedure. The stego image I' is preprocessed as in the embedding phase: I' of size M×M is partitioned into N blocks $\{B_i\}^N_{i=1}$ with 3×3 pixels. Let c'_i be the basic pixel of B'_i, and $\{b_{i,j}\}^8_{j=1}$ be the non-basic pixels of B'_i, $1 \le i \le N$. Note that $c'_i = c_i$ since the basic pixel c_i is not modified during the embedding phase.

Tsai et al. also used a sophisticated mechanism to avoid the overflow and underflow problems. In Tsai et al.'s method, the nearest prediction technique, for which pixel values are predicted by the nearest basic pixel, is employed. For the histogram based reversible data hiding technique, the peak height of the prediction error histogram determines the payload. Although the payload of Tsai et al.'s method is higher than that of Ni et al.'s method, some useful information provided by adjacent basic pixels of the current basic pixel is not fully explored. Since the values of basic pixels in the cover image are preserved after data embedding, the adjacent basic pixels of the current basic pixels should provide rich clues to have the prediction more accurate. Besides, Tsai et al.'s method does not take the block variance into account; namely, all blocks have equally probability to join the embedding process. High-variance blocks often embed less due to inaccurate prediction.

We use a simple example to illustrate how the block variance affects the payload. The averaged embeddable bits per block for given variance for Lena image. Note that the maximum embeddable bits for a 3×3 block is eight. About 6.5 bits in average can be embedded into blocks with variance 0, whereas only 3 bits can be embedded into blocks with variance 20. This figure reveals that embedding data into low variance blocks often results in a higher payload. The distribution of the averaged embeddable bits per block for Lena image. The grayscale shown in the vertical bar indicates the corresponding averaged embeddable bits. The smooth blocks possess more embeddable bits than those complex blocks.

3. Reversible Data Hiding (RDH) Scheme

Reversible data hiding (RDH) aims to embed secret message into a cover image by slightly modifying its pixels, and more importantly, the original image as well as the embedded message should be completely restored from the marked image [2]. RDH has received much attention from the information hiding community and this technique has also been applied in some applications such as image authentication, medical image processing [7], multimedia archive management, image trans-coding and data coloring in the cloud, etc. In general, RDH is a fragile technique and the marked image cannot undergo any degradation. In this light, a RDH method is usually evaluated by its capacity-distortion performance, i.e., for a given embedding capacity (EC), one expects to minimize the embedding distortion measured by PSNR of the marked image versus the original one.

Early RDH methods are mainly based on lossless compression. The idea behind these methods is to losslessly compress a feature set of cover image and utilize the saved space for reversible embedding. Fridrich *et al.* proposed to compress a proper bit-plane with the minimum redundancy. Celik *et al.* proposed a generalized least significant bit (LSB) compression method to improve the compression efficiency by using unaltered bit-planes as side information. The lossless compression-based methods cannot yield satisfactory performance, since the correlation within a bit-plane is too weak to provide a high EC. As EC increases, one needs to compress more bit-planes, thus the distortion increases dramatically.

More efficient RDH methods based on histogram modification and expansion technique have been devised. The histogram-modification-based method is firstly proposed by Ni *et al.* This method focuses on high visual quality with quite limited EC, in which the peak point of image histogram is utilized for data embedding. In this method, each pixel value is modified at most by 1, and thus the marked image quality is well guaranteed. Ni *et al.*'s method is improved by Lee *et al.* using the histogram of difference image. The spatial correlation of natural images is exploited considering the difference of adjacent pixels. Thus, a regular-shaped histogram is utilized in Lee *et al.*'s method. This histogram is centered at origin and has rapid two-sided decay which is more suitable for RDH. The expansion technique is firstly proposed by Tian. This method is performed on pixel pairs, and one data bit is embedded into each selected pixel pair by expanding its difference. Compared with the lossless-compression based RDH, Tian's difference expansion (DE) based method can provide a higher EC with an improved PSNR. The DE approach has attracted considerable attention and it makes an important progress in RDH. The expansion technique has been widely investigated and developed, mainly in the aspects of integer-to-integer transformation [3],[4], location map reduction and prediction-error expansion (PEE) [5]. Besides the histogram modification and the expansion technique, the analysis about theoretical capacity limit subjected to admissible distortion has also been studied in some recent works [8],[9].

The most effective and extensively exploited RDH technique is the PEE technique which is firstly proposed by Thodi and Rodriguez. Instead of the difference value in DE, the prediction-error is utilized in PEE for expansion embedding. Thus, unlike DE where only the correlation of two adjacent pixels is considered, the local correlation of a larger neighborhood is exploited in PEE. As a result, compared with DE, better performance can be derived by PEE. Following Thodi and Rodriguez's work, many RDH techniques related to PEE have been proposed in recent years, for example, double-layered embedding [11], adaptive embedding, context modification, optimal expansion bins selection [6], [12], and two-dimensional histogram modification, etc. On the other hand, some PEE-based methods [10] exploit advanced prediction techniques to generate a more sharply distributed prediction-error histogram (PEH), and this is also helpful for enhancing the embedding performance.

Most previous PEE-based methods are based on one- or two-dimensional PEH modification. The two-dimensional PEH based methods perform generally better than those based on one-dimensional PEH, their performance is still unsatisfactory since the

PEH modification manner is fixed and independent of image content. In this work, we focus on PEE and propose a new RDH method based on PEE for multiple histograms. Unlike the previous methods, we consider here a sequence of histograms and devise a new embedding mechanism based on multiple histograms modification (MHM). By MHM, the embedding performance can be optimized by adaptively selecting expansion bins in each histogram considering the image content. Specifically, for each pixel, its prediction value and complexity measurement are computed according to its context, and multiple histograms are generated for different complexity levels. That is to say, the pixels with a given complexity are collected together to generate a PEH, and by varying the complexity measurement to cover the whole image, a sequence of histograms can be derived. After that, two expansion bins are selected in each generated histogram and data embedding is realized based on MHM. Moreover, based on an estimation of embedding distortion, the expansion bins can be effectively determined such that the distortion is minimized. The proposed method is a generalization of some existing methods and it can well exploit image redundancy to achieve improved embedding performance. Experimental results show that the proposed method outperforms the conventional PEE (C-PEE) and its miscellaneous extensions including both one- or two-dimensional PEH based ones. Our advantages mainly lie in the MHM-based embedding mechanism and the selection of optimal expansion bins.

4. Problem Statement

Prediction-error expansion (PEE) technique is applied for Reversible Data Hiding (RDH) process. One-or two-dimensional Prediction-error Histogram (PEH) are used in the PEE techniques. The two-dimensional PEH-based methods perform better than one dimensional PEH. PEH modification is fixed and independent of image content. Multiple histograms based PEE method is adopted to improve reversible data hiding (RDH) process. Multiple Histograms Modification (MHM) method uses a sequence of histograms for the hiding process. A complexity measurement is computed for each pixel with reference to its context. Prediction-Error Histogram (PEH) is generated using the pixels with the complexity value. A sequence of histograms can be generated by varying the complexity to cover the whole image. Two expansion bins are selected in each generated histogram. The expansion bins are selected with reference to the image content. Data embedding is carried out on Multiple Histograms Modification (MHM). The following drawbacks are identified from the existing system.

- Embedding capacity (EC) is low
- Predictor selection is not optimized
- Limited embedding performance
- Complexity measure selection is not optimized
- Limited secret data security

5. RSA Algorithm

The domain name service sensitive attributes are secured using the RSA algorithm. The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Key Generation

Select p,q	p and q both prime , $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1; 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Cipher text	$C = M^e \pmod n$

Decryption

Cipher text	C
Plaintext	$M = C^d \pmod n$

6. Secured Data Transmission Channels with RDH

The reversible data hiding scheme is improved with security features. The data values are hided with reference to the histogram information. The RSA algorithm is applied to secure the secret data value. The system is divided into four major modules. They are Sender, Data security, Receiver and Data extraction.

The sender module is designed to send the image data values. Data security is designed to perform hiding and encryption process. Data receiver module collects data from the sender. Data extraction module is designed to perform unhide operations.

The data sender collects secret data and cover data from the user. Prediction-Error Histogram (PEH) technique is used in the system. Multiple Histogram Modification (MHM) is applied with Prediction Error Histogram (PEH) with different complexity levels. Histogram construction is carried out using the cover data image. Data security process is used to hide secret data values. Secret data is converted into bits. RSA algorithm is used to encrypt the data values. The sender collects the public key from the receiver node for the encryption process. Encrypted data values are hided in the cover image.

Data receiver collects data from the sender node. Received data values are updated into the local memory. The received data value is passed to unhide and decrypt process. The receiver node maintains the secret key for decryption process. Secret data is separated from the received data values. Cover data is also separated from the received data values. Decryption process is carried out to fetch the secret data. Cover data quality is analyzed with image quality measures.

7. Conclusion

Reversible Data Hiding (RDH) techniques are used to support data hiding with message and cover image retrieval mechanism. Multiple Histogram Modification (MHM)

scheme is employed for the data hiding process. The system is enhanced to improve the embedding capacity with optimized predictor selection approach. RSA algorithm is adapted to ensure the security level of secret data values. The Multiple Histogram Modification (MHM) scheme is enhanced to improve the embedding capacity. Embedding performance is improved by the system. The system supports efficient coverage image retrieval process. The system reduces the process time in hiding and un-hiding process.

REFERENCES

[1] Wien Honga, Tung-Shou Chen, "A local variance-controlled reversible data hiding method using prediction and histogram-shifting", Elsevier, 2010.

[2] R. Caldelli, F. Filippini and R. Becarelli, "Reversible Watermarking Techniques: An Overview And A Classification," EURASIP J. Inf. Security, vol. 2010, Jun. 2010, Art. ID 134546.

[3] F. Peng, X. Li and B. Yang, "Adaptive Reversible Data Hiding Scheme Based On Integer Transform," Signal Process., vol. 92, no. 1, pp. 54–62, Jan. 2012.

[4] D. Coltuc, "Low Distortion Transform For Reversible Watermarking," IEEE Trans. Image Process., vol. 21, no. 1, pp. 412–417, Jan. 2012.

[5] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens and C. Roux, "Reversible Watermarking Based On Invariant Image Classification And Dynamic Histogram Shifting," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 111–120, Jan. 2013.

[6] I. Caciula and D. Coltuc, "Improved Control For Low Bit-Rate Reversible Watermarking," in Proc. IEEE ICASSP, May 2014, pp. 7425–7429.

[7] F. Battisti, M. Carli and A. Neri, "Secure Annotation For Medical Images Based On Reversible Watermarking In The Integer Fibonacci–Haar Transform Domain," Proc. SPIE, vol. 7870, p. 78700G, Feb. 2011.

[8] W. Zhang, X. Hu, X. Li and N. Yu, "Recursive Histogram Modification: Establishing Equivalency Between Reversible Data Hiding And Lossless Data Compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.

[9] X. Zhang, "Reversible Data Hiding With Optimal Value Transfer," IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316–325, Feb. 2013.

[10] I.-C. Dragoi, D. Coltuc and I. Caciula, "Gradient Based Prediction For Reversible Watermarking By Difference Expansion," in Proc. ACM IH&MMSec, 2014, pp. 35–40.

[11] W. Hong, "An Efficient Prediction-And-Shifting Embedding Technique For High Quality Reversible Data Hiding," EURASIP J. Appl. Signal Process., vol. 2010, May 2010, Art. ID 104835.

[12] L. Dong, J. Zhou, Y. Y. Tang and X. Liu, "Estimation of Capacity Parameters For Dynamic Histogram Shifting (DHS)-Based Reversible Image Watermarking," in Proc. IEEE ICME, Jul. 2014, pp. 1–6.