Authentication of Grey Level Images using a Watermarking Scheme

S.Balusamy
Assistant Professor,
Department of Computer Science
Bharathiar University,
Coimbatore.

Absract

A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. This research proposes a novel digital watermarking scheme to detect fraudulent attacks on an authenticated image committed by a malicious hacker. The proposed method can become aware of any visually significant alteration while maintaining good visual quality. The image is divided into two regions. In the first region authentication signature is embedded. The Authentication signature is obtained by calculating the hash value of the pixels in the second region. In the proposed algorithm security lies on the secrecy of the hash function and the key. Only its owner can insert the correct watermark while any one may verify the authenticity through the corresponding key. XOR based hashing technique had been proposed to maintain the security of the image while transmission. A possible application of the proposed technique is secured transmission of images through network.

1. Introduction

Nowadays, with the rapid development of the Internet, the issue of protecting copyrights of digital contents has become more and more important. Digital watermarking is one way of achieving copyright protection by embedding some message in the protected digital content. The watermark can later be detected or extracted to verify the ownership when the dispute over the copyright of the digital content arises.

Over the past few years, there has been tremendous growth in computer networks and more specifically, the World Wide Web. Digital documents can be distributed via the World Wide Web to a large number of people in a cost-efficient way. The increasing importance of digital media, however, brings also new challenges as it is now straightforward to duplicate and even manipulate multimedia content. There is a strong need of security services in order to keep the distribution of digital multimedia work both profitable for the document owner and reliable for the customer.

Digital watermarks have been proposed as a way to tackle this tough issue. Watermarking technology plays an important role in securing the transmission of digital documents as it allows to place an imperceptible mark in the multimedia data to identify the legitimate owner, track authorized users via fingerprinting or detect malicious tampering of the document. The goal of watermarking and data hiding is to conceal information within a host data set thereby maintaining robustness, imperceptibility and security.

This paper proposes a new method to detect fraudulent alterations committed by a malicious hacker. The proposed scheme encode the watermark prior to watermark embedding to improve tolerance to attacks. This is different from the traditional watermarking schemes that directly embed watermarks into the host images. The remainder of this paper is organized as follows: Section 2 gives an overview of digital water marking. The details of the algorithm is explained in Section 3. Section 4 shows the experimental results and conclusion in section 5.

2. Digital Watermarking

The basic principle of watermarking is to embed information directly into the data, which serves as a host or a cover for that information. It can be described as a visible or preferably invisible identification code that is permanently embedded in the data. In this manner, the watermark travels with the data, which remains protected until its intended receiver removes it.

For a watermark to be effective, it should satisfy the following features. They are:

Unobtrusive: It should be statically and perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it.
Readily Extractable: The data owner or an independent control authority should easily extract it.
Unambiguous: The watermark retrieval should unambiguously identify the data owner.
Innumerable: It should be possible to generate a great number of watermarks, distinguishable from each other.

The proposed scheme contains two important phases: Watermark embedding and watermark extraction. The general representation of a watermarking embedding scheme is given in Fig.1. Watermark is calculated from image and is embedded within it before transmission. The watermarked image is formed so that there is no visible difference between original and itself.

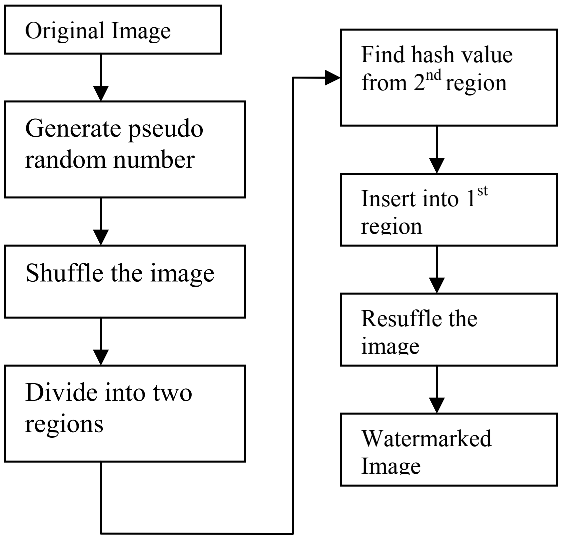

Fig. 1 Watermark embedding

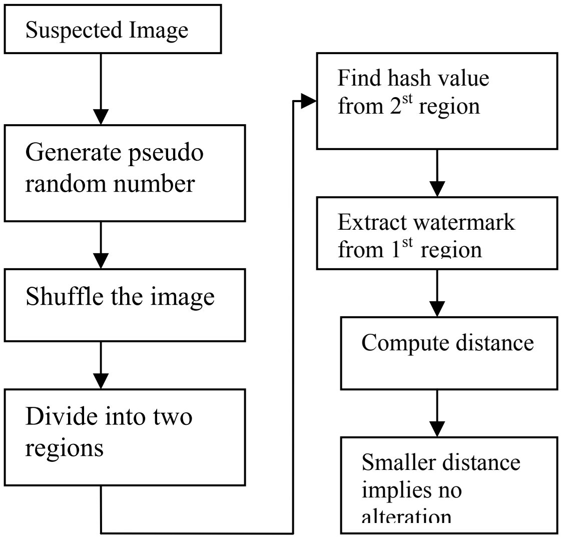
Suspected Image
Generate pseudo random number
Shuffle the image
Divide into two regions
Find hash value from 2st region
Extract watermark from 1st region
Compute distance
Smaller distance implies no alteration

Fig. 2 Watermark verification

At the destination, watermark extraction and verification takes place. A suspected image J is taken and its signal information is obtained. A suspected watermark V is extracted based on knowledge of the original image I and the watermark W. A similarity measure Ψ is performed on V and W. This process is diagrammatically represented in Fig. 2. Finally Ψ is compared to a threshold. If Ψ is smaller than the threshold, then it ensures that image has not been altered.

3. Image Authentication Watermarking

In the proposed system, the data hiding technique used is template ranking. The steps involved are:

(i) Divide the image Z into small blocks, say 8*8.
(ii) Each pixel's visual significance is recognized by identifying its neighborhood. This is done via template ranking where the 512 3*3 binary templates are ranked.
(iii) Template having the property of mirror, transpose, reverse all these are similar ranks. Some of the template patterns are shown in Fig.3.
(iv) Find the highest visibility pixel of the block and store the 0 or 1 in it. But sometimes all the pixels are underlying low visibility problem. To avoid this all the pixel data are shuffled before embedding.

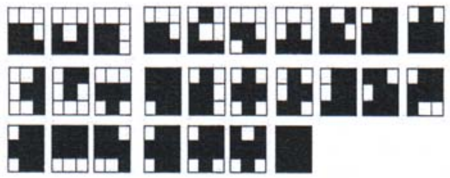

Fig . 3 3x3 templates ranked form left to right

Watermark embedding procedure is processed as follows:

(i) Decide a pseudo random number which should be the known to the receiver side.
(ii) Shuffle the full image Z with suitable shuffling vector V so that the pixels of Z are fully rearranged. The shuffled image is referred as Z′.
(iii) In data hiding algorithm we should split the image block by block, each having 8*8 dimensions of pixels. Let m be the number of pixels of each block and n be the length of Authentication signature (AS). Divide the shuffled sequence Z′ into tow regions namely $Z'_1$and Z'_2.
(iv) First Region Z'_1 should contain n * m pixels where AS is to be stored. These regions are subdivided into n blocks with m pixels. In each block, one bit of AS will be inserted.
(v) Second region Z'_2 which is the remainder of the shuffled sequence Z′. The insertion algorithm will compute AS of this region.
(vi) Select a XOR based hash function H to compute the fingerprint of all the pixels of second region S= H(Z'_2).
(vii) In the first region Z'_1 insert the resultant S. The contents of S are converted into bit pattern and are inserted in every blocks. So n blocks are needed for insertion.

(viii) Then image is reshuffled with the same random vector so that the final modified image(J) is obtained.

The Verification procedure is described as follows:

(i) First all the pixels are shuffled based on the same random basis which is public to the sender and the receiver.
(ii) Divide the suspected image (J) in two regions $J'_1$and J'_2 , by following the same way as done in the insertion step.
(iii) Compute the finger print H of J'_2.
(iv) Extract the Authentication Signature D stored in J'_1.
(v) Find the distance between D and H. If it is smaller then the watermark is verified. Otherwise image J was modified or an incorrect key was used.

4. Experimental Results

Fig.4 is an image of a cameraman, which is the original image. Fig.5 shows the same image after marking. The watermarked image is formed so that there is no visible difference between original and itself.

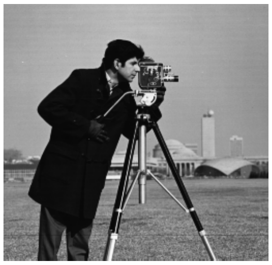

Fig. 4 Original Image

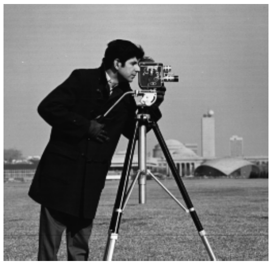

Fig. 5 Watermarked Image

5. Conclusion

This paper proposed a new method for detecting malicious attacks made by the hackers in grey scale images. The technique proposed is Template Ranking which is suitable for watermarking most binary and grey scale images. The proposed method uses public key for authentication. For watermark embedding, the technique used is XOR based hashing technique.

The method using public key authentication can be used for sending documents, images etc., thereby increasing their security.

The image taken into consideration for research is 256*256 bitmap image. This image selection can be extended to other bitmap images too. Other hashing techniques can also be applied for computing the authentication signature. Various image attacks can also be rectified.

6. References

[1]. P. S. L. M. Barreto, H. Y. Kim and V. Rijmen, "Toward a Secure Public-Key Blockwise Fragile
Authentication Watermarking,"*IEE Proc. Vision, Image and Signal Processing*, vol. 149, no. 2, pp. 57-62, 2002.\
[2]. R. de Queiroz and P. Fleckenstein, "Object Modification for Data Embedding through Template Ranking," Xerox Internal Document, 1999.
[3] M. S. Fu and O. C. Au, "Data Hiding Watermarking for Halftone Images," *IEEE Trans. Image Processing*, vol. 11, no. 4, pp.477- 484, 2002.
[4] M. S. Fu and O. C. Au, "A Robust Public Watermark for HalftoneImages," *IEEE Int. Symp. Circuits and Systems*, vol. 3, pp.639-642, 2002.
[5] M. Holliman and N. Memon "Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes," *IEEE Trans. Image Processing*, 2000, vol. 9. no. 3, pp. 432-441.
[6] Chun-Shien Lu and Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and protection", IEEE *Transactions on Image Processing*, Vol.10, 2001.
[7] Bian Yang, Fan Gu and Xiamu Niu "Block Mean Vlaue Based Image Perceptual Hashing", IEEE Proc. Intelligent Information Hiding and Multimedia Signal Processing, 2006.
[8]Schyndel,R.G., Tirkel, A.Z., Osbome,C.F.,1994, A Digital Watermark, Proceedings of the IEEE International conference on Image processing, Austin, Texas, vol.2,pp.86-90.
[9] Hae Yong Kim, Ricardo Lopesde Queiroz "Alteration Locating Authentication Watermark for binary Images" I.J. Cox et al. (Eds.): IWDW 2004, LNCS 3304, pp. 125–136, 2005.Springer-Verlag Berlin Heidelberg 2005.