ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Watermarking of Image Using Priority Based On Algorithms

B.Aarthi, M.Susmitha
Department of Information Technology,
S.A Engineering College, Chennai, India.
aarthi.2396@gmail.com, susmimadesh7@gmail.com

ABSTRACT

This paper presents a novel rank-based method for image watermarking. In the watermark embedding process, the host image is divided into blocks, followed by 2-D discrete cosine transform (DCT). For each image block, a secret key is employed to randomly select a set of DCT coefficients suitable for watermark embedding. Watermark bits are inserted into an image block by modifying the set of DCT coefficients using a rank-based embedding rule. In the watermark detection process, the corresponding detection matrices are formed from the received image using the secret key. Afterwards, the watermark bits are extracted by checking the ranks of the detection matrices. Since the proposed watermarking method only uses two DCT coefficients to hide one watermark bit, it can achieve very high embedding capacity. Moreover, our method is free of host signal interference. This desired feature and the usage of an error buffer in watermark embedding result in high robustness against attacks. Theoretical analysis and experimental results demonstrate the effectiveness of the proposed method.

Key words: Image watermarking, host signal interference, discrete cosine transform, high embedding capacity.

INTRODUCTION

With the fast growth of communication networks and advances in multimedia processing technologies, multimedia piracy has become a serious problem. In an open network environment, digital watermarking is a promising technology to tackle multimedia data piracy. In digital watermarking, the watermark data (such as publisher information, user identity, file transaction/downloading records, etc.) are hidden into the actual multimedia object without affecting its normal usage. When necessary, the owners or law enforcement agencies can extract the watermark data, by using a secret key, to trace the source of illegal distribution. While digital watermarking can be applied to various multimedia data such as audio, image and video, this paper focuses on image watermarking. In the context of image watermarking, imperceptibility, robustness, embedding capacity and security are of primary concerns. So far, various image watermarking schemes have been reported in the literature and many of them were built upon techniques related to histogram [1], [2], moment [3], [4], spatial feature regions [5], [6], spread spectrum (SS) [9]–[14] and quantization [15]–[21]. In many applications, such as covert communication, high embedding capacity is desired, while robustness against geometric attacks is not mainly concerned. Compared to the watermarking methods in [1]–[6], the methods based on SS and quantization can normally achieve higher embedding capacity under given imperceptibility and robustness. The SS-based watermarking methods usually insert watermark bits into the host image as pseudo-random noise either additively or multiplicatively. The idea of SS-based watermarking originated

from Cox's pioneer work. Christo Ananth et al. [7] proposed a system in which an automatic anatomy segmentation method is proposed which effectively combines the Active Appearance Model, Live Wire and Graph Cut (ALG) ideas to exploit their complementary strengths. It consists of three main parts: model building, initialization, and delineation. For the initialization (recognition) part, a pseudo strategy is employed and the organs are segmented slice by slice via the OAAM (Oriented Active Appearance method). The purpose of initialization is to provide rough object localization and shape constraints for a latter GC method, which will produce refined delineation. It is better to have a fast and robust method than a slow and more accurate technique for initialization. The SS-based watermarking approach has simple watermark embedding and detection structure but it suffers from the problem of host signal interference (HSI). It is known that HSI can greatly degrade the performance of watermark detection, especially in the presence of attacks, and thus lower robustness. Cannons and Moulin used the hash information of the host image in both embedding and detection phases of SS-based watermarking to reject HSI but the method is not blind. Christo Ananth et al. [8] proposed a system which uses intermediate features of maximum overlap wavelet transform (IMOWT) as a pre-processing step. The coefficients derived from IMOWT are subjected to 2D histogram Grouping. This method is simple, fast and unsupervised. 2D histograms are used to obtain Grouping of color image. This Grouping output gives three segmentation maps which are fused together to get the final segmented output. This method produces good segmentation results when compared to the direct application of 2D Histogram Grouping. IMOWT is the efficient transform in which a set of wavelet features of the same size of various levels of resolutions and different local window sizes for different levels are used. IMOWT is efficient because of its time effectiveness, flexibility and translation invariance which are useful for good segmentation results. Many efforts have been made to develop blind SS-based methods to cope with HSI. Under the additive SS structure, the method in [9] reduced HSI by modulating the watermark energy based on the correlation between the host image and the watermark sequence. Its detection performance was further enhanced in [10] by utilizing the probability distribution function leakage of the detector. In [11] and [12], two types of new watermark detectors were proposed to tackle HSI, which exploit the hierarchical spatially adaptive image model and the multi-carrier concept, respectively. Under the multiplicative SS structure, some SS-based methods have also been developed to combat HSI [13], [14]. Whilst the methods in [9]–[14] can reduce HSI to certain extents, their performance deteriorates dramatically with the rise of embedding rate.

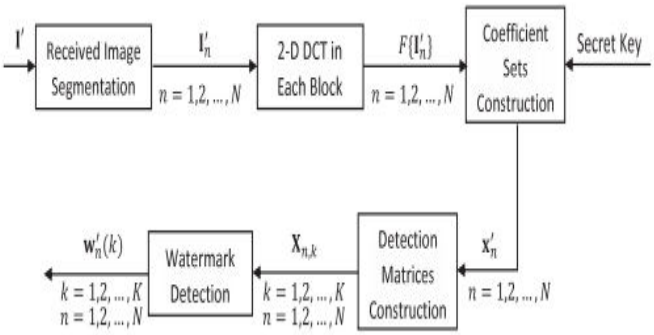
PROPOSED METHOD

The proposed image watermarking method is composed of two parts: watermark embedding and watermark detection. Figs. 1 and 2 show the watermark embedding process and detection process, respectively. A. WATERMARK EMBEDDING Consider a gray level host image I of size R × C. Without loss of generality, I is partitioned into N non-overlapping blocks I1, I2, IN, where the size of each block is M × M and M is a positive integer power of 2. The 2-D DCT is applied to each block to obtain the DCT counterparts F {I1}, F {I2}, F {IN} of dimension M × M. Since low frequency components carry perceptually important information and high frequency components are vulnerable to image compression attack, it is appropriate and common to use the DCT coefficients corresponding to the middle frequency

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

range for watermark embedding. In each block, we use a secret key to randomly select 2K suitable DCT coefficients to form a DCT coefficient set, where the purpose of using a secret key is to introduce security. Denote the length-2K coefficient set in the nth block by Xun = [Xun (1), Xun (2), Xun (2K)]



Block diagram of watermark detection

WATERMARK DETECTION

Denote the received image as I 0. Similar to the embedding process, I 0 is divided into N non-overlapping blocks I 0 1 ,I 0 2 , . . . ,I 0 N of dimension M×M. Applying 2-D DCT to the received image blocks yields the corresponding DCT components F I 0 1 , F I 0 2 , . . . , F I 0 N of dimension M × M. In the nth block F I 0 n, the secret key can be used to find the length-2K DCT coefficient set x 0 n containing K watermark bits.

SELECTION OF WATERMARKING PARAMETERS

In the proposed watermarking method, α, β and T are three important watermarking parameters and their values need to be properly chosen. The parameter T is the threshold of the error buffer, which is primarily introduced to resist Gaussian noise addition attack. The selection of T will be discussed in the analysis of robustness against Gaussian noise addition in Subsection III-A. So, we only discuss how to select α and β in this subsection.

ANALYSIS OF ROBUSTNESS AGAINST ATTACKS

The types of attacks considered in include Gaussian noise addition, amplitude scaling, constant luminance change and compression. In this section, we analyze the robustness of the proposed method against these attacks.

ROBUSTNESS AGAINST GAUSSIAN NOISE ADDITION

The robustness of the proposed method against Gaussian noise addition is facilitated by the error buffer term ban in (13). This can be explained by showing the relationship between the error probability caused by Gaussian noise addition and the buffer threshold T. We assume that in the DCT domain, the Gaussian noise follows the normal distribution Norm (0, σ2) who's mean and variance are 0 and σ 2, respectively.

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

SIMULATION RESULTS

In this section, we evaluate the performance of the proposed image watermarking method by simulations, in comparison with the methods in [12], [19], and [21]. Eight standard 512 × 512 8-bit gray scale images Bee, Elaine, Gold hill, Hill, Lena, Lighthouse, Truck, and Zelda are used as host images, which are shown in the top two rows of Fig. 4. The peak signal-to-noise ratio (PSNR) index and the bit error rate (BER) index are used to measure perceptual quality and robustness, respectively. The performance indices PSNR and BER are calculated by averaging the results obtained from the eight images. Regarding imperceptibility, the larger PSNR value, the better perceptual quality. It is mentioned in [25] that the PSNR value of 40dB indicates good perceptual quality. For example, the bottom two rows of Fig show the watermarked counterparts of the afore-mentioned eight images by our method, where PSNR = 40.32 dB. Clearly, there is no visual difference between the original images and their watermarked versions. With regard to robustness, a smaller BER value indicates better robustness, and vice versa.

Upper two rows: original images Bee, Elaine, Gold hill, Hill, Lena, Lighthouse, Truck, and Zelda. Lower two rows: watermarked counterparts of these images, where PSNR = 40.32 dB.

CONCLUSION

In this paper, we proposed a novel method for image watermarking in the DCT domain. Thanks to the rank-based watermark embedding and detection rules, the proposed watermarking method possesses some desirable features. Firstly, our method can use as little as two DCT coefficients to embed one watermark bit. Secondly, it is free of HSI. Thirdly, it can considerably tolerate the errors caused by attacks. The first feature leads to high embedding capacity. The second and third features make the proposed method robust against common attacks. The superior performance of the new method was analyzed theoretically in detail and demonstrated by simulation results.

REFERENCES

[1] S. Xiang, H. J. Kim, and J. Huang, ''Invariant image watermarking based on statistical features in the low-frequency domain,'' IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.

[2] T. Zing, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and G. Beliakov, ''Robust histogram shape-based method for image watermarking,'' IEEE Trans. Circuits Syst. Video Technol., vol. 25, no. 5, pp. 717–729, May 2015.

[3] M. Alghoniemy and A. H. Tewfik, ''Geometric invariance in image watermarking,'' IEEE Trans. Image Process., vol. 13, no. 2, pp. 145–153, Feb. 2004.

[4] P. Dong, J. G. Baranov, N. P. Galatians, Y. Yang, and F. Davion, ''Digital watermarking robust to geometric distortions,'' IEEE Trans. Image Process., vol. 14, no. 12, pp. 2140–2150, Dec. 2005.

[5] J. S. See and C. D. Yoo, ''Image watermarking based on invariant regions of scale-space representation,'' IEEE Trans. Signal Process., vol. 54, no. 4, pp. 1537–1549, Apr. 2006.

[6] X. Gao, C. Deng, X. Li, and D. Tao, ''Geometric distortion insensitive image watermarking in affine covariant regions,'' IEEE Trans. Syst., Man, Cyber. C, Appl. Rev., vol. 40, no. 3, pp. 278–286, May 2010.

[7] Christo Ananth, B.Gayathri, I. Uma Sankari, A.Vidhya, P.Karthiga, "Automatic Image Segmentation method based on ALG", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 2, Issue 4, April 2014,pp- 3716-3721

[8] Christo Ananth, A.S.Senthilkani, Kamala Geometry, J.Arockia Renaldo, G.Blesslin Jeritza, Sankari @Sarnia's., "Color Image Segmentation using IMOWT with 2D Histogram Grouping", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 5, May 2014, pp-1 – 7

[9] H. S. Malvern and D. A. F. Florencio, ''Improved spread spectrum: A new modulation technique for robust watermarking,'' IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898–905, Apr. 2003.

[10] Valizadeh and Z. J. Wang, ''Correlation-and-bit-aware spread spectrum embedding for data hiding,'' IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 267–282, Jun. 2011.

[11] K. Mairgiotis, N. P. Galatians, and Y. Yang, ''New additive watermark detectors based on a hierarchical spatially adaptive image model,'' IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 29–37, Mar. 2008.

[12] M. Li, M. K. Kulhandjian, D. A. Pads, S. N. Bata lama, and M. J. Medley, ''Extracting spread-spectrum hidden data from digital media,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1201–1210, Jul. 2013.

[13] Q. Cheng, ''Generalized embedding of multiplicative watermarks,'' IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 978–988, Jul. 2009.

[14] Valizadeh and Z. J. Wang, ''an improved multiplicative spread spectrum embedding scheme for data hiding,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1127–1143, Aug. 2012.

[15] Chen and G. W. Worn ell, ''Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,'' IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.

[16] S.-H. Wang and Y.-P. Lin, ''Wavelet tree quantization for copyright protection watermarking,'' IEEE Trans. Image Process., vol. 13, no. 2, pp. 154–165, Feb. 2004.

[17] N. K. Calamari and S. M. Avadi, ''A logarithmic quantization index modulation for perceptually better data hiding,'' IEEE Trans. Image Process., vol. 19, no. 6, pp. 1504–1517, Jun. 2010.