Advanced Materials Research Vols. 765-767 (2013) pp 1113-1117 *Online: 2013-09-04*
© (2013) Trans Tech Publications, Switzerland
doi:10.4028/www.scientific.net/AMR.765-767.1113

Study on the Digital Image Zero-watermarking Technology

LENG Xiao-xu[a], XIAO Jun[b], LI Deng-yu[c] and SHEN Zhen-ya[d]

University of the Chinese Academy of Sciences, Beijing 100049, China

[a]email: lengxiaoxu@163.com, [b]email: xiaojun@gucas.ac.cn, [c]email: 704192748@qq.com, [d]email: szy-b09@mails.gucas.ac.cn

Keywords: Zero-watermarking; information security; image feature; copyright protection; watermark

Abstract. Recently more and more researches in the information security field have been focused on the digital image zero-watermarking technology which is an important mean for protecting the digital multimedia copyright. In this paper, first the research background of image zero-watermarking is analyzed; and then the typical algorithms are presented and discussed; finally the performance of these typical algorithms are analyzed and experimented.

Introduction

With the rapid development of digital multimedia technologies and Internet, the storage, replication and transmission of multimedia information has become very convenient. Because of the characteristics of the digital multimedia itself [1], products could be copied and pirated easily. Therefore an effective solution has been proposed to protect the copyright of digital multimedia by the digital watermarking technology.

But a few problems still occur in practice [2, 3]. For example, whether it's necessary to control the generation of the watermarks, or who should be responsible for embedding watermarks etc.

For the above problems, a secure watermarking architecture was proposed by Mao et al [4], which makes use of the IMPRIMATUR (The Intellectual Multimedia Property Rights Model and Terminology for Universal Reference) – an architecture for IPR (Intellectual Property Rights) protection [5]. IMPRIMATUR could ensure to provide a feasible protective measure under the condition that the watermarking algorithm is safe. But what if there is a loophole in the watermarking algorithm?

The security problems that exist in the traditional digital watermarking algorithms were studied by Craver et al. [6], who pointed out that no quasi-invertible technique could be very difficult. In order to solve these problems, [3] points out that it's the embedding algorithm that courses the security problems. Attackers could hardly find security vulnerabilities if there is no embedding procedure, and zero-watermarking is introduced to tackle the security problems [3]. The image zero-watermarking, which is an important branch of zero-watermarking, constructs watermarks based on the main features of images, and stores watermarks into IPR databases.

The typical methods of image zero-watermarking are introduced in this paper, and then the advantages and disadvantages of these methods are analyzed which are verified in the following experiments, finally the development prospects are pointed out.

Image Zero-watermarking Typical Algorithms

The current research on image zero-watermarking is mainly focused on the space domain (Most Significant Bit (MSB), High-order Cumulant (HOC) and Scale Invariant Feature Transform (SIFT) features etc.), the transform domain (Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) etc.), the moments of images (Hu's Moments, Zernike Moments, and Wavelet Moments etc.), principal component analysis (PCA) and singular value decomposition (SVD) etc. five fields.

(1) Space Domain

The space features of images mainly include MSB, HOC and SIFT features etc. three categories.

The image zero-watermarking algorithms based on MSB construct zero watermarks using MSB [7]; the image zero-watermarking algorithms based on HOC construct zero watermarks based on three order and four order cumulants [3]; the zero-watermarking algorithms based on SIFT features construct zero watermarks based on features located in larger scale space and their corresponding descriptors [8].

(2) Transform Domain

The image features in transform domain mainly include the alternating current (AC) coefficients of DCT domain and the low frequency coefficients of DWT domain etc. two categories.

The image zero-watermarking algorithms based on DCT construct zero watermarks using AC coefficients which have large absolute values [9]; the image zero-watermarking algorithms based on DWT construct zero watermarks using the low frequency coefficients of DWT domain [10].

(3) Moment

The main features of images could be extracted by calculating varieties of image moments. The moments usually used mainly include Hu's moments, Zernike moments and wavelet moments etc. three categories.

The image zero-watermarking algorithms based on Hu's moments construct zero watermarks using the seven moments of invariance which can resist RST (Rotation, Scale and Translation) attacks [11]; the image zero-watermarking algorithms based on Zernike moments construct zero watermarks based on amplitudes of Zernike moments which have characteristics of rotation invariance and reversal invariance [12]; the image zero-watermarking algorithms based on wavelet moments construct zero watermarks using wavelet moments which can resist RST attacks [13].

(4) PCA

Due to the connectivity among image pixels in adjacent space, the image can be divided into nonoverlapping blocks which can be reflected into vectors, based on which the K-L transform is performed on the vector set. After being transformed, the first few elements in each vector accommodate the main feature information of the corresponding image block.

The image zero-watermarking algorithms based on PCA construct zero watermarks using the principal components of each image block being transformed [14].

(5) SVD

SVD is a numerical algorithm which diagonalizes matrices. The singular values of images have very stable properties. When the perturbation is exerted to an image, the singular values of that image will not change so much, therefore the main feature information of images are contained in the singular values.

The image zero-watermarking algorithms based on SVD construct zero watermarks using singular values of images [15].

Performance Comparison and Analysis

The typical image zero watermarks construction methods were introduced in previous section, in this section five most representatives are selected with their performance to be analyzed and compared. Among the five representative algorithms, algorithm 1 is based on MSB [7]; algorithm 2 is based on DCT [9]; algorithm 3 is based on Zernike moments [12]; algorithm 4 is based on PCA [14]; algorithm 5 is based on SVD [15].

In this section, the performance of the five algorithms will be discussed in the following four parts: (1) the watermark capacity; (2) the time complexity; (3) the robustness resisting general signal process; (4) the robustness resisting affine attacks. In order to make the discussion to be concrete, the carrier image size is supposed to be 256×256.

A. Watermark Capacity

The capacity of zero watermarks must be big enough to improve the distinguishing of zero-watermarking, and could insert more copyright information.

Algorithm 1 could construct 1 bit zero watermark according to 1 pixel, therefore it could construct 65536 bits zero watermarks; algorithm 2 is based on DCT, the number of AC coefficients with large absolute values tends to be set to 1024 bits in practice; algorithm 3 is based on Zernike moments, in practice we set $n_{\min} = 2, n_{\max} = 30$, then it could construct 254 bits watermarks; algorithm 4 is based on PCA, the number of vectors tends to be set to 1024 in practice, but the zero watermarks are constructed by comparing the adjacent principal components, so the watermark capacity is 512 bits; algorithm 5 is based on SVD, the level of wavelet transform is set to be 2, and the block size is set to be 8×8, then it could construct 256 bits watermarks.

To sum up, algorithm with largest capacity is algorithm 1; second is algorithm 2; third are algorithm 4 and 5; algorithm 3 has the smallest capacity.

B. Time Complexity

Due to the largely identical processes of construction and detection in zero-watermarking, and in the detection process has just one more step which is similarity calculation than in the construction process, therefore the time complexity of these algorithms can be reflected in the time complexity of the construction processes only. And the theories referred to in some algorithms are rather complex, the quantitative analysis is very difficult in theory, so the time complexities of these algorithms are evaluated in form of experiment data.

In the evaluation experiment, the Matlab R2009b is selected as the simulation platform, and the time used to extract watermarks is obtained from five images (as shown in Fig. 1) on which performing each algorithm respectively. The experiment results are shown in Tab. 1. The five first rows show the time used to construct watermarks on each image by each algorithm respectively, and the bottom row shows the average time used to construct watermarks on the five images by each algorithm. It can be inferred based on Tab. 1 that algorithm 3 has the highest time complexity, second is algorithm 1, and algorithm 2, 4, and 5 have somewhat low time complexities.

(a) Image 1 (b) Image 2 (c) Image 3 (d) Image 4 (e) Image 5

Fig.1. Experimental images

C. Robustness Resisting General Signal Process

The general signal processing usually occurs in stages of processing and disseminating multimedia products, and resisting which is a basic ability of image zero-watermarking algorithms. JPEG compression, noises and filter are common operations of general signal process. In this section, we present three experiments to evaluate the robustness of these five algorithms resisting JPEG compression, gaussian noises and mean filter.

Fig. 2 shows the comparison of experimental results among the five algorithms resisting JPEG compression. The results indicate that all these algorithms have strong robustness against JPEG compression, while the algorithm based on DCT has the best performance, second is algorithms based on Zernike moments and PCA, and third is algorithms based on MSB and SVD.

Fig. 3 shows the comparison of experimental results among the five algorithms resisting gaussian noises. The results indicate that all these algorithms can resist gaussian noises effectively, while the algorithm based on DCT has the strongest robustness, second is algorithms based on Zernike moments, PCA and SVD, and the algorithm based on MSB has the weakest robustness.

Tab. 2 shows the comparison of experimental results among the five algorithms resisting mean filter. The results indicate that algorithms based on DCT and PCA have best performance, second is algorithms based on Zernike moments and MSB, and the algorithm based on SVD has the worst performance.

The three experimental results indicate that all these algorithms can resist general signal process effectively, and the algorithms based on DCT and PCA have the best effect, second is the algorithm based on Zernike moments, and the algorithm based on SVD and MSB have the relatively worse effects.

Tab.1. Time comparison of 5 algorithms constructing watermarks

Images	Time (s) Used For Constructing Watermarks				
	MSB	*DCT*	*Zernike*	*PCA*	*SVD*
Image 1	2.6542	0.0949	6.9833	0.1360	0.1862
Image 2	2.6374	0.0963	6.9659	0.1373	0.1870
Image 3	2.6569	0.0980	6.9804	0.1389	0.1863
Image 4	2.6584	0.0969	6.9428	0.1381	0.1853
Image 5	2.6542	0.0974	6.9898	0.1395	0.1847
Mean Time	2.6522	0.0967	6.9724	0.1379	0.1859

Tab.2. Comparison of 5 algorithms resisting mean filter

Template Parameter	*MSB BER*	*DCT BER*	*Zernike BER*	*PCA BER*	*SVD BER*
3*3	0.0211	0.0000	0.0157	0.0176	0.0352
5*5	0.0372	0.0068	0.0157	0.0293	0.0898
7*7	0.0505	0.0459	0.0236	0.0332	0.1094

D. Robustness Resisting Affine Attacks

The algorithm based on MSB constructs zero watermarks based on the space domain, which makes it have strong robustness against cropping; the other four algorithms have robustness against cropping as well, while the algorithm based on the integral DCT has relatively weaker robustness.

Among the five algorithms, only the algorithm based on Zernike moments can resist rotation attacks, the rest can resist rotation attacks with small angles; and only the algorithm based on Zernike moments can resist affine attacks with scale changes, the rest call for the identical size of the carrier image when detecting watermarks from the detected images.

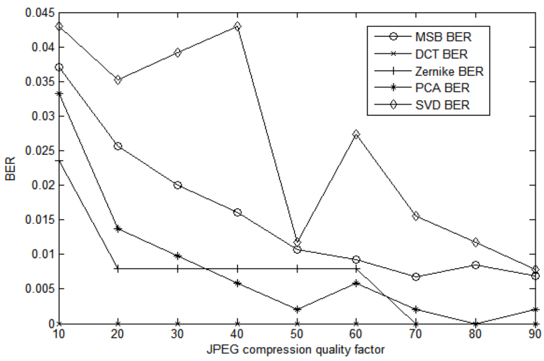

Fig.2. Comparison of 5 algorithms resisting JPEG compression

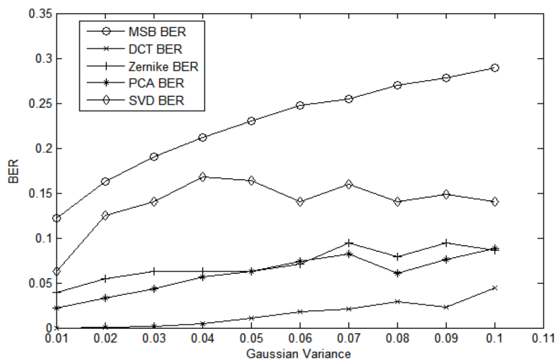

Fig.3. Comparison of 5 algorithms resisting gaussian noise

Conclusion

In this paper, the image zero-watermarking technology was introduced and reviewed. And the typical image zero-watermarking algorithms were studied in theoretical analysis and experimental evaluation two aspects. In general, all these zero-watermarking methods obtain good performance, but still have some defects respectively. For example, in aspect of resisting general signal process, most of them show robustness; while in aspect of resisting affine attacks, only a few of them show robustness, even so the few methods are not perfect in every way, because they have little ability to resist combinational attacks. There are varieties of attacks at present, which calls for methods as perfect as possible to resist as many attacks as possible and have lower false alarm rates in the meanwhile.

Through analyzing the theory and performance of image zero-watermarking algorithms, the algorithms which can resist combinational attacks can be studied in the following three aspects: (1) the majority of algorithms construct watermarks based on the integral image features, once the integral image feature is damaged the algorithms based on which cannot detect watermarks, therefore the local image features could be used to construct watermarks; (2) although there are some algorithms based on local image features, the false alarms of them are relatively high, in order to reduce the false alarm rates the topology information of these local feature points can be introduced; (3) consider jointly put methods based on integral image features and methods based on local image features together to improve robustness and reduce the alarm rates in the meanwhile.

Acknowledgement

This work is supported by National Natural Science Foundation of China (No.61003275) and the President Fund of CAS.

References

[1] Y. Wang, J. Xiao and Y.H. Wang, “Digital Watermarking Principles and Techniques,” Beijing: Science Press, pp. 1-6, 2007. (In Chinese)

[2] Q.D. Zhou, “Research on Digital Image Copyright Protection Based on Non-watermarking,” Wuhan: Huazhong University of Science & Technology, pp. 9-12, 2004. (In Chinese)

[3] Q. Wen, “Research on Robustness and Imperceptibility of Multimedia Digital Watermarking,” Jilin: Jilin University, 2005. (In Chinese)

[4] Q. Mao, Y.X. Yang and T.N. Tan, “The Research of Secure Digital Watermarking Architecture,” Journal of Electronics and Information Technology.vol.23(9), pp. 833-840, Sept. 2001. (In Chinese)

[5] Daniel Augot,Jean-Marc and Jean-Francois, “Secure delivery of image over open networks,” Proc.IEEE,vol.87(7), pp. 1251-1266, July 1999.

[6] Scott Craver, Nasir Memon and Boon-Lock Yeo, “Resolving Rightful Ownerships with Invisible Watermarking Techniques : Limitations, Attacks, and Implications,” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, vol.16(4), pp. 573-586, Nov.1998.

[7] W.H. Niu, S.H. Yang, “A Non-Watermarking Algorithm Based on the MSB Structure Key,” Computer Engineering & Science, vol.32(4), pp. 55-58, Apr. 2010. (In Chinese)

[8] X.Y. Zhao, J.Y. Sun, “Novel zero-watermarking based on SIFT feature of digital image,” Application Research of Computers, vol.4(27), pp. 1517-1520, Apr. 2010. (In Chinese)

[9] Q. Wen, T.F. Sun, S.X. Wang, “Concept and Application of Zero-Watermark”, Acta Electronica Sinica, vol.31(2), pp. 214-216, Feb. 2003. (In Chinese)

[10] J.H. Ma, J.X. He, “A Wavelet-Based Method of Zero-Watermark,” Journal of Image and Graphics, vol.12(4), pp. 581-585， Apr. 2007. (In Chinese)

[11] Y.T. Zhai, D.Y. Peng, “A image zero-watermarking scheme for resist geometric attacks,” Information Technology,vol. 11, pp. 33-35, Nov. 2007. (In Chinese)

[12] D.W. Xu, J.C. Wang and R.D. Wang, “An Object-based Video Zero-watermarking Algorithm Using Zernike Moments,” Journal of Image and Graphics, vol.14(9), pp. 1825-1931, Sep. 2009. (In Chinese)

[13] J.H. Wu, “Research on Zero Watermarking Algorithm Based on Wavelet Moment,” Chongqing: Chongqing University, 2009. (In Chinese)

[14] Y.F. Hu, S.A. Zhu, “Zero-watermark algorithm based on PCA and chaotic scrambling”, Journal of Zhejiang University(Engineering Science), vol.42(4), pp. 593-597, Apr.2008. (In Chinese)

[15] T.Y. Ye, Z.F. Ma, X.X. Niu, etc, “A Zero-Watermark Technology with Strong Robustness”, Journal of Beijing University of Posts and Telecommunications, vol.33(3), pp. 126-129, June. 2010. (In Chinese)

Advanced Information and Computer Technology in Engineering and Manufacturing, Environmental Engineering
10.4028/www.scientific.net/AMR.765-767

Study on the Digital Image Zero-Watermarking Technology
10.4028/www.scientific.net/AMR.765-767.1113