

An Optimum Method Research Based on Bit Plane Combination of Digital Image and Fingerprint Watermarking*

ZHAO Huimin^{1,2}, GUO Yizhen², DING Xiaoyan²

(1. Guangdong Polytechnic Normal University, School of Electronic and Information, Guangzhou 510665, China;

2. Xi'an University of Posts & Telecommunication, School of Communication and Information Engineering, Xi'an 710121, China)

Abstract: To enhanced robustness and capacity as well as maintains of image transparency of the watermark, a novel watermarking technique combination bit plane is proposed. In this method, carrier image and fingerprint image are decomposed into bit planes after discrete multiwavelet transform (DMWT), respectively. By means of the ranked bit-stream of the image sub-band coefficients using the bit planes combination, the method may adaptively embed hidden fingerprint data into wavelet sub-band coefficients. Experimentation results shows that the algorithm achieves better tradeoff between invisibility and robustness in various Conditional compression.

Key words: bit plane; fingerprint; digital watermark; correlation coefficient

一种数字图像和指纹水印位平面合成的优化方法

赵慧民^{1,2}, 郭一镇², 丁晓艳²

(1. 广东技术师范学院电子与信息学院, 广东 广州 510665;

2. 西安邮电学院通信与信息工程学院, 陕西 西安 710121)

摘要: 为了提高水印鲁棒性、容量以及透明性, 提出了利用图像位平面合成实现的一种新的水印技术。在此技术中, 经离散多小波变换 (DMWT) 变换后, 载体图像和指纹图像分别被分解成不同的位平面。借助于图像子带系数在位平面的排列顺序, 这种方法通过位平面合成可自适应地把指纹数据嵌入到小波子带系数中。结果表明, 在不同条件压缩攻击下, 方法达到了不可见性和鲁棒性的一种折中。

关键词: 位平面; 指纹; 数字水印; 相关系数

中图分类号: TP309 **文献标志码:** A **文章编号:** 0529-6579 (2010) 06-0064-05

1 Introduction

Information hiding technology is an emerging research area which encompasses application such as copyright protection for digital media, watermarking,

fingerprinting, steganography, and data embedding^[1]. In the past literature on watermarking, it is observed that bit plane method is one of the recommended methods of watermarking in spatial domain. This method is characterized by spread spectrum and is blind while

* 收稿日期: 2010-04-06

基金项目: 国家自然科学基金重点资助项目 (60633030); 国家自然科学基金资助项目 (90604008); 广东省自然科学团队基金资助项目 (04205407)

作者简介: 赵慧民 (1966年生), 男, 博士, 教授; E-mail: zhaohuimin@tom.com

watermark retrieval^[2]. Optimal implementation of this method maximizes the fidelity and robustness against different attacks. This method is based on the fact that the least significant bit plane of the image does not contain visually significant information. Therefore it can be easily replaced with watermark bits without affecting the quality of original image^[3-4]. However the survival of the watermark is an open issue and two main drawbacks of inserting watermark in least significant and most significant bits are:

1) If watermark is inserted in least significant bit planes, then the watermark may not survive against coding, channel noise, mild filtering or random bit-flipping.

2) On the other hand, if the watermark is embedded in most significant bit plane, watermark survives but image quality is degraded.

Therefore, to get optimal results, in terms of fidelity, robustness, and high embedding capacity, a new bit plane modification method is proposed in this paper.

To overcome above problems, we propose the novel method for image watermarking. Proposed method differs in two different ways than the earlier technique of bit plane watermarking^[5-6]. Firstly, to prove the ownership or identify the owner, most effective digital signature watermark (as fingerprint data) is embedded instead of pseudorandom watermark. Secondly, instead of LSB, a previous bit to LSB is identified for watermark embedding to avoid the degradation of image and to survive the watermark after different general attacks like various Conditional compression.

2 Proposed Watermarking Algorithm

Without significant loss of generality, we shall focus on watermarking still images with 256 gray levels of size 512×512 pixels. To trade off between the invisibility and robustness of the watermark, the high-energy sub-band (LL4) is not used. Furthermore, the coefficients in high frequency subbands (LH1, HL1 and HH1) are not used since they often contain few energy. In other subbands, we group the coefficients corresponding to the same spatial location together. Figure 1 shows an example of a group with one coefficient from HL4, 4 coefficients from HL3, and 16 coefficients

from HL2^[7-9].

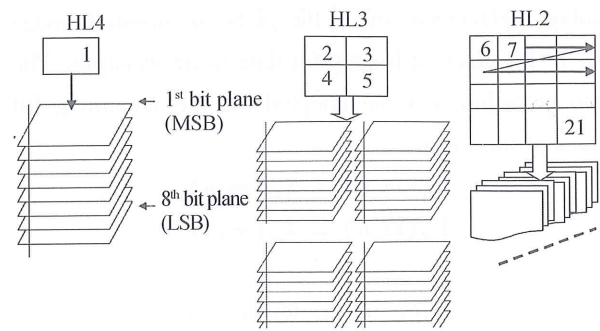


Fig. 1 A group of multiwavelet coefficients and Bit plane representation

Let $X(m, n)$ be the grey level image and $W(m, n)$ be the fingerprint image, The grey level image is transformed into the watermarked image $Y_w(m, n)$ by DMWT with fingerprint data embedded. The grey scale image X is defined as follows: $X = \{X(m, n), m \in \{1, \dots, M\}, n \in \{1, \dots, N\}\}$, and M, N are maximum dimensions of an image, where $X(m, n) \in \{0, \dots, 255\}$ total number of grey levels^[10-11]. Step by step algorithm for proposed method is explained below:

Step 1: Decompose the grey level image to bit planes: Grey level image is decomposed in to bit plane image. Each pixel in the image is represented by 8-bits. Therefore the image is decom-posed into eight 1-bit planes, ranging from 8th bit plane for LSB to 1st bit plane for the MSB. The 8th bit plane contains all the lowest order bits in the pixels comprising the image and 1st bit plane contains all the higher order bits as shown in Fig. 1.

The image would be decomposed in to bit planes as follows. A subband coefficient Decomposition of original image into 8-bit planes:

$$X_l(m, n) = X_{b1}(m, n) + X_{b2}(m, n) + \dots + X_{b8}(m, n) \quad (1)$$

Similarly, decomposition of fingerprint image into 8-bit planes:

$$W_k(m, n) = W_{b1}(m, n) + W_{b2}(m, n) + \dots + W_{b8}(m, n) \quad (2)$$

Where l and k indicates number of bit planes of image and $\in \{b1, b2, \dots, b8\}$.

Step 2: Replace the significant bit plane of original image with fingerprint bit plane (this is done so as to

decide by HVS), which bit planes of the image are good for watermarking^[12]. Following set of equations display replacement of 7th bit plane of original image with 1st bit plane of fingerprint data as an example. The same procedure can be adopted for the remaining bit planes of the image.

$$\begin{aligned} Y_{b1}(m,n) &= X_{b1}(m,n) \\ Y_{b2}(m,n) &= X_{b2}(m,n) \\ &\dots \\ Y_{b7}(m,n) &= W_{b1}(m,n) \\ Y_{b8}(m,n) &= X_{b8}(m,n) \end{aligned} \quad (3)$$

Combination watermarked image is as follows:

$$Y_w(m,n):Y_w(m,n) = Y_{b1}(m,n) + Y_{b2}(m,n) + \dots + Y_{b8}(m,n) \quad (4)$$

This bit plane watermarked image $Y_w(m,n)$ is recomposed in to grey level image $I(m,n)$ by IDMWT.

Step 3: Formulation for watermarked image subjected to attacks: In real life when watermarked image is distributed on the World Wide Web, it is encountered by different attacks. In this step, watermarked image is subjected to different types of attacks, leading to attacked image as $I_i^*(m,n)$, $i \in$ difference attacks.

Step 4: Watermark Retrieval: In this step attacked image $I_i^*(m,n)$ is again transformed in to binary image i. e. 8-bit planes as shown below.

$$I_{il}^*(m,n) = I_{ib1}^*(m,n) + I_{ib2}^*(m,n) + \dots + I_{ib8}^*(m,n) \quad (5)$$

Extract the watermark bit plane from the attacked image. This retrieved watermark after attack, is denoted as $W_{ib1}^*(m,n)$.

Step5: Computation of CRC: Correlation coefficient between retrieved watermark and original fingerprint is estimated using a standard equation (6)^[4]. The estimated correlation coefficients are denoted as $CRC_i(l,k)$. Where, i indicate different attacks, l is taken as 7th and 8th bit planes of original image as selected in step 2 and k denotes the bit planes of fingerprint watermark from 1 to 8. The quality of watermarked image is observed by HVS. CRC varies between 0 and 1. CRC is defined as given below:

$$CRC = \frac{\sum_{m=1}^{256} \sum_{n=1}^{256} W(m,n) \cdot W^*(m,n)}{\sqrt{\sum_{m=1}^{256} \sum_{n=1}^{256} W(m,n) \cdot \sum_{m=1}^{256} \sum_{n=1}^{256} W^*(m,n)}} \quad (6)$$

$$\text{if CRC} = \begin{cases} 1, & \text{highly robust watermarking} \\ 0, & \text{less robust watermarking} \end{cases} \quad (7)$$

Step6: Estimation of peak signal to noise ratio (PSNR): PSNR is calculated by using following equation. Capacity of the original image to carry the fingerprint watermark is computed by measuring PSNR, which is defined as follows:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ (dB)} \quad (8)$$

Mean square error is defined as:

$$MSE = \frac{1}{m \times n} \sum_{m=1}^{256} \sum_{n=1}^{256} (W(m,n) - W^*(m,n))^2 \quad (9)$$

Step 7: Weighted correlation coefficient computation: Weighted correlation coefficient is defined as follows:

$$CRC_w(l,k) = \sum_{i=1}^5 CRC_i(l,k) \times \beta_i \quad (10)$$

Where, β_i are the different weightings of attacks such that total $\sum_{i=1}^5 \beta_i = \beta_1 + \beta_2 + \dots + \beta_5 = 1$, and i is the number of attacks in various compression. The identified attacks are assigned weightings based on damage caused, frequency, intensity and criticality or any other such criterion by the user. Based on these weightings, considering all the ten attacks, weighted correlation coefficient are estimated, for each bit plane combination of image and watermark under consideration. The step is repeated for combinations of selected bit planes of image and the entire bit planes of watermark respectively.

Step 8: Optimization: The above step 7 is repeated by varying the weightings of attacks. The bit plane combination of original image and fingerprint for which, the weighted correlation coefficient is maximum, is selected as the optimized one for the given user requirements. This combination is used for optimized watermarking in terms of robustness and fidelity.

3 Experiment Results and Analysis

Here, we employed Lenna, Baboo, Perppers as test carrier images, which size of the images was fully 512×512 , Size of the embedded fingerprint watermarks was 64×64 , as figure 2. in the bit planes combination, we use 1st bit plane of fingerprint watermark embedded in 7th bit plane of original image.

The invisibility of the hidid image may be measured by histogram statistics charts, and Peak-value

Signal Noise Ratio (PSNR) [13-14]. To the definite information hiding Capacity, the method hold a kind of different hiding efficiency in various compress ratio with JPEG2000 [15].

Retrieval of fingerprint image after difference compression attack was showed in finger 3 when the compression factor $Q = 100$, $Q = 20$, $Q = 10$ and $Q = 7$, and $Q = 5$, as well as $Q = 2$, respectively. The histogram

statistics charts of the *Lenna* images composited was showed in figure 4, respectively.

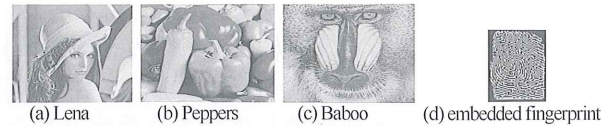


Fig. 2 The carrier image and embedded fingerprint images

Compression factor		100	20	10	7	5	2
Lena	PSNR/dB	36.2	35.8	34.8	34.0	33.0	30.5
	Retrieval fingerprint						
Baboo	PSNR/dB	35.0	29.1	25.6	24.2	23.0	20.6
	Retrieval fingerprint						
Peppers	PSNR/dB	36.3	34.7	33.4	32.8	32.4	30.3
	Retrieval fingerprint						

Fig. 3 Retrieval of fingerprint image after difference compression attack

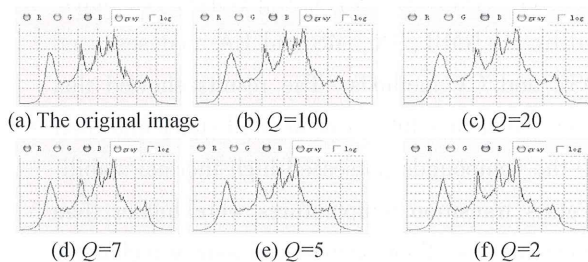


Fig. 4 The histogram statistics charts of the *Lenna* images composited data

From these simulation results, we can find out, where the images composited data possessed better image quality, and the influences to the carrier images was a littler after embedded a fingerprint [8]. Another, the shapes of the histogram statistics charts closed to auxiliary distributions. It shows, the method has better invisibility in various compression ratio, and the highest compression ratio is able to reach the 100:5 at conditioned embedding images.

4 Conclusions

Based on bit plane decomposition of the original image and the fingerprint image, the paper proposed an effectively information hiding method, which may adaptively embed hidden fingerprint data into wavelet coefficients from low to high frequency sub-band according to in space bit Planes. Experimentation results shows, that The proposed method is found to be useful for authentication and to prove legal ownership, and possesses better tradeoff between invisibility and robustness in various conditional compression.

References:

[1] PRAYOTH K, KITTI A, ARTHIT S. A robust image watermarking scheme using multiwavelet tree [C] // Proceedings of the World Congress on Engineering, London, U. K. July 2 - 4, 2007.

参考文献:

- [1] ROSU F, PAUW E D, GABELICA V. Electrospray mass spectrometry to study drug-nucleic acids interactions [J]. *Biochimie*, 2008, 90(7): 1074 - 1087.
- [2] TERRIER P, TORTAJADA J, BUCHMANN W. A study of noncovalent complexes involving single-stranded DNA and polybasic compounds using nanospray mass spectrometry [J]. *J Am Soc Mass Spectrom*, 2007, 18(2): 346 - 358.
- [3] ZHOU X M, SHEN Z, LI D Z, et al. Study of interactions between actinomycin D and oligonucleotides by microchip electrophoresis and ESI-MS [J]. *Talanta*, 2007, 72(2): 561 - 567.
- [4] 林秀丽, 陆玮洁, 主沉浮. 电喷雾质谱在药物和 DNA 相互作用研究中的应用 [J]. *中国生化杂志*, 2007, 28(2): 124 - 126.
- [5] 饶小平, 宋湛谦, 高宏. 脱氢枞胺及其衍生物的研究与应用进展 [J]. *化学通报*, 2006, 60(3): 168 - 172.
- [6] 陈泳, 林中祥. *N*-苯甲酰基-脱氢枞胺-7-酮的合成及其对雄激素受体活性的研究. [J]. *林产化学与工业*, 2009, 10(增刊): 121 - 124.
- [7] WAN C H, CUI M, SONG F R, et al. A study of the non-covalent interaction between flavonoids and DNA triplexes by electrospray ionization mass spectrometry [J]. *Int J Mass Spectrom*, 2009, 283(1/2/3): 48 - 55.
- [8] POCSFALVI G, LANDA G D, FERRANTI P, et al. Observation of non-covalent interactions between beauvericin and oligonucleotides using electrospray ionization mass spectrometry [J]. *Rapid Commun Mass Spectrom*, 1997, 11(3): 265 - 272.
- [9] JANSSEN P A, DONGEN J J, MEIJER E W, et al. Electrospray-ionization mass spectrometry for screening the specificity and stability of single-stranded - DNA templated self-assemblies [J]. *Chemistry European*, 2009, 15(2): 352 - 360.
- [2] SUSHMA K, MANESH K. Optimization of bit plane combination for efficient digital image after marking [J]. *International Journal of Computer Science and Information Security*, 2009, 4(2): 19 - 20.
- [3] ZHANG L. Combined the information hiding technology with JPEG2000 [D]. University of TianJin, 2003: 95 - 98.
- [4] ZHAO H M. Fingerprint system and DSP fast processing technology [J]. *Research & Progress of Solid State Electronics*, 2004, 24(3): 337 - 342.
- [5] TAUBMAN D S, MARCELLIN M W, et al. Image compression foundation, standard and practice of the JPEG2000 [M]. Electronics Industrial Publisher, 2004: 415 - 417.
- [6] LI K, ZHANG X P. An image watermarking method integrating with JPEG-2000 still image compression standard [C] // *Electrical and Computer Engineering IEEE CCECE Canadian Conference on*, 2003: 2053 - 2054.
- [7] TRAPPE W, WU M, WANG Z J. Anti-collusion fingerprinting for multimedia [J]. *IEEE Transactions on Signal Processing*, 2008, 53(4): 1069 - 1087.
- [8] WANG Z J, WU M, TRAPPE W. Group-oriented fingerprinting for multimedia forensics [J]. *EURASIP Journal on Applied Signal Processing*, 2004, 14(8): 2142 - 2162.
- [9] WANG Y, LIANG F, XIAO M M. Color image watermarking adaptively in DC coefficients [J]. *Acta Scientiarum Naturalium Universitatis Sunyatseni*, 2010, 49(4): 43 - 48.
- [10] SWANSON M D, KOHAYASHI M, TEWFIK A. Multimedia data embedding and watermarking technologies [J]. *Proc of the IEEE*, 1998, 86(6): 1064 - 1087.
- [11] REN J, NADOOSHAN T. A cryptographic watermark embedding technique [C] // *IEEE Asilomar Conf on Signals, Systems and Computers*, 2004: 382 - 386.
- [12] MAEDER A J, PLANITZ B M. Medical image watermarking for multiple modalities [C] // *34th IEEE Proc on Applied Imagery and Pattern Recognition Workshop*, 2005: 158 - 165.
- [13] FEI C, KUNDER D, KWONG R H. Analysis and design of secure watermark-based authentication systems [J]. *IEEE Trans On Information Forensics and Security*, 2006, 1(1): 43 - 55.
- [14] PRAYOTH K, KITTI A, ARTHIT S. A new approach for optimization in image watermarking by using genetic algorithms [J]. *IEEE Trans on Signal Processing*, 2005, 53(12): 4707 - 4719.
- [15] COX J, KILIAN J, THOMSON F, et al. Secure spread spectrum watermarking for multimedia [J]. *IEEE Trans on Image Processing*, 1997, 6(12): 1673 - 1686.

(上接第 67 页)