A Dual Binary Image Watermarking Based on Wavelet Domain and Pixel Distribution Features

Wei Xia, Hongwei Lu*, and Yizhu Zhao

College of Computer Science and Technology,
Huazhong University of Science and Technology,
Wuhan, China
xw7932@126.com, luhw@hust.edu.cn, missbamboofirst@163.com

Abstract. Considering that the binary images are featured little capability in data hiding, difficulty in watermarking embedding and two values, in order to improve the robustness and invisibility of watermarkings embedded into the binary images, a novel algorithm is presented which is based on DWT (Discrete Wavelet Transformation). The original watermarking signal is embedded into the lowest frequency sub-band of the wavelet domain. Combined with the technique of encryption, the extracted invariant pixel distribution features of the binary image establish another layer virtual watermarking and a mapping relationship between the two layer watermarkings. The mapping enables the self-restoration of the original watermarking with virtual watermarking when the binary image is attacked. The watermarking can be well extracted without the original binary image. The invisibility and robustness of the proposed algorithm are demonstrated by the Simulations such as Gaussian noise, JPEG compression and some geometric attacks.

Keywords: DWT, pixel distribution features, virtual watermarking, watermarking restoration.

1 Introduction

As an effective method of multimedia copyright protection and information security maintenance, digital watermarking technique is becoming a hot topic in the area of information processing. At present, a large amount of references mainly involve gray image, color image and the research of the video and audio watermarking. The binary image is bi-level and it is difficult to embed watermarking into it, so the binary image watermarking is seldom considered. With the global progress of the information digitalization, a lot of important binary text data, such as personal files, medical records, academic certificates, patent certificates, handwriting signatures, design patterns, library books, confidential documents have turned into digital documents by scan. In

[*] Corresponding author. This work is partially supported by the special funds for university basic research work of China (No.M2009020).

S. Boll et al. (Eds.): MMM 2010, LNCS 5916, pp. 130–140, 2010.

addition, with the increasingly prevalent e-commerce and e-government, the copy tracing and the integrity authentication of the electronic binary text documents are urgently required. We can deem most of these documents as binary text images. In some fields, the binary images are much more valuable than common gray and color images or video and audio files. So the copyright protection and information security maintenance of the binary images are especially important.

Currently, few domestic papers about binary image watermarking are found. The familiar binary image watermarking methods are line space encoding and character space encoding. Line space encoding is proposed by Brassil etc [1] in bell lab and implements watermarking embedding by means of changing the line space. Character space encoding is proposed by Huang etc [2] and implements watermarking embedding by means of left-right shifts of a word.

In general, we can classify image watermarking into two categories depending on the embedding domain: the spatial domain techniques and the frequency domain techniques. In spatial domain, the watermarking is embedded in the original image by modifying the pixel values or the least significant bits (LSB). All of the above bi-level image watermarking schemes are based on spatial domain. Compared with the schemes based on transform domain, these schemes are featured little capability in data hiding, poor robustness and complicated watermarking extraction process. Moreover, Chinese characters have no character space and baseline in the sense of English, so the effectiveness of Chinese character watermarking embedding is not always ideal by above methods. Recently, some works has focused on the frequency domain watermarking. Among the transform domains, the wavelet, due to its similarity to human visual system (HVS), is a proper domain for watermarking embedding. By using this transformation, modification is imposed on those regions that are less sensitive to human eyes. Therefore it causes effective achievement in the fidelity and robustness requirements. In addition, both newly JPEG2000 image and MPEG-4 video compression standard adopt this transformation, so the watermarking scheme is in well compatible with the new standards.

Dual digital watermarking technique embeds two layer watermarkings in one image and effectively increases information quantity of the embedded watermarkings. Traditional dual watermarking mainly emphasizes on realizing the functionally expansion of the watermarking to meet various practical requirements [3, 4]. Generally speaking, it can actuate two or more functions simultaneously and obviously has advantage in information quantity, but it is also far inferior to others in invisibility [5]. The algorithm features such as higher complex computation restrict the self-development of the dual watermarking.

The paper presents a new dual digital watermarking scheme which is based on wavelet domain and invariant distribution features of pixels in binary images. Therefore, a blind binary image watermarking algorithm with excellent robustness, invisibility and low computational complexity is realized.

The rest of the paper is structured as follows. As the backgrounds of the watermarking scheme, the pixel distribution features are presented in section 2. The entire watermarking scheme, including the two layer watermarking embedding process and the watermarking restoration, is introduced in detail in section 3. In section 4, the performance of the proposed watermarking method is evaluated by applying some familiar attacks to the watermarked binary images. Finally in section 5 we conclude our method.

2 Pixel Distribution Features of Binary Images

As for a binary image $f(x, y)$, target pixels (If the coordinate of the target pixel is (a, b), then $f(a,b)=1$) are parts of the global image region, so gravity center $(\overline{x}, \overline{y})$ can be selected as the centroid of the image and it meets the below equations.

$$\overline{x}=(\sum_i\sum_j i\times f(i,j))/(\sum_i\sum_j f(i,j)) \ . \tag{1}$$

$$\overline{y}=(\sum_i\sum_j j\times f(i,j))/(\sum_i\sum_j f(i,j)) \ . \tag{2}$$

$$f(i,j)=\begin{cases}1,,(i,j)\in R\\0,(i,j)\notin R\end{cases} \ . \tag{3}$$

"R" represents the target pixel region of the binary image. Computing the Euclidean distance between the centroid and every target pixel and finding out the maximum distance (denoted as $D_{\max}$) must be executed after getting the centroid. Subsequently, we obtain a circumcircle of the target pixel region. The circle center of the circumcircle is the centroid and the radius of it is $D_{\max}$.

Assuming that there are K bits of watermarkings to be embedded into the original image and the total number of target pixels is X, we can divide the circumcircle of the target pixel region into one circle sub-region and $\lfloor K/(\lfloor \log_2 X \rfloor+1)\rfloor-1$ concentric ring sub-regions and all sub-regions have the same circle center (the centroid). These sub-regions are separately denoted as $R_1, R_2, \cdots, R_M$ from inside to outside ($M=\lfloor K/(\lfloor \log_2 X \rfloor+1)\rfloor$). There are two sub-region division methods namely equidistant division method and equal-area division method [6].

Here we use the equal-area division method. Every sub-region interval has the same area with the assumption that $1\le i\le M$. It is described in equation (4).

$$R_i=\left\{(x,y)\,|\,(i-1)\times D_{\max}{}^2/M<(x-\overline{x})^2+(y-\overline{y})^2\le i\times D_{\max}{}^2/M\right\} \tag{4}$$

Fig. 1 shows the results under the condition of $M=4$. Certainly, in the real application, M is much larger than 4.

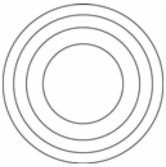


Fig. 1. One circle and three concentric ring sub-regions divided by equal-area method under the condition of $M = 4$

The target pixel number of every sub-region can be represented to $S_i (i = 1,2,\cdots,M)$. With the maximum value of S_i ($S_{\max} = \max\limits_{i=1,2,\cdots,M}(S_i)$), we can calculate the probability density of the target pixels of every sub-region.

$$r_i = S_i / S_{\max} (i = 1,2,\cdots,M) \ . \tag{5}$$

In theory, $r_i (i = 1,2,\cdots,M)$ is comparatively invariant under all kinds of familiar geometric attacks such as rotation, translation and scaling, so we can encode every element of $r_i (i = 1,2,\cdots,M)$ with $\lfloor \log_2 X \rfloor + 1$ binary bits and then get $M \times (\lfloor \log_2 X \rfloor + 1)$ binary bits. If $M \times (\lfloor \log_2 X \rfloor + 1)$ is less than K, in order to make the length of the obtained binary code be equal to K, we fill it with the lowest $K - M \times (\lfloor \log_2 X \rfloor + 1)$ bits of $S_{\max}$. In the end, the obtained binary code with the length of K bits are denoted as B. We can define the binary code as the pixel distribution features of the binary image.

3 The Watermarking Scheme

Without affecting the results, we suppose that the size of the original host image F and the watermarking image W_1 are $b \times b$ and $a \times a$ respectively, as shown below.

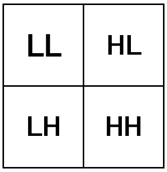
$$W_1 = \{ w(i,j) \mid w(i,j) = 0,1; 1 \le i \le a, 1 \le j \le a \} \ . \tag{6}$$

$$F = \{ f(i,j) \mid f(i,j) = 0,1; 1 \le i \le b, 1 \le j \le b \} \ . \tag{7}$$

The watermarking embedding steps are described as follows.

3.1 The First Layer Watermarking Scheme

As shown in Fig. 2, after One-level wavelet transformation, the original image is decomposed into four sub-bands: LL, HL, LH, HH. As for binary image, the higher frequency sub-bands include ample texture features, poor energies and are liable to the affection of interference, so the coefficients in LL (lowest frequency sub-band) sub-band are selected to implement watermarking scheme.



LL	HL
LH	HH

Fig. 2. Four sub-bands after One-level wavelet decomposition

Using L-level wavelet transformation, the original image is decomposed into its sub-bands. The coefficient matrix (denoted by FA_L) in the lowest frequency sub-band of the last level is selected and L can be obtained by the following formula.

$$L \leq \lfloor \log_2 (b/a) \rfloor \ . \tag{8}$$

The robustness is better and the decomposition and reconstruction time becomes longer when L is increasing.

Finally we can embed watermarking into FA_L by means of modifying the coefficients in it and a binary logical table in relation to the original watermarking is produced. It is actually a superposition method. Some related formulae are listed here.

$$FA_L^{'}(i,j) = FA_L(i,j) + \alpha W_1(i,j) \ . \tag{9}$$

$$FA_L^{*}(i,j) = round(FA_L^{'}(i,j)/t) \ . \tag{10}$$

$$FA_L^{''}(i,j) = FA_L^{*}(i,j) \times t \ . \tag{11}$$

$$kk(i,j) = FA_L^{*}(i,j) \bmod 2 \ . \tag{12}$$

$$key(i,j) = kk(i,j) \oplus W_1(i,j) \ . \tag{13}$$

"α" represents the watermarking embedding strength. Aiming at the robustness and invisibility of the watermarking scheme, the value range of the quantization parameter t is 0~0.5 according to the coefficients in FA_L. "round" in equation (**10**) is the integral function by rounding rule. After watermarking embedding and quantization, the selected coefficient matrix is transformed to $FA_L^{''}$. HASH function is used to assure the reliability of the binary logical table (denoted as $key(i, j)$). The binary logical table is necessary for original watermarking extraction. As the secret key, it can be used to apply to the third party for copyright protection.

Watermarking extraction is the reverse process of the watermarking embedding. L-level wavelet decomposition of the watermarked image is carried out to extract the coefficient matrix in the lowest frequency sub-band of the last level. The matrix is denoted as $T\_FA_L(i,j)$. We can easily extract watermarking (denoted as $W^*(i,j)$) according to the matrix and the produced binary logical table. The original image is not required in this method. It is described as below equations.

$$T\_FA_L^*(i,j) = round(T\_FA_L(i,j)/t) \; . \tag{14}$$

$$kk^*(i,j) = T\_FA_L^*(i,j) \bmod 2 \; . \tag{15}$$

$$W^*(i,j) = kk^*(i,j) \oplus key(i,j) \; . \tag{16}$$

3.2 The Second Layer Watermarking Scheme

Using the method discussed in section 2, a pixel distribution feature matrix (denoted as B) of the watermarked image can be obtained and the size of the matrix is $b \times b$. We get the second layer watermarking W_2 using the following formula.

$$W_2(i,j) = E(B(i,j) \oplus W_1(i,j)) \; . \tag{17}$$

E is the encryption function for the purpose of increasing the security of the watermarking. A variety of encryption methods can be employed. Here we use disorder processing with M and $S_{\max}$ being the secret keys. $\oplus$ is XOR operator($1\oplus 1=0$, $0\oplus 0=0$, $1\oplus 0=1$, $0\oplus 1=1$). W_2 is virtual because in fact, it is not embedded into the host image. On the contrary, together with M and $S_{\max}$, it is stored in an encrypted XML document [7]. When the watermarked image suffer some serious attacks, the virtual watermarking may be useful to restore the first layer original watermarking which is in fact embedded into the host binary image. We can see it in section 3.3 and well realize it later from experiments. Furthermore, the equation (17) establishes a mapping relationship between the first and the second layer watermarking.

3.3 Watermarking Restoration

It has been widely recognized that the robustness of the watermarking is an important issue in applications of the watermarking algorithm. It can be defined as “ability to detect the watermarking after common signal processing operations”. Watermarkings could be removed intentionally or unintentionally after some distortions such as compression, noise adding, shear transformation. For image watermarking, the robustness of the watermarking under geometric transformations, among other possible distortions, has to be addressed first and foremost, because they can dramatically affect the correct detection of the watermarking.

In the sequel we propose a low complexity watermarking restoration scheme which is computationally simple. It is based on the stability of the pixel probability density which is formerly put forward. The restorarion scheme is especially effective under attacks such as rotation, scaling and translation. Even under other attacks, the pixel probability density of an image is comparatively stable only if the watermarked image is not damaged a lot under these attacks. So we can also compute the pixel probability density of every target pixel sub-region of the watermarked image under attacks.

According to the discussion in section 3.2, with the extraction and using of M and $S_{\max}$ that are stored in the XML document, after computing the pixel probability density of every target pixel sub-region of the watermarked image under attacks, we can get a matrix T. The size of the matrix is equal to that of the second layer virtual watermarking. The formula of watermarking restoration process is a simple XOR operation.

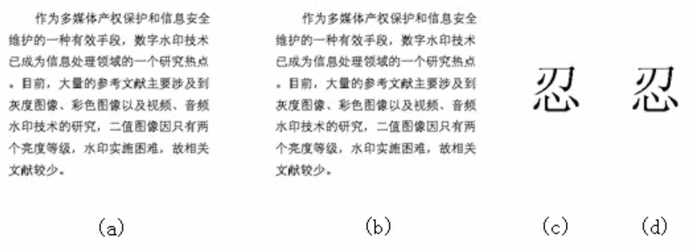
$$W_1^{'}(i,j) = T(i,j) \oplus \underline{E}(W_2(i,j)) \ . \tag{18}$$

$\underline{E}$ is the decryption function which is the reverse process of E in equation (17). The matrix $W_1^{'}$ is the final result of the watermarking restoration process.

4 Experimental Results

In order to evaluate the proposed scheme, we choose an original binary image of size 384×384 and a watermarking image of size 96×96 and perform experiments as following.

Fig. 3 shows the process of embedding and extraction of the watermarking without any attacks. The result of comparing the original image with the watermarked image shows that the algorithm has good imperceptibility and the result of comparing the original watermarking and the extracted watermarking shows the effectiveness of the extraction.



作为多媒体产权保护和信息安全维护的一种有效手段，数字水印技术已成为信息处理领域的一个研究热点。目前，大量的参考文献主要涉及到灰度图像、彩色图像以及视频、音频水印技术的研究，二值图像因只有两个亮度等级，水印实施困难，故相关文献较少。

(a)

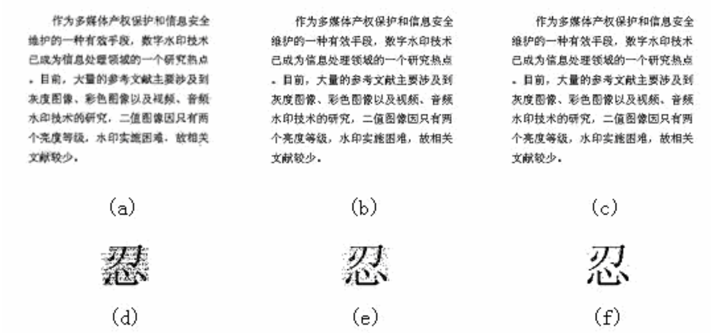
作为多媒体产权保护和信息安全维护的一种有效手段，数字水印技术已成为信息处理领域的一个研究热点。目前，大量的参考文献主要涉及到灰度图像、彩色图像以及视频、音频水印技术的研究，二值图像因只有两个亮度等级，水印实施困难，故相关文献较少。

(b)

Fig. 3. (a) Original image, (b) Watermarked image, (c) Original watermarking, (d) Extracted watermarking

Subsequently, let us see the robustness of the dual watermarking scheme under some familiar attacks.

Fig. 4 shows the robustness under JPEG compression attacks with compression rate of 10%, 50% and 90% respectively. According to the extracted watermarkings


作为多媒体产权保护和信息安全
维护的一种有效手段，数字水印技术
已成为信息处理领域的一个研究热点
。目前，大量的参考文献主要涉及到
灰度图像、彩色图像以及视频、音频
水印技术的研究，二值图像因只有两
个亮度等级，水印实施困难，故相关
文献较少。

作为多媒体产权保护和信息安全
维护的一种有效手段，数字水印技术
已成为信息处理领域的一个研究热点
。目前，大量的参考文献主要涉及到
灰度图像、彩色图像以及视频、音频
水印技术的研究，二值图像因只有两
个亮度等级，水印实施困难，故相关
文献较少。

作为多媒体产权保护和信息安全
维护的一种有效手段，数字水印技术
已成为信息处理领域的一个研究热点
。目前，大量的参考文献主要涉及到
灰度图像、彩色图像以及视频、音频
水印技术的研究，二值图像因只有两
个亮度等级，水印实施困难，故相关
文献较少。

Fig. 4. (a) 10% compression, (b) 50% compression, (c) 90% compression, (d) Watermarking from (a), (e) Watermarking from (b), (f) Watermarking from (c)

from the three watermarked images, even the compression rate is 10%, the watermarking is very easy to be seen.

Fig. 5 shows the robustness under 20% shearing attack. The result shows that the extracted watermarking is slightly fuzzy in a small part of the center region using the usual single DWT watermarking scheme. Using the restoration scheme described in section 3.3, we can see that the restored watermarking image can be clearly identified. By the way, the issue “restored watermarking” in this paper is always obtained by the restoration scheme described in section 3.3.

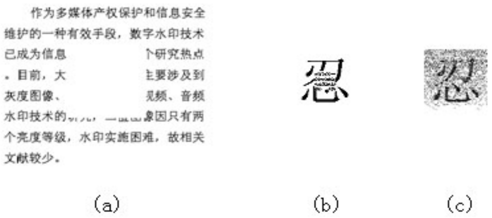

作为多媒体产权保护和信息安全
维护的一种有效手段，数字水印技术
已成为信息 个研究热点
。目前，大 主要涉及到
灰度图像、 视频、音频
水印技术的 象因只有两
个亮度等级，水印实施困难，故相关
文献较少。

Fig. 5. (a) 20% sheared image, (b) Extracted watermarking using usual DWT scheme, (c) Restored watermarking using dual watermarking scheme

Fig. 6 shows the good robustness under Gaussian noise attacks with intensity of 0.005, 0.010, 0.015 and 0.020 respectively. From the extracted watermarking images, it is obvious that the scheme has good ability of resisting Gaussian noise attacks. Comparing the extracted watermarkings using the usual single DWT watermarking scheme and the restored watermarkings, it implies that at the same intensity level of the noise, the quality of the restored watermarking image is higher than that of the extracted watermarking image using the usual single DWT watermarking scheme.

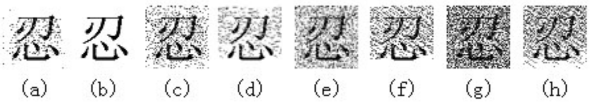


Fig. 6. (a) Extracted watermarking under 0.005 Gaussian noise using usual DWT scheme, (b) Restored watermarking under 0.005 Gaussian noise using dual watermarking scheme, (c) Extracted watermarking under 0.010 Gaussian noise using usual DWT scheme, (d) Restored watermarking under 0.010 Gaussian noise using dual watermarking scheme, (e) Extracted watermarking under 0.015 Gaussian noise using usual DWT scheme, (f) Restored watermarking under 0.015 Gaussian noise using dual watermarking scheme, (g) Extracted watermarking under 0.020 Gaussian noise using usual DWT scheme, (h) Restored watermarking under 0.020 Gaussian noise using dual watermarking scheme

Fig. 7 shows the robustness under translation attack. After translating the watermarked image down and to the right by 25 pixels, the extracted image is very fuzzy using the usual single DWT watermarking scheme, but as we see, the restored watermarking image is almost the same as the original watermarking image.

Fig. 7. (a) Extracted watermarking under translation attack using usual DWT scheme, (b) Restored watermarking under translation attack using dual watermarking scheme

Fig. 8 shows the robustness under 0.75-time scaling attack. The quality of the watermarked image under the scaling attack declines obviously. After scaling to the original size of the watermarked image, we obtain a satisfied result of the extracted watermarking using the usual single DWT watermarking scheme. But sometimes, not knowing the original size of the watermarked image, we are still satisfied with the quality of the restored watermarking.

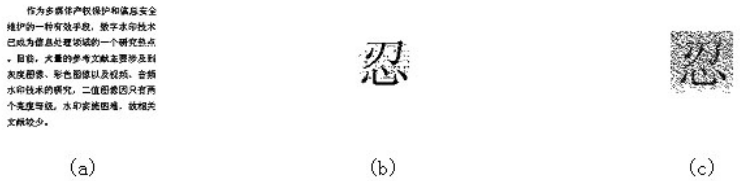

作为多媒体产权保护和信息安全维护的一种有效手段，数字水印技术已成为信息处理领域的一个研究热点。目前，大量的参考文献主要涉及到灰度图像、彩色图像以及视频、音频水印技术的研究，二值图像因只有两个亮度等级，水印实施困难，故相关文献较少。

Fig. 8. (a) Watermarked image after 0.75-time scaling attack, (b) Extracted watermarking after scaling to the original size using usual DWT scheme, (c) Restored watermarking using dual watermarking scheme

Fig. 9 shows the powerful restoration scheme again. The extracted watermarkings are too fuzzy to be identified using the usual single DWT watermarking scheme. The result shows that the quality of the restored watermarkings are all fairly good by rotating the watermarked image by 20, 40 and 60 degrees respectively.

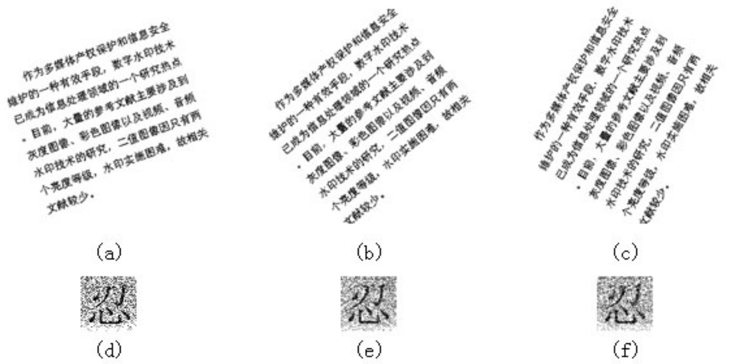

作为多媒体产权保护和信息安全
维护的一种有效手段，数字水印技术
已成为信息处理领域的一个研究热点
。目前，大量的参考文献主要涉及到
灰度图像、彩色图像以及视频、音频
水印技术的研究，二值图像因只有两
个亮度等级，水印实施困难，故相关
文献较少。
(a)
(b)
(c)
忍
(d)
(e)
(f)

Fig. 9. (a) Watermarked image after rotated by 20 degrees, (b) Watermarked image after rotated by 40 degrees, (c) Watermarked image after rotated by 60 degrees, (d) Restored watermarking from (a), (e) Restored watermarking from (b), (f) Restored watermarking from (c)

5 Conclusion

In this paper, a dual DWT and pixel distribution features based blind binary image watermarking scheme has been proposed. The comparatively invariant pixel distribution features against a lot of attacks are used to form the second layer virtual watermarking and establish a mapping relationship between the two layer watermarkings. So the watermarking scheme is robust against all kinds of familiar attacks. Using DWT decomposition, the lowest frequency sub-band of the last level is selected to embed the first layer original watermarking because it is not liable to the interference. Therefore the scheme has excellent invisibility. The invariant features described in this paper can be easily obtained. In other words, the watermarking algorithm has low complexity and it is easy to manipulate. In addition, compared with other schemes, less virtual watermarkings are required to be stored in the encrypted XML document. These arguments are strongly supported by the experiment results.

References

1. Brassil, J., Low, S., Maxemchuk, N.F.: Copyright Protection for the Electronic Distribution of Text Documents. Proceedings of IEEE 87(7), 1181–1196 (1999)
2. Huang, D., Yan, H.: Interword Distance Changes Represented by Sine Waves for Watermarking Text Images. IEEE Trans. on Syst. Video Technology 11(12), 1237–1245 (2001)
3. Mohanty, S.P., Ramakrishnan, K.R., Kankanhall, M.: A Dual Watermarking Technique for Images. In: Proceedings of the 7th ACM International Multimedia Conference, pp. 49–51. ACM Press, New York (1999)
4. Lie, W.N., Hsu, T.L., Lin, G.S.: Verification of Image Content Integrity by Using Dual Watermarking On Wavelets Domain. In: International Conference on Image Processing, Barcelona, vol. 3, pp. 487–490 (2003)

5. Barni, M., Bartolini, F.: Data Hiding for Fighting Piracy. IEEE Signal Processing Magazine 21(2), 28–39 (2004)
6. Li, G., Xing-hua, S., Yuan-yuan, H., et al.: Distance Distribution Histogram and Its Application in Trademark Image Retrieval. Journal of Image and Graphics 7A(10), 1027–1031 (2002)
7. Frattolillo, F., D'Onofrio, S.: An Image Watermarking Procedure Based on XML Documents. In: The 11th International Conference on Distributed Multimedia Systems, Banff, pp. 22–27 (2005)