Proc. VIIth Digital Image Computing: Techniques and Applications, Sun C., Talbot H., Ourselin S. and Adriaansen T. (Eds.), 10-12 Dec. 2003, Sydney

Image Ownership Verification via Private Pattern and Watermarking Wavelet Filters

Zhuan Qing Huang and Zhuhan Jiang

School of Computing and IT, University of Western Sydney, NSW 2150, Australia

Abstract. In this paper, we propose a watermarking scheme for the image ownership verification in terms of a private key pattern and wavelet filters. The watermarking is mainly achieved within the process of decomposition and reconstruction by forging watermark-carrying wavelet filters. This scheme improves the watermark robustness and invisibility since it maximally avoids inserting the watermark into the images directly. It also allows the flexibility to optimize the wavelet filters for better performance. The private key pattern is free from watermark restriction and is associated with individual images. It adds an additional layer of security in a different dimension. The detection of our watermarks, can moreover be achieved without the aid of the original images, and will also be broadly discussed in regard to cropped images or images of certain other distortions.

1 Introduction

Image ownership verification is becoming increasingly important for the copyright protection of digital images due to their ever easier accessibility made possible by the widespread Internet and digital technologies. Watermarking, in this regard, is to hide crucial information inside digital images so that it can be detected later to resolve copyright or ownership issues. Different digital watermarking technologies have been investigated over the past decade [1] with recent attention directed more towards transform domains due to such as DCT and wavelet transforms for more robustness and power [1-8]. In particular, pseudo-random codes are added [2] to the large coefficients at the high and middle frequency bands, watermarks are decomposed [3] into different resolution to be embedded into the corresponding resolution of the decomposed images, and watermarks are inserted into both the high frequency components [7] and the middle frequency band [8] for somewhat different purposes.

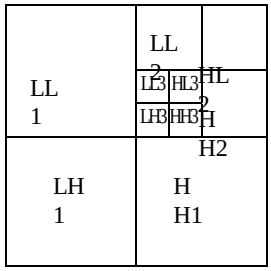

Fig. 1 Multiresolution decomposition

An important feature of wavelet filters is its ability to decompose an image into different frequency bands as in Fig.1. This makes it possible to perform various operations on the different resolution levels. The decomposition is based on the analysis filters [1]

$$c_j = \sum_{k\in Z} h_{k-2j} x_k, \quad d_j = \sum_{k\in Z} (-1)^k \bar{h}_{1-k+2j} x_k , \qquad (1)$$

and the reconstruction is done through the synthesis filter

$$x_k = \sum_{j\in Z} \bar{h}_{k-2j}\, c_j + \sum_{j\in Z} (-1)^k h_{1+k-2j}\, d_j, \quad k\in Z, \qquad (2)$$

where Z denotes the set of all integers. The decomposition can be carried out recursively, and likewise for the reconstruction. We note that the quality of the filters directly impact on the correlation of the derived frequency bands: a better filter will result in better separation of the detail components from the smooth components of the image. There are different ways to construct the wavelet filters, orthogonal or biorthogonal [9,10]. For example, by [11] factorizing $P(z) = G_0(z)G_0(z^{-1})$ from a given $P(z) = 1+ \Sigma\, a_k\, z^{-k}$ with $a_k=a_{-k}$, $a_k \geq 0$ and $\Sigma_k\, a_k = 1$, orthogonal wavelets can be systematically constructed. A more convenient factorization will however be adopted later on for our proposed scheme.

Traditional watermarking algorithms either embed the watermark into certain frequency band by adding the watermark, or replace the selected band with the watermark. In this paper, we will however propose to construct dynamically the wavelet filters that are to contain watermarks directly. This approach has more potential for further security enhancement, allows additional freedom at processing the selected bands and improves the watermark invisibility since watermark is not directly added into the image. We will in this work limit ourselves to the use of the orthogonal wavelet filters, and the paper is organized as the following. We will first explain in section 2 the image ownership verification process and the roles of digital watermarks and the private key patterns. A new watermarking scheme is then proposed in section 3 along with the feasibility and performance analysis, as well as the discussion on the potential attacks by cropping or other distortions. The experimental results are then summarized in section 4, and the final conclusion, in section 5.

2 Ownership Verification

When a watermarked image is under suspicion, the owner of the image may require a legal authority to verify the copyright. The verification process obviously depends on the watermarking algorithm, and the watermark algorithm should in turn comply with the requirement of a practical verification system. From the requirement of a practical verification system, there are a number of aspects that need to be taken into account in the design of a watermarking scheme.

Firstly the verification procedure should be simple and efficient, hopefully minimum partners are involved and minimum amount of information flow is required in the procedure. Secondly, The watermark should be registered with the authority and each watermark should be associated with the corresponding images. An author may register one or one set of watermarks for his images. The watermark is allowed to label one image as well as different images. Thirdly since everyone could claim a watermark by applying certain algorithm to the image, the watermarking algorithm should be prior-approved by the authority. The algorithm should be easy to carry out with low number of false alarms. Fourthly the owner should have full control for the detection process, he can carry out the detection process while the authority can perform detection only after

obtaining the necessary information such as a private key from the owner. As the fifth, the authority deals with a huge number of authors, the storage for verification should be minimized when designing the algorithm. Individual authors should take most responsibility at storing the relevant data. Finally, in order to provide better protection to an original image, the original image should not be required for the detection process so as to minimize the chances of exposing the original image to the other parties.

Traditional algorithms may try to reduce the number of registered watermarks to lower the storage and may have to scramble the watermark to avoid using the same watermark in different images. In our proposed algorithm, the watermark will be embedded into the wavelet filters. When registering the watermark the owner actually registers the method that generates the filters for a watermark, see Fig.2. The owner may use the same watermark in different images with different interpretations or use different watermarks in different images with the same interpretation. The storage for such watermarks is expected to be fairly low. The private key is thus crucial to the successful watermark detection and will be stored by the owner. The private key here is a private bit or block pattern to be processed with the selected band. The owner will undertake to store all his images and the patterns to be used. Since a private key is not known to anyone but the owner, apart from having to present it to the legal authority when the need arises, it is very difficult for attackers to collude or guess the watermark embedding, or to remove the watermark by exhaustive brute-force. The private pattern in this approach can be flexibly chosen by the owner, and can be used to enhance the security of the watermarking. We note that the private pattern is traditionally used exclusively as the watermark. The use or even non-use of the private pattern in our approach thus, in contrast, also reduces the amount of data needed to be stored with the legal authority.

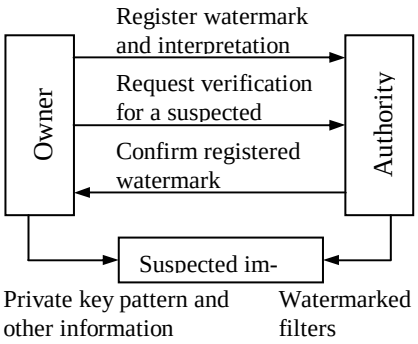

Fig. 2 Verification process

3 Proposed Watermarking Scheme and Its Analysis

We first observe that filter change will result in different band details even under the same decomposition tree or path. We here propose to embed the watermark information into the wavelet filters that are used to decompose the image. What decomposed band is to be selected to accommodate an optional private pattern, characterized by the decomposition path, is a part of the private key associated with the image. The wavelet filters are dynamically constructed to contain the watermarks. Since an attacker does not know the exact filters and the private key, he can't even locate the proper band for further analysis. In order to embed the watermark information into the filters, we need to exploit the following result: let $A(z) = \sum_{k \in Z} A_k z^{-k}$, and A = $\{A_k\}$ be a real-valued 2 x 2 matrix sequence with

$$A_k = \begin{bmatrix} h_{2k} & h_{2k+1} \\ g_{2k} & g_{2k+1} \end{bmatrix} ,$$

then $A(z)$ induces orthogonal wavelet filters if and only if $A(z)$ admits the following factorization [12]

$$A(z) = z^d \begin{bmatrix} 1 & 0 \\ 0 & \sigma \end{bmatrix} R(\theta_0) \begin{bmatrix} 1 & 0 \\ 0 & z^{-1} \end{bmatrix} R(\theta_1) \ldots \begin{bmatrix} 1 & 0 \\ 0 & z^{-1} \end{bmatrix} R(\theta_q) ,$$

$$R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \qquad (3)$$

with $\sigma = \pm 1$, $q \geq 0$, q, $d \in Z$ and $\theta_0 + \theta_1 + \ldots + \theta_q \equiv \pi/4 \pmod{2\pi}$. Hence these free θ's will be used to carry the watermarks. We can in fact partition θ's into 2 subsets, one contains the predefined watermark, the other can be optimized to improve the quality of filters or as a part of the private key. This approach to some extent embeds the watermark into the algorithm itself rather than into the image. The watermark can be transferred to a bit pattern, these bits can then be embedded into θ's. We know from (3) that θ has a period of 2π. If the θ can be divided into small units so that the result would exceed the detection threshold when θ changes one unit, then these units can be used to represent the watermark bit pattern. How much can θ be changed without destroying the watermark detectability? This will be answered in the next subsection. Before that we first note that if q is set to 2 in (3), then the set of wavelet filter coefficients $\{h_j, g_j\}$ can be calculated from (3) via

$$A(z) = \begin{bmatrix} h_0 - z^{-1} h_2 - z^{-2} h_4 & h_1 - z^{-1} h_3 + z^{-2} h_5 \\ -\sigma g_0 - \sigma z^{-1} g_2 - \sigma z^{-2} g_4 & -\sigma g_1 - \sigma z^{-1} g_3 + \sigma z^{-2} g_5 \end{bmatrix} ,$$

and then be expressed as

$$h_0 = \cos(\theta_0)\cos(\theta_1)\cos(\theta_2), \quad h_1 = \cos(\theta_0)\cos(\theta_1)\sin(\theta_2)$$
$$h_2 = -\sin(\theta_0)\sin(\theta_1)\cos(\theta_2) - \cos(\theta_0)\sin(\theta_1)\sin(\theta_2)$$
$$h_3 = -\sin(\theta_0)\sin(\theta_1)\sin(\theta_2) + \cos(\theta_0)\sin(\theta_1)\cos(\theta_2)$$
$$h_4 = -\sin(\theta_0)\cos(\theta_1)\sin(\theta_2), \quad h_5 = \sin(\theta_0)\cos(\theta_1)\cos(\theta_2)$$
$$g_0 = -\sigma h_5, \quad g_1 = -\sigma h_4, \quad g_2 = -\sigma h_3, \quad g_3 = \sigma h_2, \quad g_4 = -\sigma h_1, \quad g_5 = \sigma h_0 \qquad (4)$$

where $\theta_0 + \theta_1 + \theta_2 = \pi/4$. Thus there will be 2 free parameters in this case for each pair of wavelet filters, and these parameters are thus available for carrying a watermark and for performance optimization. If $q = 3$, then the filter will have 8 coefficients obtained through the same procedure as above and thus there will be 3 free parameters available.

3.1 The Algorithm and the Feasibility Measure

For a watermark given in terms of a bit sequence, we typically represent a section $\{b_k\}$ of the watermark bits by

$$\theta = \alpha(\Sigma_k b_k 2^k)\Delta\theta \qquad (5)$$

where $\Delta\theta$ is a chosen θ step and α is an optional adjusting factor. For instance, we watermark the image *goldhill* with "goldhill", if five bits are chosen for representing the watermark, then the watermark bits representing the "goldhill" are 00111 01111 01100 00100 01000 01001 01100 01100. Each value of θ is then calculated via (5). If $\alpha = 1$ and $\Delta\theta = 0.1$, then the θ values for the watermark characters become respectively $\theta_g = 0.7$, $\theta_o = 1.5$, $\theta_l = 1.2$, $\theta_d = 0.4$, $\theta_h = 0.8$, $\theta_i = 0.9$, $\theta_l = 1.2$ and $\theta_l = 1.2$. We use these θ's and determine the rest of θ's to calculate the filter coefficients via (4). This way, the obtained wavelet filters will carry the watermark "goldhill". Using these watermarked filters to decompose the image with a chosen path, we then obtain the unique subband characterized by the watermarked filters.

The robustness requires that the system can at least resist certain distortion due to such as noise and compression. The θ step, $\Delta\theta$, should be chosen in such a way that the system should be capable of tolerating a reasonable amount of white noise without affecting the watermark detection. A threshold for the θ step will be determined in terms of the effect of white noise, and the effect of θ on the selected band to be extracted and distinguished. When $\Delta\theta$ is large enough, the watermark can't be detected by another set of filters deviating in values by $\Delta\theta$ from the filters representing the watermark. Likewise for the white noise, once it exceeds certain threshold, it destroys the detection process. We can however balance these two factors and determine a suitable threshold for the θ step. The larger the θ step is chosen, obviously the better the resistance to the white noise, albeit at the cost of reducing the amount of the carried watermark information.

Two approaches for helping determine the threshold are designed as following. One is to sort the selected band. This method is straight forward, the sorted line is sensitive to filters and is easy to compare with one another. The other method is to replace the selected band with a desired pattern. The pattern can be anything and is routinely scrambled to improve the watermarking security. For the scrambling we can randomly generate a seed to scramble the pattern, or create a seed based on decomposition path and the θ's to scramble the pattern so that no additional storage is needed for the seed. The choice of $\Delta\theta$ should accommodate noise resistance to a certain degree, and that when noises added to the image do not cause visible visual degradation, the pattern can be detected by using the predetermined θ's that carry the watermark. But if the θ changes even only one step, the pattern cannot be detected by using the filters generated from this θ. If we want the system to be more robust to noise, however, we can artificially choose a higher threshold.

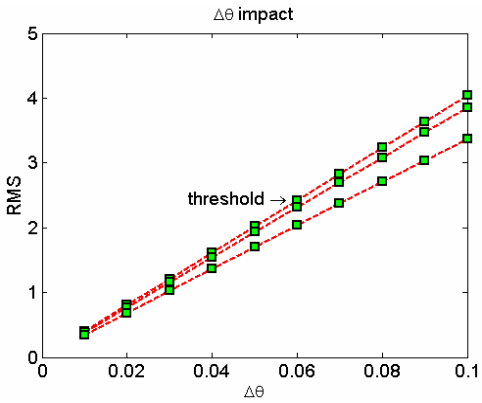

Fig. 3 θ step impact

We now use the Lena 256x256 image to illustrate the threshold of $\Delta\theta$. We tested with both the methods and with q=2 in (3). More precisely, we fix θ_1 in a selected zone as a private key and let θ_0

be free. The decomposition levels are 4 and always land at a middle frequency band. The ratio of white noises added to the image is ranged from 1% to 10% with the step of 1%. The $\Delta\theta$ is from 0.01 to 0.1 with the step 0.01. The results are in Fig. 3 and Fig. 4. They show when $\Delta\theta$ is less than 0.06, the pattern can be detected easily. The PSNR is 40.5 dB and RMS is 2.43 at $\theta = 0.06$. It becomes difficult to detect the pattern when the $\Delta\theta$ further increases. On the other hand, the pattern can be detected when the white noise ratio is no more than 4%, the PSNR is 40.4 dB and the RMS is 2.45. When the value of θ increases, the corresponding RMS increases too. The other paths and the patterns have also been tested and they yield similar results. If we choose 0.06 as the threshold λ for the θ step, and RMS 2.5 as the threshold ε for detection, we conclude that the pattern is detectable when noises ratio is less than 4%. If the θ has been changed by one step, implying a change of watermark information, the RMS of resulted pattern will be larger than the threshold ε, implying the user can't obtain the desired pattern. To achieve better invisibility, some of the θ's can be optimized.

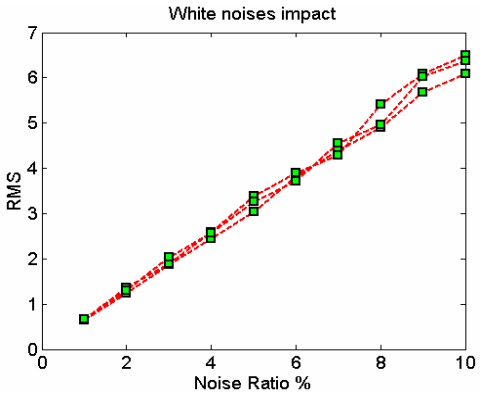

Fig. 4 Noise impact

3.2 Watermarking and Detection

With a suitably determined θ, the watermarking process is depicted in Fig. 5, and can be described as following: We first calculate the θ according to the watermark, then we decide whether the rest of θ will be used for optimization or as part of the private key. The filters will then come from (3), and for each level of decomposition, we will have 2 sets of analysis filters via (1) available to embed the watermark bits. After deciding the decomposition path and the pattern to be used, scramble the pattern and adjust the energy of desired pattern to match the selected band, then replace the selected band in the image with this pattern. The reconstructed image is thus the watermarked image.

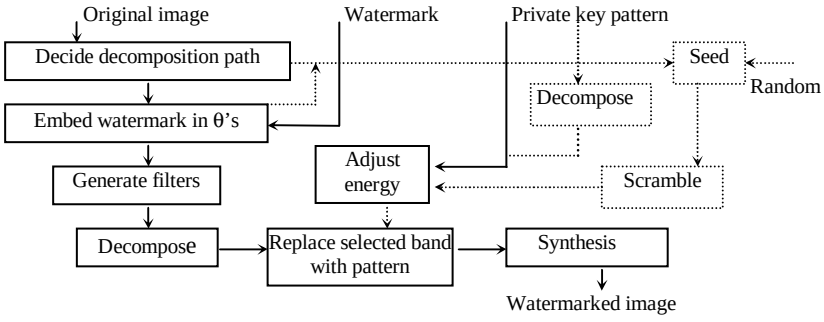

Fig. 5 Embedding process

We note that extra free θ's may also be utilized to optimize the filters and subsequently the watermarking performance.

The watermark invisibility can be achieved by adjusting the decomposition levels, paths, patterns and filters. Deeper decomposition levels and higher frequency band will result in a better invisibility. As is known, a lossy compression typically [10,13] round off or eliminate the high frequency components. As a result, we avoid making watermark-incurred image alteration to high frequency components for the robustness purpose. Otherwise all decomposition paths are valid for our purposes. Moreover, the pri-

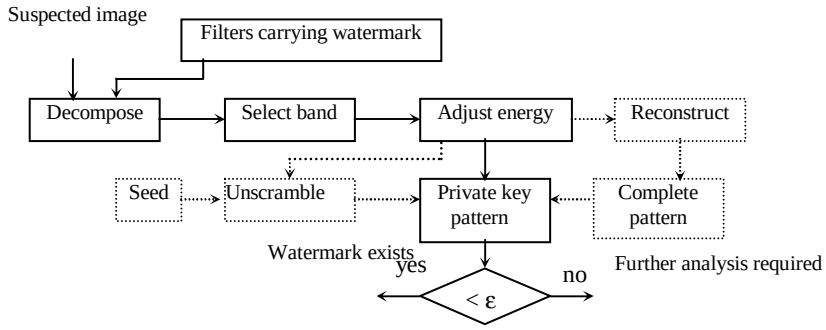

Fig. 6 Detection process

vate pattern itself can simply be non-existent. It can be dynamically constructed via scrambling the selected band with a private seed. In other words, the scrambling seed conceptually takes the role of a private pattern in this case.

The watermark detection practically reverses the embedding process, see Fig.6, and requires no original images. We for the detection first decompose the image by using the filters carrying the watermark, unscramble the selected band if needed, and then compare the outcome with the private key pattern. If the RMS of the selected band is smaller than the detection threshold ε, it can then be asserted that the predefined watermark does exist on the image, otherwise further analysis required.

3.3 Image Cropping and Distortion

The watermarked image may undergo certain distortion such as cropping and rescaling. Cropping is an easy operation that could lead to unauthorized use of part of the image. We will here briefly explain why our proposed algorithm is also capable of resisting cropping attacks. As we known, the wavelet-based watermarking can spread the watermark all over the image. If one crops a part of the image, it may still contain sufficient information on the watermark. Such a watermark may still be detected by certain mechanism even if the image has undergone further distortion such as rescaling and rotation. The strategy we are proposing here is to derive the watermark from the cropped image with the help of the original watermarked image: considering the original watermarked image with the cropped image replacing its corresponding area. In the case of cropped image containing noise, the detection remains difficult despite the large area of cropped image containing more watermark because of noise interference. We

hence approach this problem from a different angle. Since the difficulty is caused by the noises in the cropped image, if we add the noises M to the full-sized watermarked image, this noise can mollify the effect of noises N in the cropped image if M > N. In other word, the difference between the patched image and full-sized original watermarked image should decrease when the cropped area increases. If the cropped image has no specified watermark, such a difference should increase instead when the area of the cropped image becomes larger. This sharply contrasted trend of decreasing or increasing difference proves to be clear and universal, and suffices to differentiate cropped images corresponding to a given watermark.

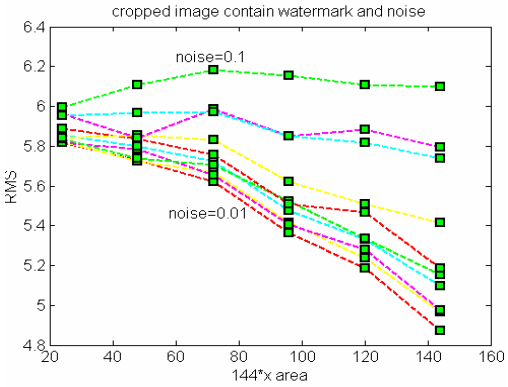

Fig. 7 Image contains the watermark

For a simple but convincing test, we divide the cropped image into 6 pieces equally and add the white noises with ratio less than that of watermarked image to the cropped image, then place one by one the subdivided pieces of the cropped image on top of the original watermarked image at the corresponding positions. The experiments show that the RMS of patched image decreases with more pieces of the cropped image being put back if cropped image contains watermark, see Fig.7, while the RMS of the patched image increases sharply with each additional piece from the cropped image if not containing specified watermark. Our experiments show that even when the cropped image is distorted by noises of ratio 10%, our proposed strategy still works fine. Although we are so far only concerned with cropped square images, the principle should readily apply to the irregularly cropped images too. If cropped images further undergo rescaling or rotation, we just need to reverse the effect before applying to it the same procedure for testing the cropped images. However details on regular cropping and other forms of distortion will be left to a future work.

4 Experiments

We here first use the image *Goldhill* of 512x512 pixels for our experiments. The decomposition path is LH1, HL2, LH3, LH4, see Fig.1 for the meaning of the labels. The filters will come from (3) with q=2. We embed the watermark “goldhill” into the θ's in the following way. We choose to store 5 bits of the

(a) (b)

Fig. 8 Original and watermarked images

watermark into a single θ, leading to the step 0.19. All the θ_0's are to be used for the watermarks, all the θ_1's will contribute to the private key. We thus embed each character into each of θ_0's respectively. We decompose the image using the filters embedded with "goldhill" watermark, replace with the UWS logo as the pattern, and then synthesize to obtain the watermarked image Fig.8(b) from the original Fig.8(a).

To illustrate the robustness of our watermarking scheme, we watermark the same Goldhill image with different watermarks and add different level of noises. The results are consistent with our theory in the previous section, and are subsequently tabulated in Table 1, where 1-4 in the path stand for the quadrants LL, HL, HH and LH respectively.

Table 1. Watermark detection

path	watermark	noise	PSNR	RMS	ε
4244	goldhill		318.08	0	<
4242	goldhill		23.81	16.439	>
4234	goldhill		24.89	14.522	>
4244	goldhill	2%	45.06	1.425	<
4244	goldhill	3%	41.47	2.153	<
4244	goldhill	4%	39.13	2.818	>
4244	goldhill	5%	37.55	3.38	>
4244	**golehill**		38.47	3.040	>
4244	**llihdlog**		24.23	15.501	>

Another test using the image *Peppers* as in Fig.9 is similarly conducted and the results are shown in Table 2. In our choice of $\varepsilon = 2.5$ as the threshold for the watermark detection, we have assumed that images distorted by the noise ratio of 4% or over will seriously degrade the images in such a way that we won't be interested in general in pursuing their copyright issues. This threshold is consistent with the results in Table 1 as well as with the results conducted similarly on Barbara an Baboon test images to name a few. If the watermark tolerance is to exceed the noises of over 4%, we can either design the scheme with a larger step for θ and thus with a newer threshold ε, or simply make use our proposed second strategy designed mainly for detecting watermarks from the cropped images. To conclude this section we note that many experimental results that are directly related to the design of our scheme are already presented in the earlier sections and will thus not be reproduced here again.

Table 2. Watermark detection

path	watermark	noise	RMS	ε
4244	peppers		0	<
4242	peppers		16.77	>
4234	peppers		17.42	>
4244	peppers	2%	1.37	<
4244	peppers	3%	2.00	<
4244	peppers	4%	2.77	>
4244	peppers	5%	3.50	>
4244	**geggers**		7.78	>
4244	**pfppers**		3.78	>

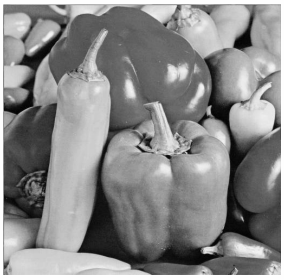

Fig.9 Peppers

5 Conclusion

We proposed a watermarking scheme on the basis of watermark-embedded wavelet filters and owner-assigned private keys, for the purpose of image ownership verification. Two detection strategies have been proposed: one through the use of detection threshold ε, and the other though a patching process. The latter is also applicable to the cropped images. Our proposed scheme has moreover an adjustable robustness via the choice of the parameters, and allows greater flexibility for watermark storage or performance optimization. The watermark detection also requires no original images for either of the proposed detection strategies.

References

1. Katzenbeisser,S., Fabien, A.P. Petitcolas, A.P. (eds.): Information Hiding Techniques for Steganography and Digital Watermarking. MA: Artech House, Norwood (2000)
2. Xia, X.G., Boncelet, C.G., Arce, G.R.: A Multiresolution Watermark for Digital Images, ICIP'97 (1997) 548-551
3. Hsu, C.T., Wu, J.L.: Multiresolution Watermarking for Digital Images, IEEE Trans. Circuits and Systems-II: analog and digital signal processing, Vol. 45(8) (1998) 1097-1101
4. Barni, M., Bartolini, F., Piva, A.: Improved Wavelet-Based Watermarking Through Pixel-Wise Masking, IEEE Trans. Image Proc., Vol. 10(5) (2001) 783-791
5. Zhu, W., Xiong, Z., Zhang, Y.Q., Multiresolution Watermarking for Images and Video, IEEE Trans. Circuits and Systems for Video Technology 9(4) (1999) 545-550
6. Sebe, F., Ferrer, J.D.: Oblilvious Image Watermarking Robust against Scaling and Geometric Distortions, Lecture Notes in Computer Science 2200 (2001) 420-432
7. Song, G., Wang, W.: Image-Feature Based Second Generation Watermarking in Wavelet Domain, Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 2251/2001 (2001) 16
8. Wang, Y., Doherty, J.F., and Dyck, R.E.V.: A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images, IEEE Trans. Image Proc. 11 (2002) 77-88
9. Jiang, Z., and Guo, X.: A Note on the Extension of A Family of Biorthogonal Coifman Wavelet Systems, The ANZIAM Journal, in press (2003)
10. Jiang, Z., and Guo, X.: Wavelets of Vanishing Moments and Minimal Filter Norms and the Application to Image Compression, Proc. of 6th ISSPA. Kuala-Lumpur, Malaysia, (2001) 108-111
11. Vetterli, M., Kovačević, J.: Wavelets and Subband Coding, Prentice-Hall, Englewood Cliffs (1995)
12. Burrus, C.S., Gopinath, R.A., Guo, H.: Introduction to Wavelets and Wavelet Transforms: A Primer. Prentice Hall, New Jersey (1998)
13. Jiang, Z., De Vel, O., Litow, B.: Unification and Extension of Weighted Finite Automata Applicable to Image Compression, Theoretical Computer Science A 302 (2003) 275-294