http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (2): 358-363, 2006
ISSN 1812-5638

A Robust Wavelet-based Blind Digital Watermarking Algorithm

[1,2]Cong Jin and [1]Jiaxiong Peng
[1]Institute for Pattern Recognition and Artificial Intelligence,
Huazhong University of Science and Technology, Wuhan 430074, People's Republic of China
[2]Department of Computer Science, Central China Normal University,
Wuhan 430079, People's Republic of China

Abstract: In this study we proposed a novel blind digital watermarking algorithm in wavelet domain. In order to realize extracting which not to depend on the original image excessively, we apply quantifying idea. Since the human visual system has especial responses on textures, the watermark embedded on textures has good robustness to general image processing and other attacks. So adjusting embedding strength through classifying embedded coefficients by using the detail coefficients that lies in the same layer with embedded coefficients. Present algorithm proved its robustness to general image processing and geometric attacks through experiments. The conclusions obtained by experiments are useful to the copyright protection and covert communication research in the future.

Key words: Digital watermarking, wavelet transform, robustness, blindness

INTRODUCTION

Recently, digital contents can be easily accessed by using computer networks and the problem of protecting multimedia information has become more and more important. As a solution to this problem, digital watermark technology is now drawing the attention as a new method of protecting copyrights for digital data[1,2]. It is realized by embedding information data with an insensible form for human audio/visual systems. We call the embedded information data watermark.

In general, a digital watermark technique must satisfy the following two properties. First, the embedded watermark does not spoil the quality of the image and should be perceptually invisible. The second property is that it doesn't require the original image for watermark detection. It is also robust to common image processing and geometric distortions.

Today, almost all of the proposed watermark algorithms could not meet the above requirements simultaneously, especially resistance to rotation, cropping, etc. A binary watermark sequence is embedded into the highest magnitude DCT coefficients[3]. Hence, this algorithm is robust against image processing and common geometric transformations. Hsu and Wu[4,5] proposed discrete cosine/wavelet transform algorithms to embed a binary watermark by modifying the middle-frequency coefficients. This algorithm is resistant to common image processing; but geometric distortions are still challenges. The main drawback[3-5] is requiring the original image to detect/extract the watermark.

Recently, a grayscale digital watermarking technique was proposed by Niu *et al*.[6]. The grayscale watermark, a visually recognizable pattern, is decomposed into eight binary bitplanes[6]. Some binary bitplanes are embedded into the middle DCT components of the original image, with the remainder used as the secret keys. The main disadvantages of this private watermarking algorithm are: (1) the original image is required to verify the existence of the watermark; (2) the robustness property is resistant to JPEG compression and general image processing, but geometric distortions are still challenges.

Base on the above facts, we propose an image watermarking algorithm based on the Discrete Wavelet Transform (DWT). The features of our algorithm are as follows. We do not require the original image for watermark detection and it is robust to common image processing and geometric attacks.

PRELIMINARIES

Wavelet transform: The wavelet transform is a mathematical tool for decomposing. We briefly review the DWT model (Fig. 1), which shows a 2-scale wavelet transform. The image is first decomposed into four subbands denoting LL_1, LH_1, HL_1 and HH_1. LH_1, HL_1 and

Corresponding Author: Cong Jin, Department of Computer Science, Central China Normal University, Wuhan 430079, People's Republic of China

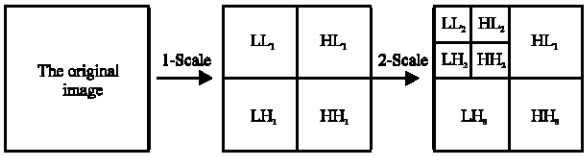

Fig. 1: The image is divided into seven subbands through 2-scale level wavelet transform

HH_1 contain the finest scale detailed wavelet coefficients, i.e., the higher frequency detailed information. LL_1, the coarse overall shape, is the low frequency component containing most of the energy in the image. The wavelet transform is then applied to obtain the next coarser scale by further decomposing LL_1 into LL_2, LH_2, HL_2 and HH_2. If the process is repeated t times, we can obtain the subband LL_t through t-scale level wavelet transform.

In the human visual system, people are more sensitive to low frequency components than high frequency components. Under reasonable attacks, the low frequency components can survive. Consequently, LL_t of the original image is very close to that of the altered image.

QUANTIZATION

Quantization is a lossy data compression method. A quantization is nothing more than an approximator. A simple example of quantization is shown in Fig. 2.

Here, every number less than -2 is approximated by -3. Every number between -2 and 0 are approximated by -1. Every number between 0 and 2 are approximated by +1. Every number greater than 2 is approximated by +3. Note that the approximate values are uniquely represented.

PROPOSED ALGORITHM

Although the low frequency components can survive after reasonable attacks, they are perceptible to the human eye. For this reason, most frequency-domain watermarking algorithms try to insert the watermark into the middle-range frequencies. However, that the low frequency components can survive under considerable attacks is a good property for watermark security. Hence, in this paper, we will apply the low frequency component for inserting watermark.

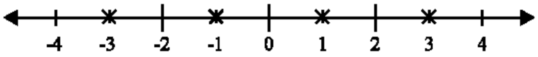

Fig. 2: A example of quantization

Usually the watermark is a pseudo-random sequence of real numbers. This kind of watermark can be used only to determine whether the watermark is present or not by detector, but the watermark oneself has no actual meaning. Along with request of the copyright protection increasing gradually, many scientists focus on meaningful watermark. Therefore, in this paper, meaningful binary pattern is used to the watermark.

The proposed new robust watermarking algorithm has the advantages of robustness for common image processing and not requiring the original image for watermark detection. The stages for this algorithm can be grouped into embedding stages and detection stages.

EMBEDDING WATERMARKING STAGES

We firstly introduce the following notation. Integer I(i, j), I′(i, j) indicate (grayscale or) luminance of the original image I and the watermarked image I' with eight bits per pixel, respectively. The original image I is defined as follows:

$$I = \{I(i,j) \mid 0 \le I(i,j) \le 255,\ 1 \le i \le W_I, 1 \le j \le H_I\}$$

Where, W_I and H_I is the width and height of I, respectively.

$$W = \{w(m,n) \mid w(m,n) \in \{0,1\}, 1 \le m \le W_W, 1 \le n \le H_W\}$$

Where, W_W and H_W is the width and height of W, respectively. Without losing the generality, let W_I and H_I are a power of 2. Let meaningful binary watermark W be stored into a one-dimension vector, defined as $\tilde{W}$.

Step 1. Wavelet transforming of the original image: Mallal[7] stated that we know that wavelet Haar has very good performance. Since filter length of wavelet Haar is the most short, computational complexity of its decomposing and reconstructing is lower than other wavelet. At the same time, Mallat algorithm is to infinite signal, but natural image is finite, therefore wavelet need be continued when processing image. However, it is very special for wavelet Haar, its boundary needn't be continued. Further, Liuetal[8] also stated that we know that wavelet Haar is the most suitable for digital watermarking. Therefore, in this study, wavelet Haar is used.

In the wavelet transform phase, assume that the original grayscale image is decomposed into t scale subbands and LL_t is obtained. Here t is a predetermined constant. The owner can determine the value of t according to the tradeoff between the efficiency and the robustness. The size of the coarse overall shape, i.e., subband LL_t (L for short), is W_L by H_L, where:

$$W_L = \frac{W_I}{2^t}, \quad H_L = \frac{H_I}{2^t}$$

and

$$L = \{L(i,j) | \ 0 \le L(i,j) \le 255, 1 \le i \le W_L, 1 \le j \le H_L\}$$

All wavelet coefficients in the L were stored into a one-dimension vector C.

Step 2. Selection of embedding coefficient: A random sequence Index is generated firstly by secret key K. Only algorithm's designer owns this secret key and position of embedding i-th watermark bit $\tilde{W}(i)$ is determined by Index(i), i.e., the wavelet coefficient of embedding watermark bit is C(j)(j = Index(i)). Therefore, it are required that Index's element is mutually inequality and the Index's value don't exceed number of the wavelet coefficients.

Step 3. Embedding watermark method: By modifying selected the wavelet coefficient C(j), the watermark bit flow $\tilde{W}(i)$ is embedded. After selected the wavelet coefficient C(j) is quantized by step length q, which is a predetermined positive integer, if $\tilde{W}(i) = 0$, then quantization value is modified into an even number of the nearest C(j)/q; and if $\tilde{W}(i) = 1$, then quantization value is modified into an odd number of the nearest C(j)/q. And inverse quantization is adopted. Based on the above, the embedding watermark method was described as follows:

- By step length q, whole real field were divided into some small subintervals, i.e.,$[k\cdot q,(k+1)\cdot q]$, $(k = 0,\pm1,\pm2,...)$. Without losing the generality, let real number $C(j) \in [N\cdot q,(N+1)\cdot q]$ where N is integer.
- Let quantization value of C(j) be Q(j). If $\tilde{W}(i) = 0$, one of N and N+1 is an even number inevitably, then let Q(j) equal to this even number and if $\tilde{W}(i) = 1$, one of N and N+1 is an odd number inevitably, then let Q(j) equal to this odd number.
- After Q(j) inverted quantization, modified wavelet coefficient $C'(j) = Q(j)\cdot q$ is obtained.

Step 4. Wavelet inverse transform: For the wavelet coefficients of have embedded watermark, t-scale level wavelet inverse transform were adopted and watermarked image is obtained.

Detect watermarking stages: The original image isn't required to detect the existence of the watermark. The detect process have four steps as follows:

Step 1: The tested image is t-scale level discrete wavelet transform.

Step 2: By secret key K, the same with embedding watermark, the positions of embedding watermark were determined and corresponding coefficients were obtained.

Step 3: Let C′(j) be an obtained coefficient and N = round $\frac{C'(j)}{q}$. Watermark bit values were extracted by using N's odevity.

Step 4: Let one-dimension watermark bit flow be stored into a two-dimensional meaningful binary watermark.

RELEVANT QUESTIONS DISCUSSING

Decide quantization step length q: To improve the robustness of our algorithm for to common image processing and geometric distortions, the quantization step length q have to be decided.

For the low frequency coefficients, according to the strong or weak of the locally texture in the corresponding position, it will be divided into two classes, defined as S_1 and S_2, respectively. Where, S_1 is a point set with the strong texture and S_2 is other point set with the weak texture. Embed points of corresponding different class should adopt different the quantization step length.

Because subbands LH_t, HL_t and HH_t contain the finest scale detailed wavelet coefficients, i.e., LH_t, HL_t and HH_t contain texture or edges information of the image, texture of embedding coefficients was classed by using them. For embedding coefficient L(i,j), let corresponding subbands wavelet coefficients be LH(i, j), HL(i, j) and HH(i, j), respectively. Let the average of corresponding subbands wavelet coefficient amplitudes be mean LH, mean HL and mean HH, respectively.

We know that the bigger the absolute value of coefficient, the stronger the texture of corresponding position. Therefore, to judge the texture strong or weak of corresponding position by using subbands, mean LH, mean HL and mean HH will be used. Judgment method is described as follows:

If (LH(i, j)≥ mean LH) or (HL(i, j)≥ mean HL) or (HH(i, j) ≥ mean HH),

Then LH(i, j)$\in S_1$, else LH(i, j)$\in S_2$.

If LH(i, j)$\in S_1$, then $q = q_1$, else $q = q_2$, where, $q_1 > q_2$.

Selection of the wavelet decomposing scale t: We know that, as the wavelet decomposed scale t increasing, the amplitude of low frequency coefficient increases with the approximate 2 multiple. Usually, the watermark is thought to be a weak signal added to strong background (i.e., the original image). So long as the weak signal added is lower than the contrast sensitivity threshold, the human vision system can't feel its existence. According to Weber's law[9], the contrast sensitivity threshold is proportional to amplitude of the background signal. This shows that, as the wavelet decomposed scale t increasing, strength of embedding watermark can increase with approximate 2 multiple.

According to the above consider, as the wavelet decomposed scale t increasing, strength of embedding watermark will increase significantly. Thus, robustness of the watermark may be improved. Moreover, the more wavelet decomposed scale t, the better components of watermark can be spread. So, for the watermark algorithms, the wavelet decompose scales should be improved possibly according to the amount of the watermark data.

RESULTS AND DISCUSSION

To prove the robustness of our algorithm for common image processing and geometric distortions, we performed some experiments with some grayscale standard images. Here, we describe experimental results using the standard image baboon (512×512 pixels, 8 bits/pixel) in Fig. 3a. The watermark is (64×64 pixels) in Fig. 3b and the watermarked image I' after embedding Fig. 3b into Fig. 3a according to our algorithm is shown in Fig. 3c.

In present experiments, the original image is 4-scale level wavelet transformed and the quantization step lengths are $q_1 = 16$ and $q_2 = 8$, respectively.

For evaluate the quality the test image and the original image using the Peak Signal-to-noise Ratio (PSNR), where

$$\text{PSNR} = 10\log_{10}\frac{255\times 255\times W_I\times H_I}{\Sigma(I(i,j)-I'(i,j))^2}$$

Here, similarity between the original watermark and extracted watermark is simply expressed in terms of the fraction y = X/M, where, M is the total number of original watermark points in both figures and X is the count of points from either original watermark that have at least one point from other original watermark in their 3×3 neighborhood.

PSNR of Fig. 3c is 41.8757dB. Figure 3d is a extracted watermark from Fig. 3c using our algorithm. Similarity between Fig. 3b and d is 1. This shows that the extracted watermark using our algorithm is very accurate.

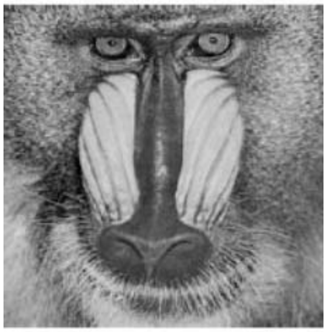

Fig. 3a: Original image

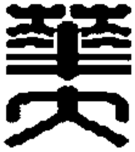

Fig. 3b: Original watermark

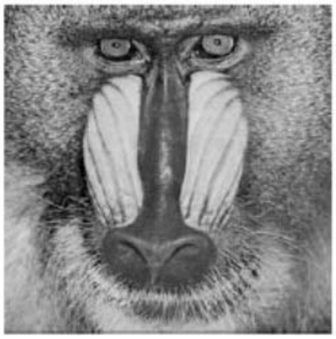

Fig. 3c: Watermarked image

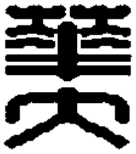

Fig. 3d: Detected watermark

TO TEST ROBUSTNESS

Image JPEG compression: The extracted watermarks are shown Fig. 4a-f, after JPEG compression version of Fig. 3c with parameters of 60, 50, 40, 30, 20 and 10 qualities, respectively and all 0% smoothing. Their PSNRs are reduced to 33.0483, 29.7978, 29.1957, 28.3831, 26.2983 and 23.8089, respectively.

Image noising: We add Gaussian noise (zero-mean and variance 0.001) to Fig. 3c, its PSNR is reduced to 29.9573 dB. The extracted watermark image are still recognizable and shown in Fig. 5a.

We add Salt and Pepper noise (noise density 0.005) to Fig. 3c, its PSNR is reduced to 28.5867 dB. The extracted watermark image are still recognizable (Fig. 5b).

Similarity measures between Fig. 5a, b and Fig. 3b shown in Table 1.

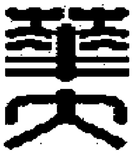

Fig. 4a: Quality = 60

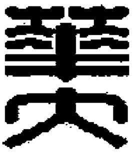

Fig. 4b: Quality = 50

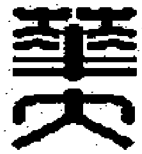

Fig. 4c: Quality = 40

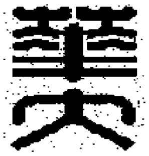

Fig. 4d: Quality = 30

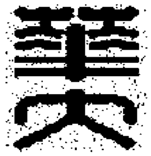

Fig. 4 e: Quality = 20

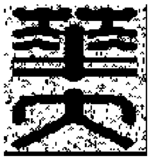

Fig. 4f: Quality = 10

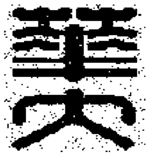

Fig. 5a: Gaussian

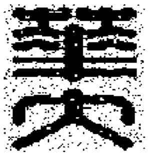

Fig. 5b: Salt and pepper

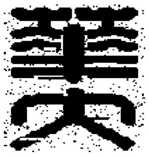

Fig. 5c: Rotation

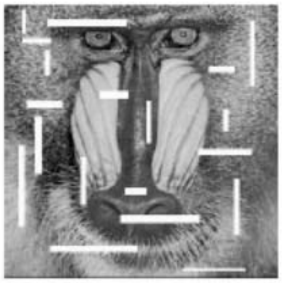

Fig. 6a: This is an image by cropping Fig. 3c irregularly

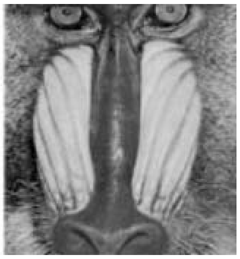

Fig. 6b: This is an image by cropping Fig. 3c

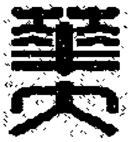

Fig. 6c: Cropped irregularly

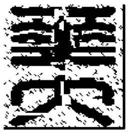

Fig. 6d: Cropped

Table 1: Similarity measure

Experiments	Similarity
Fig. 3c and 4a	0.9901
Fig. 3c and 4b	0.9695
Fig. 3c and 4c	0.9403
Fig. 3c and 4d	0.9215
Fig. 3c and 4e	0.8752
Fig. 3c and 4f	0.8160
Fig. 3c and 5a	0.9003
Fig. 3c and 5b	0.8752
Fig. 3c and 5b	0.7644
Fig. 3c and 6c	0.7904
Fig. 3c and 6d	0.7377
Fig. 3c and 7a	0.8541
Fig. 3c and 7b	0.7683
Fig. 3c and 7c	0.7126
Fig. 3c and 8a	0.8040
Fig. 3c and 8b	0.8742

Image rotation: Most watermarking schemes cannot survive after rotation. We rotate Fig. 3c 2° and resize it to 512×512. The PSNR is seriously reduced to 14.8170 dB. However, the extracted recognizable watermark image shown in Fig. 5c is still extracted.

Image cropping: Figure 6a shows an irregularly cropped version of Fig. 3c and Fig. 6b shows a cropped version of Fig. 3c where only the central region, containing the face of baboon remains. Their PSNRs are reduced to 11.3662 dB and 8.7647, respectively. We can still clearly retrieve the watermark image, as shown in Fig. 6c and d.

Image filtering: The detected watermarks are shown in the Fig.7a, b and c, after high-pass filtering, 3×3 median filtering and 3×3 mean filtering versions of Fig. 3c.

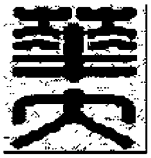

Fig. 7a: High-pass filtering

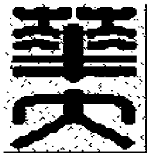

Fig. 7b: 3×3 median filtering

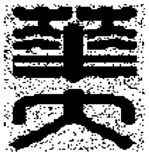

Fig. 7c: 3×3 mean filtering

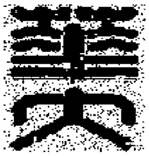

Fig. 8a: StirMark attack

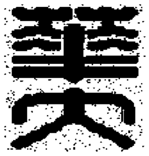

Fig. 8b: UnZignk attack

StirMark attack: Figure 3c is attacked using the StirMark attack one time with default parameters. Although Fig. 3c suffers an attack from the most powerful watermarking benchmark and the PSNR is reduced to 18.2970 dB, the retrieved watermark image is still recognizable to the human eyes. Figure 8a show the result.

UnZign attack: Figure 3c is attacked using the unZign process one time with default parameters and then the unZign-attacked Fig. 3c image is resized back to 512×512. Although Fig. 3c suffers the unZign attack and the PSNR is reduced to 23 dB, present watermark image is still recognizable. The retrieved watermark is shown in Fig. 8b.

Besides above experiments, we let other images be original images selected from USC-SIPI Image Database[10] for testing new algorithm. The experiment results show that this algorithm is still robustness for resisting various attacks.

In our algorithm, the exact ownership is verified if the retrieved watermark image is meaningful to the verifier. Through the experimental results, our algorithm has the following properties:

Robustness: Under standard attacks, our algorithm is robust to various image processing and geometric translations, such as JPEG compression, noising, rotation, cropping and filtering attacks.

Blindness: The extraction watermark does not require the original image. In practice, this is an essential property of the copyright protection and covert communication.

StirMark and unZign attacks: Experiment 6 and experiment 7 show that our algorithm survives under the StirMark and unZign attacks.

CONCLUSIONS

We believe that wavelet transform can play an important role in the digital image watermark. Based on this idea, we apply wavelet transform and quantization in our algorithm. This novel algorithm can be resistant to common image processing and simple geometric attacks. Furthermore, our algorithm can also resist StirMark and unZign attacks. It shows that our algorithm can apply in the copyright protection and covert communication.

REFERENCES

1. Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.
2. Swanson, M.D., M. Kobayashi and A.H. Tewfik, 1998. Multimedia data embedding and watermarking technologies. Proc. IEEE, 86: 1064-1087.
3. Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.
4. Hsu, C.T. and J.L. Wu, 1998. Multiresolution watermarking for digital images. IEEE Transactions on Circuits and System II: Analog and Digital Signal Processing, 45: 1092-1096.
5. Hsu, C.T. and J.L. Wu, 1999. Hidden Digital Watermarks in Images. IEEE Trans. Image Process., 8: 58-68.
6. Niu, X.M., Z.M. Lu and S.H. Sun, 2000. Digital watermarking of still images with gray-level digital watermarks. IEEE Trans. Consumer Electronics, 46: 137-145.
7. Mallat, S., 1998. A Wavelet Tour of Signal Processing. Academic Press, pp: 56-124.
8. Liu, J.F., D.R. Huang and J.Q. Hu, 2003. The orthogonal wavelet bases for digital watermarking (in Chinese). J. Elect. Inform. Technol., 25: 453-459.
9. Gonzalez, C. and P. Wintz, 1987. Digital Image Processing. 2nd Edn., IEEE Press: Piscateway, NJ, USA, Addison-Wesley Publishing Co., pp: 45-138.
10. USC-SIPI Image Database, 1997. http://sipi.usc.edu /database/database.cgi?volume=misc