Key Engineering Materials Vols. 321-323 (2006) pp 1301-1305
online at http://www.scientific.net

Online available since 2006/Oct/15

Wavelet Based Multi-bit Fingerprinting Against Geometric Distortions

Won-gyum Kim [a*], Yong-seok Seo[b], Hye-won Jung[c], Seon-hwa Lee[d], and Won-geun Oh[e]

Digital Contents Research Division, Electronics & Telecommunications Research Institute (ETRI)
161 Gajeong-dong, Yuseong-gu, Daeduk Science Town, Daejeon, Korea

[a]wgkim@etri.re.kr, [b]yongseok@etri.re.kr, [c]leonid92@etri.re.kr,
[d]seonhwa@etri.re.kr, [e]owg@etri.re.kr

Keywords: Digital fingerprinting, Watermarking, Wavelet, Geometric distortion.

Abstract. This paper presents a new image fingerprinting scheme which embeds a multi-bits fingerprinting code and is robust against the geometric attack such as rotation, scaling and translation. We construct a 64 bits fingerprinting code and embed into wavelet subband of 512x512 images repeatedly. In order to restore an image from geometric distortion a noise reduction filter is performed and a rectilinear tiling pattern is used as a template. Results of experimental studies show that our method is robust against geometric distortions and JPEG compression.

Introduction

Digital fingerprinting is one possible application of data embedding techniques, whereby some unique information, such as a serial number or a user ID assigned by the vendor to a given user/purchaser, is embedded into the multimedia content using watermarking techniques. One powerful class of attacks that adversaries may employ against watermarks and the corresponding fingerprints is collusion [1,2], whereby a coalition of users combines their different marked copies of the same multimedia contents in an attempt to attenuate/remove the trace of any original fingerprint. The fingerprint must, therefore, survive both standard distortions (such as compression, filtering and geometric distortion) and collusion attacks by users intending to destroy it.

Several methods have been proposed in the literature to embed fingerprints (watermarks) into different media and different domains [1,2]. But, these methods are not enough to present the variety of customer information as a fingerprint. To identify lots of customer's multi-bits embedding scheme is required. Moreover, RST distortions are also a big problem to be solved in the image watermarking and fingerprinting area [3].

In this paper, we propose a new image fingerprinting scheme which embeds 64-bits customer ID into the discrete wavelet transform (DWT) domain and extract this ID from the geometrically distorted image using ACF(Auto Correlation Function). The paper is organized as follows. How to embedding and extracting fingerprint information are presented in Section 2. The simulation results and conclusions are given in Section 3 and 4, respectively.

Proposed Fingerprinting Scheme

Fingerprint Embedding. In this section, we describe the way of 64-bits fingerprint construction and embedding procedure. Assume that a 64-bits message which can be separated as 8 symbols whose length is 8 bits is given. We suppose that each symbol has Alphabet capital and small letters and numeric numbers from 0 to 9, $S=\{s_1, s_2, s_3,...,s_N\} \in \{a,...,z,A,...,Z,0,...,9\}$. Then, we generate random sequences for every symbol from a secret key which can be represented in $r_i \in \{-1, +1\}$. Therefore, the total number

* Corresponding author

of r_i is (26×2+10)*8+1 = 497. Here, one random sequence is a sync message for the translation restoration. Finally, in order to produce fingerprint signal, *W*, the 9 random sequences corresponding to fingerprint symbols are merged together and the sign of the merged sequence is taken.

In order to be robust against JPEG compression the periodic fingerprint patterns are embedded into the detail subbands of wavelet decomposition level 2. The overall process of the proposed fingerprint embedding is shown in Figure 1. To extract fingerprint correctly from the corrupted image, it is important to restore the image from geometrical distortions. In the proposed system a rectilinear tiling pattern is used to do this. To construct the latticed template random sequence is embedded repeatedly as shape of unit block. Embedding unit blocks are used as a template to restore the captured image. In this paper the size of unit block is 32x32. For instance, if the image size is 512x512, then unit block is embedded 16 times repeatedly in the HL_2, LH_2, and HH_2 sub-bands.

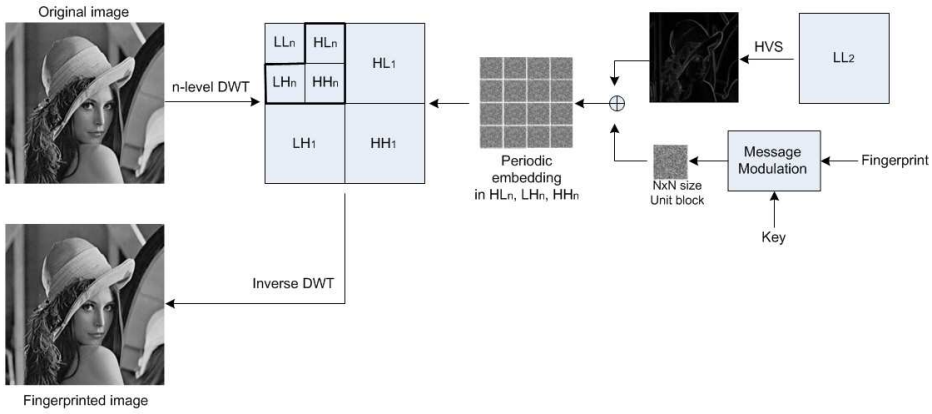


Fig. 1 Fingerprint embedding process.

HVS(Human Visual System) is a weighted function to make the image robust to various kinds of attacks and to improve imperceptibility. The basic idea of our HVS is that fingerprint is embedded strongly into the less recognizable regions of the image. To do this, we separate the image into three regions; flat, strong edge, and texture region according to edge detection value. If the edge detection value, *Edge(i,j)* is smaller than 2, we set position *(i,j)* to flat. On the contrary if the edge detection value is bigger than 2, we set position *(i,j)* to texture area. Especially if the edge detection value is bigger than threshold *T*, we set position *(i,j)* to strong edge area. *T* is defined as follows:

$$T = Aver_{Edge}(I) + 2 * StD_{Edge}(I)$$

Aver(i,j), *StD(i,j)*, and *Edge(i,j)* are local average, standard deviation, and edge detection value on *x(i,j)* respectively. For edge detection Prewitt operator is used. $Aver_{Edge}(I)$ and $StD_{Edge}(I)$ are average and standard deviation of edge detection values. HVS function is as follows:

$$\lambda(i,j) = \begin{cases} \alpha & Flat, Strong\ edge\ area \\ StD(i,j) * WF(Avg(i,j)) & Otherwise \end{cases} \quad where,\ \ WF(i) = (2 - \tanh(i/25))/3,\ \ i = [0...255]$$

α is minimum embedding strength and set to 3. *WF(*)* is a weighted function for dark and bright area. So, fingerprint is embedded strongly by this function because these areas are less sensitive than normal area.

Fingerprint Extracting. In this paper general correlation detector is used to extract fingerprint. But, pre-processing is needed before extracting because the fingerprinted image includes various kinds of distortions. Although we embed the fingerprint into the DWT domain, we can extract the periodicity of the fingerprint like the spatial domain method by using a high-pass filter or a noise removal filter. In our method, the periodic signal is extracted by using a Wiener filter, and the average of the local variances is used as the noise variance of the Wiener filter.

To find the periodicity, the ACF of the estimated signal is calculated. The ACF can be calculated by a fast correlation function based on FFT. The peak detection is described in the following steps.

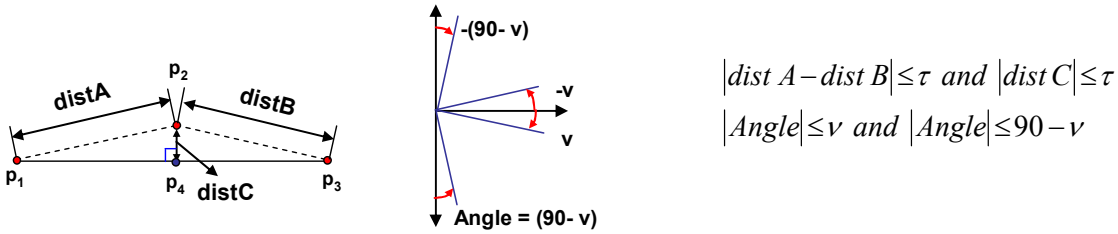
step 1: The AC peaks are filtered by applying an adaptive threshold as follows:

$$ACF > \mu + K\sigma$$

μ and σ denote the average and standard deviation of the auto-correlation function, respectively. K is a user defined value and set to 2.

step 2: Local maximum of each unit block is found from a lot of AC peaks. This preprocess removes a number of unnecessary auto-correlation points, and we have some candidate peaks of the real peaks.

step 3: The lines are extracted from three points using the offset information of the local peak points, and line groups are also classified from those lines as following conditions.



$$|dist\ A - dist\ B| \le \tau \ and\ |dist\ C| \le \tau$$
$$|Angle| \le \nu \ and\ |Angle| \le 90 - \nu$$

Fig. 2 Line extraction and grouping condition.

where, $|distA|$ and $|Angle|$ are the distance between two peaks and difference of the gradient between two lines. The threshold τ (pixels) and ν (degree) are decided experimentally according to the performance of the system. Because the peaks to find have a uniform periodicity, line groups including the same gradient and same distance exist. The lager the number of line groups, the higher priority.

step 4: The orthogonal pair is extracted from the line groups with high priority. Although x scale differs from y scale, two lines must meet at the right angle. Orthogonal pair, $OP=\{op_1,op_2,...,op_N\}$, among angles of line groups can be found. The answer with the highest probability is op_1. We can finally restore the fingerprinted image using op_i including angle and scale value. op_i is can be found from two lines. However, only a line may be detected due to strong attacks. In this case, we can extract orthogonal pairs through comparison of the right angle between the line and AC peaks.

Figure 3 shows the extracted lines from local maximum peaks.

(a) Attacked image (b) Local max peaks (c) Extracted lines

Fig. 3 Local maximum peaks and line detection result.

We propose a novel design to restore the translation because of the difference of the size between the sync and extracted fingerprint. Figure 4 shows the restoration process for translation error.

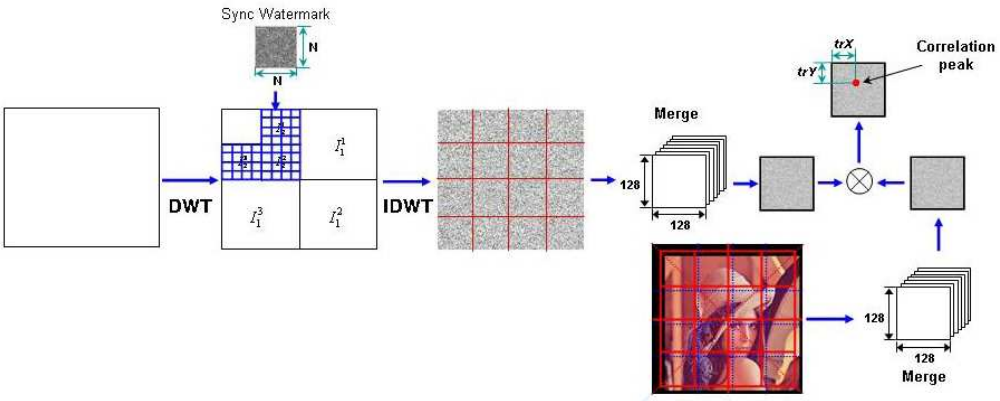


Fig. 4 Translation restoration process.

Following steps describes the process of the translation restoration:

step 1: Zero padding image(M×M) is decomposed by DWT up to the 2nd level.

step 2: Then, a fingerprint for sync is embedded in a way we describe in previous section.

step 3: The sync image coming out of Inverse DWT(IDWT) and the image getting out of the RS restoration are divided into 16 parts, which are merged into an image of size M/4×M/4.

step 4: To find out the correlation peaks, the ACF between two merged signals is calculated.

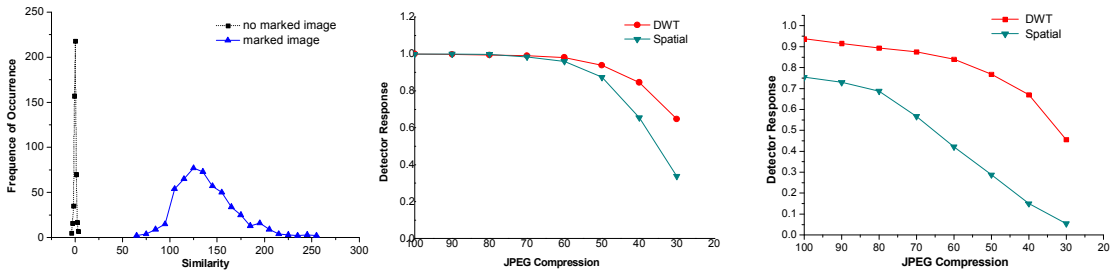
step 5: The translation restoration is performed through the circular-shift algorithm by the peak point(*trX, trY*).

After correcting translation error, IDWT is applied to the image to extract the fingerprint. Actually the fingerprint is extracted by performing cross-correlation function between the last estimated fingerprint signal and the random sequence set. The one symbol is determined by the location having the maximum value among the 62 random sequences corresponding to symbols. All 8 symbols can be extracted using the same way.

Experimental Results

We measure the fingerprint similarity and the detector response of fingerprint signal according to JPEG compression, and the fingerprint detection performance against geometric attacks. For this test, we use 500 photo images(512×512, 24 bits). The average PSNR of the fingerprinted image is 38dB on average. To obtain a period(128×128) in the spatial domain, 16 periodic fingerprinting patterns(32×32) are embedded in the 2nd level wavelet sub-bands. The detector response between the original and the extracted fingerprint is shown in Figure 5(a).

We test the detection responses from estimated fingerprint signal after JPEG compression comparing the DWT to the spatial domain. And we also test the fingerprint detection response against 240 RST attacks, which is randomly selected from 30 images. The ranges of RST attack are -44°~+44° for rotation, 50%~200% for scaling, and 0~128pixels for translation.



(a) Detector response (b) Only JPEG compression (c) Rotation & Scaling attack

Fig. 5 Detector response after JPEG Compression.

Figure 5(b) shows that the fingerprint detection rate for JPEG compression(QF 40%) is about 85% in the DWT domain. While the fingerprint detection rate in the same condition is about 65% in the spatial domain. Figure 6(c) shows that the fingerprint detection rate for RS attacks with JPEG compression(QF 40%) is about 78% in the DWT domain, while about 15% in the spatial domain. We notice that the drastic difference in the RST attack makes an appearance. Experiments show the proposed method has better robustness than a conventional ACF-based watermarking against geometric distortions and JPEG compression. Next, we test robustness for collusion attack. We embed different fingerprint ID into different images and average together. Simulation results, until 4 collusions we can extract fingerprint ID completely, but we fail to extract fingerprint ID when 5 colluders joins the collusion.

Summary

We have a proposed a novel image fingerprinting scheme which embeds a 64-bits customer ID as a fingerprint code. In order to restore a corrupted image from distortions a noise reduction filter is performed and a rectilinear tiling pattern is used as a template. To make the template a multi-bits fingerprint is embedded repeatedly like a tiling pattern into the DWT domain of the image. Simulation results show that the proposed scheme has some robustness against JPEG compression, RST and collusion attacks.

References

[1] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, “Collusion-Resistant Fingerprinting for Multimedia,” *IEEE Signal Processing Magazine*, pp.15-27, 2004.

[2] J. Dittmann, "Combining Digital Watermarks and Collusion Secure Fingerprints for Customer Copy Monitoring," *Proc. IEE Seminar Sec. Image & Image Authentication*, pp.128-132, Mar. 2000.

[3] S. Pereira, and T. Pun, “Robust Template Matching for Affine Resistant Image Watermarks,” *IEEE Transaction on Image Processing*, vol. 9, no. 6, pp.1123-1129, 2000.