A COMPOSITE APPROACH FOR BLIND GRAYSCALE LOGO WATERMARKING

Elliot First[1] and Xiaojun Qi[2]

[1]FirstE@ripon.edu
Mathematics and Computer Science Department, Ripon College, Ripon, WI 54971
[2]xqi@cc.usu.edu
Computer Science Department, Utah State University, Logan, UT84322-4205

ABSTRACT

This paper presents a composite blind digital watermarking technique, CompMark, to hide a visually meaningful grayscale logo in a host image. The multi-resolution fusion principles are used to embed the grayscale logo in perceptually significant blocks in wavelet subbands of the host image. A modulus approach is further used to embed a binary counterpart of the logo in the approximation subband. The extraction process combines both extracted grayscale and binary logos to obtain a better, recognizable logo at the receiver. The watermark detection decision is based on either the correlation between the thresholded extracted and embedded logos or the visual similarity. Experimental results demonstrate our scheme is robust against compression, white noise addition, histogram equalization, and image filtering techniques. In addition, it performs better than a peer blind scheme, XFuseMark.

Index Terms— Grayscale logo watermarking, modulus embedding, additive fusion principles

1. INTRODUCTION

Watermarking is a viable solution to copyright protection of digital images. It normally embeds an invisible digital code into a host image to provide authentication information. In general, watermark is embedded in spatial or frequency domain and extracted by applying the same embedding process on the probe image (a blind extraction) or on the probe and original images (a non-blind extraction). A statistical approach may be further applied to detect the presence of the watermark.

In this paper, we propose a novel blind grayscale logo watermarking technique to protect copyrights since a recognizable mark is more convincing than a random numerical sequence and visually meaningful mark may improve the trustworthiness of identification or security for *non-technical arbitrators* [1]. Several logo watermarking techniques are briefly reviewed here. Voyatzis and Pitas [2] use a chaotic system to scramble a binary logo to modify selected host image pixels. A statistical detection certainty is provided to indicate the watermark existence without resorting to the original image. Zhang *et al.* [3] embed a binary logo into the multi-wavelet domain of the image and extract the logo using the characteristics of the relationship between the logo and the watermarked image. Hien *et al.* [4] embed a binary logo in the wavelet domain of the host image and apply ICA (Independent Component Analysis) to extract the logo. Niu *et al.* [5] present a non-blind watermarking scheme by inserting the bit planes of grayscale logos into the wavelet domain of the original video clip. Kundur and Hatzinakos [6] develop a FuseMark system to combine the wavelet-based multi-resolution subimages of the host image and the grayscale logo using data fusion principles and Dooley's HVS (Human Visual System) model. Reddy and Chatterji [7] improve the FuseMark system by using Barni's pixel-wise masking HVS model. However, both systems need the original host image to extract the embedded logo. Xie and Shen [8] develop a blind watermark system, XFuseMark, by fusing multi-resolution subimages of the host image and the DCT-based grayscale logo. However, all these systems either require the original image to gain more robustness against various common image processing attacks or require human's visual judgment on the extracted noisy logo for determining the existence of the watermark.

In this paper, we develop a blind grayscale logo watermarking system called CompMark to resist compression, and other common image processing attacks. This technique embeds a grayscale logo and its binary version in different wavelet-based multi-resolution subimages using two complementary approaches, namely, the additive image fusion and the modulus embedding, respectively. The two extracted logos are then combined to construct the final logo and a correlation value is used to determine the presence of the watermark. The remainder of the paper is as follows. Section 2 describes the proposed logo embedding scheme. Section 3 presents the details of the logo extraction and detection. Section 4 shows the experimental results. Section 5 draws conclusions.

2. LOGO EMBEDDING SCHEME

CompMark uses two complementary techniques to embed a grayscale logo and its binary counterpart in different

wavelet subbands. The first technique is to adaptively embed a DCT-based grayscale logo into the wavelet-based multi-resolution subimages of the host image using the additive fusion principles. The second technique is to embed the binary counterpart of the grayscale logo into the detail subband using the modulus embedding. These two techniques compensate the shortcomings of each other to provide more robustness in logo watermark extraction and detection and provide more robustness against common image processing attacks.

2.1. Additive Grayscale Logo Embedding and Modulus Binary Logo Embedding

The following seven steps describe the embedding procedure in detail.

Step 1: Obtain a wavelet coefficient matrix H by performing a 3-level DWT on the host image h using the Daubechies 9/7 bi-orthogonal filters.

Step 2: Prepare a grayscale logo g whose size is smaller than or equal to the approximation subband (the top left subband) of H and perform several preprocessing steps on g. Specifically, a DCT is first applied on g to obtain a DCT coefficient matrix G_1. The upper left square corner of G_1 is then set to 0's to ensure that all the DCT coefficients are relatively small, where the corner size equals min(m, n)/4 with m and n being the number of rows and columns in g. Normalization is further applied to this newly changed matrix G_2 by dividing each element by a scaling factor $\left\| \sum_{i-1,j=1}^{i=m,j=n} G_2(i,j)/100 \right\|$ to reduce the logo strength for invisible distortion. The final preprocessed logo G is obtained by permuting the normalized G_2 using a private key K_1 to ensure security.

Step 3: Find suitable regions for adaptive additive embedding. First, independently partition the subband images in level 1 and level 2 into nonoverlaping blocks H_k of size $m \times n$. Second, compute the perceptual significance of each block by $Q_k = \sum_{i=1,j=1}^{i=m,j=n} H_k(i,j)^2$. Third, obtain ordered blocks H_{ksort} by sorting H_k in a descending order of Q_k.

Step 4: Separately embed the preprocessed logo G to the top B percentage of the ordered H_{ksort} by:

$$H'_{ksort}(i,j) = H_{ksort}(i,j) + \alpha \cdot G(i,j) \quad (1)$$

where $1 \le i \le m, 1 \le j \le n$, and α is the embedding strength.

Step 5: Obtain a binary logo b by:

$$b(i,j) = \left\lceil \frac{g(i,j) - \text{mean}(g)}{\max(g)} \right\rceil \quad (2)$$

where $1 \le i \le m$, and $1 \le j \le n$.

Step 6: Embed the private key K_1-based permuted binary logo b into the detail subband H_a using quantization-based Eq. (3), where β is the modulus embedding strength and is empirically set to 30 in our system.

Step 7: Apply the inverse DWT on the modified wavelet coefficient matrix H' to obtain the watermarked image h'.

Since both logos are randomly shuffled in their embedding schemes, they behave like random noise [9]. That is, embedding two correlated logos into different subbands is equivalent to adding two kinds of noise by:

$$h'(i,j) = h(i,j) + \alpha A(i,j) + C(i,j) \quad (4)$$

where $A(i,j)$ is noise added by embedding the grayscale logo using the additive method and $C(i,j)$ is the noise added by embedding the binary logo using the modulus method.

2.2. Determination of Two Adaptive Parameters

Two parameters, additive embedding percentage B and additive embedding strength α, are adaptively determined for each host image.

The additive embedding percentage B is determined by the texture of the host image. A range filter is first applied to decide a texture map $T(i, j)$ of the host image h. That is, for every pixel in h, its texture is computed as the difference between the maximum and minimum pixel intensities within its 3×3 neighborhood window. The following formula is then applied to compute B:

$$B = \frac{\sum_{i=1,j=1}^{i=m,j=n} \lceil T(i,j) - mean(T)/4 \rceil}{m \times n} \quad (5)$$

The ideal embedding strength α is adaptively computed as follows:

1. Determine the target PSNR value Φ using image h_0, which is generated by adding a small amount of uniform white noise to the host image h.
2. Choose an initial strength range as $[\alpha_0, \alpha_1]$ with $\alpha_0 = 0.1$ and $\alpha_1 = 2$.
3. Compute the embedding strength as $\alpha = (\alpha_0+\alpha_1)/2$.
4. Embed the grayscale logo g into h using steps 1, 2, 3, 4, and 7 as described in section 2.1 to produce a watermarked image h'.
5. Compute the distortion d as the PSNR value of h'.
6. If $\|\Phi - d\| < 0.25$, the current α value will be the ideal additive embedding strength.
7. Else if $d < \Phi$, $\alpha_0 = \alpha$. Go back to step 3.
8. Else if $d > \Phi$, $\alpha_1 = \alpha$. Go back to step 3.

$$H'_a(i,j) = \begin{cases} H_a(i,j) - \left(H_a(i,j) \bmod \beta\right) + .75\beta & \text{if } b(i,j) = 1 \text{ and } \left(H_a(i,j) \bmod \beta\right) \ge 0.25\beta \\ \left[H_a(i,j) - .25\beta\right] - \left[(H_a(i,j) - .25\beta) \bmod \beta\right] + .75\beta & \text{if } b(i,j) = 1 \text{ and } \left(H_a(i,j) \bmod \beta\right) < 0.25\beta \\ H_a(i,j) - \left(H_a(i,j) \bmod \beta\right) + .25\beta & \text{if } b(i,j) = 0 \text{ and } \left(H_a(i,j) \bmod \beta\right) \le 0.75\beta \\ \left[H_a(i,j) + .5\beta\right] - \left[(H_a(i,j) - .5\beta) \bmod \beta\right] + .25\beta & \text{if } b(i,j) = 0 \text{ and } \left(H_a(i,j) \bmod \beta\right) > 0.75\beta \end{cases} \quad (3)$$

3. BLIND LOGO EXTRACTION AND DETECTION

The blind logo extraction procedure is described as follows:

Step 1: Obtain a wavelet coefficient matrix P by performing a 3-level DWT on the probe image p using the Daubechies 9/7 bi-orthogonal filters.

Step 2: Independently partition the subband images in levels 1 and 2 into nonoverlaping blocks P_k of size $m \times n$.

Step 3: Apply the same range filter and Eq. (5) as described in the embedding process to choose B' percentage of the most perceptually significant blocks for grayscale logo extraction, where we set $B' = 0.85B$ to ensure all the chosen blocks contain the possibly embedded logo.

Step 4: Generate the shuffled logo in DCT domain by:

$$w_a^s(i,j) = \sum_{k=1}^{k=N} \frac{P_k(i,j)}{Q'(k)} \tag{6}$$

where N equals the number of blocks for extraction (i.e., top B' percentage of the most perceptually significant blocks) and $Q'_k = \sum_{i=1,j=1}^{i=m,j=n} P_k(i,j)^2$.

Step 5: Use the private key K_1 to restore w_a^s and apply the inverse DCT to obtain the extracted grayscale logo w_a .

Step 6: Normalize the extracted grayscale logo w_a by:

$$w_a^{'} = round\left(\frac{w_a - \min(w_a)}{\max(w_a)} \times 255 \right) \tag{7}$$

Step 7: Extract the shuffled binary logo from approximation subband P_a:

$$w_b^s = \begin{cases} 1 & if\ P_a(i,j) \bmod \beta > 0.5\beta \\ 0 & if\ P_a(i,j) \bmod \beta \le 0.5\beta \end{cases} \tag{8}$$

Step 8: Restore the extracted binary logo $w_b^{'}$ by applying the private key K_1 on w_b^s .

Step 9: Obtain the final extracted logo w' by:

$$w'(i,j) = \begin{cases} w_a^{'}(i,j) - \delta \times mean(w_a^{'}) & if\ w_b^{'}(i,j) = 0 \\ w_a^{'}(i,j) + \delta \times mean(w_a^{'}) & if\ w_b^{'}(i,j) = 1 \end{cases} \tag{9}$$

where δ is empirically determined to 0.25 in our system.

The watermark detection decision is based on either the correlation between the extracted and embedded grayscale logos or the visual similarity. Specifically, the extracted logo is converted into its binary counterpart using Eq. (2). The correlation between the original and extracted binary logos is computed and compared with a predetermined threshold to determine the logo presence. In our system, the threshold is set to 0.4 since it is experimentally proved to be a good measure with few false positives.

4. EXPERIMENTAL RESULTS

The performance of CompMark has been tested on a variety of 512×512 grayscale images using several 64×64 grayscale logos under different common image processing attacks. These grayscale images contain low, medium, high textures, or a combination of different textures on different areas.

Watermark invisibility is evaluated on images of Lena, Baboon, Peppers, Plane, Texture, and Beach. The PSNR values for these 6 watermarked images are 43.93, 44.02, 44.01, 44.14, 44.40, and 44.15, respectively. These values are greater than 35.00db, which is the empirical value for the image without any perceivable degradation. Fig. 1 shows these watermarked images to demonstrate the invisibility.

Fig. 1: The invisibility of the watermarked images

Simulation results for JPEG compression with different QFs (Quality Factors) including 90, 60, and 40, JPEG2000 compression with different bit rates including 0.9, 0.6, and 0.3bpp, GF (Gaussian Filtering), mean filtering, median filtering, HE (Histogram Equalization), additive noise, and sharpening are presented. Figures 2 through 5 show logos extracted from 4 watermarked images under the above attacks. *The correlation value between the thresholded extracted and original images is listed below each attack.* In addition, the watermark detection failure is specifically marked by a letter "F". From these figures, it clearly shows that most extracted logos, though distorted, are still easily recognizable by human eyes. The average of the correlation values computed from 4 different textured watermarked images under the attacks listed in the same order as shown in figures 2 through 5 are: 0.9589, 0.8481, 0.6648, 0.5388, 0.9600, 0.9611, 0.8605, 0.9382, 0.3783, 0.4534, 0.4947, 0.8517, 0.4270, and 0.6449, respectively. It clearly demonstrates our scheme is robust against all the listed attacks except the mean filtering. This performance is better than the peer system XFuseMark [7], which is robust to certain level of noise addition, JPEG compression with QF down to 65, and JPEG2000 compression with a bit rate down to 0.6bpp. Our system also provides an effective correlation measure to determine the logo presence.

5. CONCLUSIONS

In this paper, we propose a blind watermarking scheme, CompMark, to hide a small grayscale logo invisibly in the host image. The major contributions are: 1) Use two complementary approaches, the additive image fusion and the modulus embedding, to respectively hide the grayscale logo and its binary counterpart for increasing the quality of the extracted logo. 2) Design two blind schemes to extract the grayscale and binary logos. 3) Combine the two extracted logos to construct the final recognizable logo with less distortion. 4) Derive a correlation measure using the binary versions of the extracted and embedded logos.

Our scheme is robust against a wide variety of image processing attacks as indicated in the experimental results. It also achieves better performance than the XFuseMark system. However, it is not as robust against common image processing attacks as the non-blind watermarking system, FuseMark [6]. A more efficient fusion and extraction system will be explored to improve the robustness against common image processing and possibly geometric attacks.

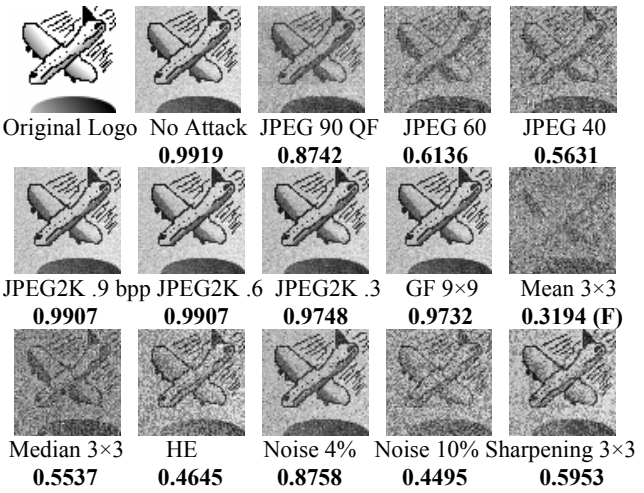


Fig. 2: Logos extracted from watermarked Lena image under different image processing attacks

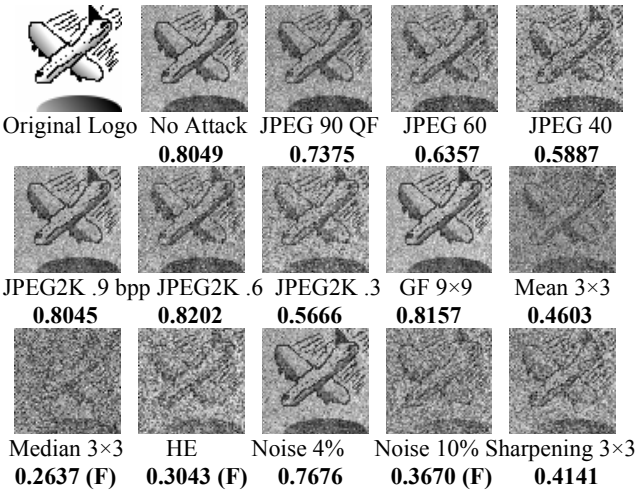
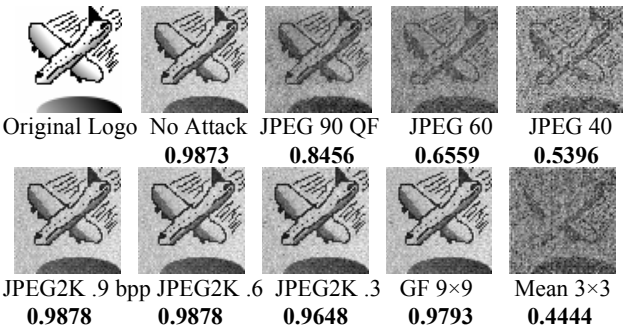


Fig. 3: Logos extracted from watermarked Baboon image under different image processing attacks



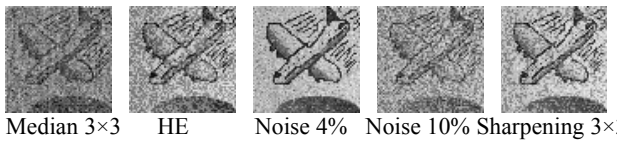


Fig. 4: Logos extracted from watermarked Pepper image under different image processing attacks

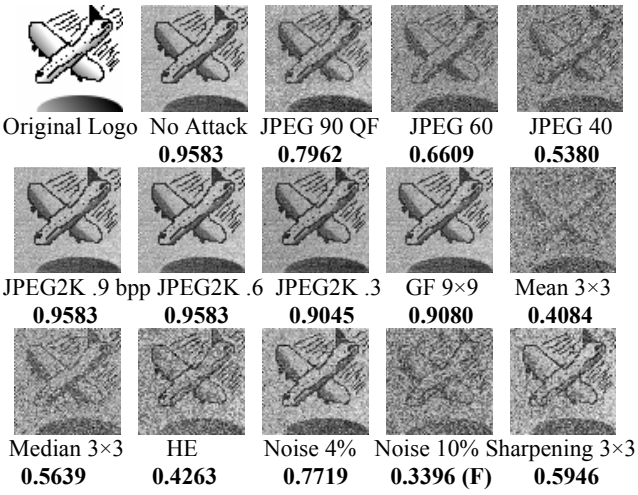


Fig. 5: Logos extracted from watermarked Plane image under different image processing attacks

6. REFERENCES

[1] G. W. Braudaway, "Protecting Publicly-Available Images with an Invisible Image Watermark," *Proc. of IEEE Int. Conf. on Image Processing*, Vol. 1, pp. 524-527, 1997.

[2] G. Voyatis and I. Pitas, "Digital Image Watermarking Using Mixing Systems," *Computational Graph*, Vol. 2, No. 4, pp. 405-416, 1998.

[3] J. Zhang, N. Wang, and F. Xiong, "Hiding a Logo Watermark into the Multiwavelet Domain Using Neural Networks," *Proc. of the 14th IEEE Int. Conf. on Tools with Artificial Intelligence*, pp. 477-482, 2002.

[4] T. D. Hien, Z. Nakao, and Y. W. Chen, "ICA-Based Robust Logo Image Watermarking," *Proc. of SPIE on Security, Steganography, and Watermarking of Multimedia Contents VI*, pp. 162-172, 2004.

[5] X. Niu, S. Sun, and W. Xiang, "Multiresolution Watermarking for Video Based on Gray-Level Digital Watermark," *IEEE Trans. on Consumer Electronics*, Vol. 46, pp. 375-384, May 2000.

[6] D. Kundur and D. Hatzinakos, "Toward Robust Logo Watermarking Using Multiresolution Image Fusion Principles," *IEEE Trans. on Multimedia*, vol. 6, no. 1, pp. 185-198, 2004.

[7] A. A. Reddy and B. N. Chatterji, "A New Wavelet Based Logo-Watermarking Scheme," *Pattern Recognition Letter*, Vol. 26, No. 7, pp. 1019-1027, 2005.

[8] G. Xie and H. Shen, "A New Fusion-Based Blind Logo Watermarking Algorithm," *IEICE Trans. on Information and Systems*, Vol. E89-D, No. 3, pp. 1173-1180, 2005.

[9] T. Leighton, I. J. Cox, J. Killian, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, Vol. 6, pp. 1673-1687, 1997.