Similar Patterns for Semi-blind Watermarking

Jae-hyun Cho, *Member, KIMICS*

Abstract—In this paper, we present a watermarking scheme based on the DWT (Discrete Wavelet Transform) and the ANN (Artificial Neural Network) to ensure the copyright protection of the digital images. The problem to embed watermark is not clear to select important coefficient in the watermarking. We used the RBF (Radial-Basis Function) to solve the problem. We didn't apply the whole wavelet coefficients, but applied to only the wavelet coefficients in the selected node. Using the ANN, although even the watermark casting process and watermark verification process are in public, nobody knows the location of embedding watermark except of authorized user. As the result, the watermark is good at the strength test-filtering, geometric transform and etc.

Index Terms—Watermarking, DWT(Discrete Wavelet Transform), ANN(Artificial Neural Network), RBF (Radial-Basis Function)

I. INTRODUCTION

Recently, various methods that protect the copyright of digital multimedia contents have been proposed [1-4]. In the situation, the studies of copyrighting multimedia contents have been proposed in many ways. About the time the term watermark was coined, counterfeiters began developing methods that forge watermarks used to protect paper money. Watermarking can be used in a wide variety of applications. In general, if it is useful to associate some additional information with a work, this metadata can be embedded as a watermark. The most important character of digital watermarking is imperceptible [5]. If the watermark is embedded, viewers should not see nor notice the mark. If the information of image is being distributed illegally, we can trace the flow of the data using the embedding the watermark in the information of the image. We can find the man who has distributed it.

There are various types of watermarking techniques that is public watermarking, blind watermarking and semi-blind watermarking [13]. There as been some confusion about the naming of watermarking techniques and the main reason is that people involved in this field come from different backgrounds (in particular signal processing and computer security). On top of this some terminology has been imported from the related field of steganography.

- Public watermarking: It is the same mean as the blind watermarking, but the wording was confusing with public-key watermarking and 'signal processing people' took over the field so only the later tends to remain. In these schemes the cover signal (the original signal) is not needed during the detection process to detect the mark.
- Semi-blind watermarking: Solely the key, which is typically used to generate some random sequence used during the embedding process, is required. In some cases you may need extra information to help your detector (in particular to synchronize its random sequence on the possibly distorted test signal). In particular some watermarking schemes require access tȯ the 'published' watermarked signal, which is the original signal just after adding the watermark
- Private watermarking: It is the same mean as the non-blind watermarking; the original cover signal is required during the detection process. At last, by asymmetric watermarking or public-key watermarking, people refer to watermarking schemes with properties reminding asymmetric cryptosystem (or public key cryptosystem). In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to blind watermarking where a secret key is required.

Recently, digital watermarking has been classified by two ways; spatial domain and frequency domain. In the spatial domain, the watermark is embedded directly in the spatial domain. In this process, various researches have been developed as PN-sequence (Pseudo random Noise Sequence) [6] and statistical method etc. The process to embed the watermark in spatial domain is simple and fast but it has disadvantaged that it's weak from the external attack, noise and JPEG compression.

Because of the result, the study of the watermarking is mainly researched in the frequency domain in recent. The process of watermarking in the frequency domain is that the watermark is embedded in the repetitive and characteristic coefficient among the generated coefficients which are transformed from FFT, DCT, Wavelet, and etc. Cox [4], [5] proposed the process of watermarking using the DCT. In the process, signal spread of frequency domain is widely distributed to transmit effectively the watermark signal without noise; filtering, compression and transform using spread spectrum communication. The energy of the specific signal spread is too small to be noticed, but the signal is extracted by PSNR (Peak Signal to Noise Ratio) using the location and variation of the original image signal. The problem of the process is not clear to select important coefficient, and partly characters can not be effective because of transforming the whole

Manuscript received September 30, 2004.

Jae-hyun Cho : School of Computer & Information Engineering, Catholic University of Pusan, Busan, Korea.

image. It is hard to select important coefficients for embedding watermark using the DCT. Further, the watermark embedded by the robustness of JPEG compression is easily loss because compression used the 8×8 block DCT. Besides, at this scheme, if it does block transformation, it could be happened the Block phenomenon. So it brings the loss of image.

This paper is organized as follows; we propose the watermarking scheme in section 3, the experimental result and conclusion at the final section.

II. ANN (Artificial Neural Network)

In usual, when the watermark is embedded in a certain image, it is important to decide the location where it is embedded. It is difficult to select the location that has robustness from the attack. The extract of this region is generally expressed to ROI (Region of Interest).

There are various algorithms in the ANN algorithm. In this paper, we apply the RBF algorithm among ANNs for ROI. Each algorithm has each application field. In general, when the purpose is to classify the cluster of the data in the characteristic similarity, the applications; ART, SOM and RBF, should be used in large. The RBF is proposed the ANN model by Broomhead and Lowe, and it's characteristics with comparison of MLP(Multi-Layer Perceptrons) is as follows[11].

a) An RBF network (in its most basic form) has a single hidden layer, whereas an MLP may have one or more hidden layers.
b) The computation nodes in the hidden layer of an RBF network are quite different and serve a different purpose form those in the output layer of the network whereas an MLP shares a common neuron model.
c) The hidden layer of an RBF network is nonlinear, whereas the output layer is linear but an MLP used as a classifier are usually all nonlinear.
d) The argument of the activation function of each hidden unit an RBF network computes the Euclidean norm between the input vector and the center of that unit, whereas an MLP computers the inner product of it.
e) MLPs construct global approximations to nonlinear input-output mapping whereas RBF networks using exponentially decaying localized nonlinearities construct local approximations to it.

We use the character of similar pattern node of the RBF to decide the location to embed the watermark. The RBF can select the location of node where users want to embed, so it has a strong point that the embedding location can be controlled by the character of the image. Nobody knows about the location of embedding watermark except of authorized user who has the trained data. If they processed same RBF, the trained data would different from the result of ours.

III. PROPOSED ALGORITHMS

A. Embedding Watermark

When the image data is transformed into frequency domain if it is communication channel, the watermark is that signal is transmitted by the communication channel. The signal should not be affected by noise, filtering, compression and transmission during the transmission. We use the signal of the watermark as gaussian normal distribution (1, 1): the average is 1, and variance is 1. Gaussian random vector is invisible when it is embedded and it's also stronger than the binary watermark [4].

We decompose the original image with the DWT to 3-levels of MRA. In most natural images, the energy is concentrated on the lower frequency domain that relates with human vision. If the image data damaged in the lower frequency domain, people could have noticed about it Accordingly, for protecting the quality of the image and making the watermarked image, we embed the watermark at the highest frequency domain where a little information of images is in. Using the DWT, embedding the watermark calculated the threshold to embed the watermark with equation 1 to calculate the threshold which decides to embed each sub-band.

$$T = 2^{\left[\log_2 MAX(Wavelet Coefficient)\right]} \tag{1}$$

It is the one of the image compression algorithm that Shapiro [12] proposed to calculate the threshold which used zero padding in the EZW (Embedded zerotree wavelet algorithm). EZW method is very efficient to encode important wavelet coefficient and express the energy concentration phenomenon by using the wavelet transform. It is to embed the watermark that used to calculate the first threshold. But, It is to embed the watermark which a several bigger wavelet coefficient using the maximum of sub-band. So, it couldn't express the characters of the image nor adjust the length of the watermark. If we adjust the hidden node, we will adjust the amount of the watermark in the same image. So we can say that it is strong for the image processing like compression or cropping.

In this paper, we classify wavelet coefficients of the highest sub-band (LH, HL and HH) using the RBF. In case of the SOM which is one of other competitive learning proposed by Kohonen, it sets the number of clusters in advance, so that it is influenced by the size of the image. For example, in the case of a test image, the number of wavelet coefficients in a cluster changes following to the change of image size. And that of Lena image which have big wavelet coefficients, the number of wavelet coefficients in a cluster is more than that of others. As so, before considering of the characteristics of image, we can't adjust the number of the watermark. We can say the RBF is adaptable to the image because it is not influenced by the size of the image. Disadvantage of competitive learning algorithm is different train data according to sequence of input data; it is different position to embed the watermark. And we could adjust the amount of watermark in the same image and could do that following the specialties of each image.

$$X_i' = X_i + \alpha W_i \tag{2}$$

$$X_i' = X_i\left(1 + \alpha W_i\right) \tag{3}$$

X_i' is a watermarked coefficient, X_i is a wavelet coefficient, and W_i is a watermark. When we embed watermark to the image to obtain the watermarked image using equation 2 and 3. Equation 2 is just adding the watermark, so it is not proper when the variation of the value has extreme differences.

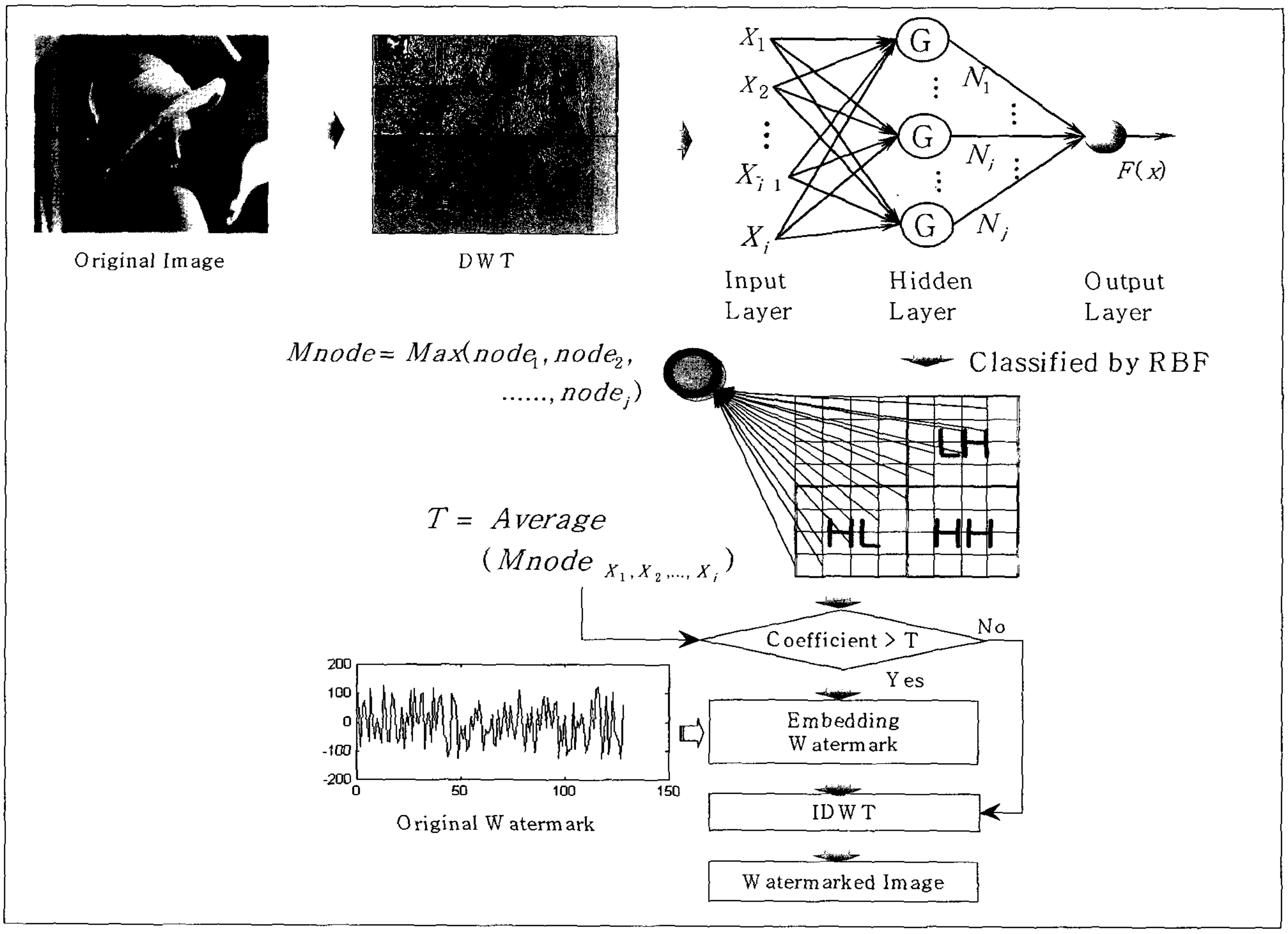


Fig. 1 Embedding watermark (X_i is a wavelet coefficient in the highest sub-band and N_j is a node)

In equation 3, the variation of a α (scaling parameter) affects largely the embedding watermark. As a result, we used equation 3, and α is 0.6, 0.8 and 1 according to variance of coefficients.

As we tested, we select the biggest node among the classified nodes. We set the average to threshold in the selected node and embed the watermark to the coefficient what is bigger than that of the average in those of the selected node in equation 4 and Fig. 1.

$$\begin{gathered}
Mnode = Max\left(node_1, node_2, \cdots, node_j\right) \\
T = Average\left(Mnode_{X_i}\right) \\
X_i' = \begin{cases} X_i\left(1 + \alpha W_i\right) & if\left(Mnode_{X_i} > T\right) \\ X_i & if\left(Mnode_{X_i} \le T\right) \end{cases}
\end{gathered} \tag{4}$$

B. Extracting Watermark

We decompose the watermarked image like the processing of embedding watermark to 3-level using the DWT. We calculated the train data which classified by using the RBF in the embedding processing. It is used to extract the watermark without original image. Information has a location and average of embedding the wavelet coefficients. Unauthorized users know about location of embedding the watermark, and the watermark will remove easily. So, in this paper, nobody knows about the location of embedding watermark using the RBF. Even the watermark is embedded using the RBF and the watermark verification process is in public, unauthorized users don't know about the information of the trained data. As a result, the algorithm is safer than others.

For evaluating similarity, there are some schemes. One is the way of calculating vector projection, other is the way of calculating correlation, other is the way of calculating bit error, and etc [4].

$$Correlation\left(X, X^*\right) = \frac{\Sigma XX^*}{\sqrt{\Sigma X^2 \Sigma X^{*2}}} \tag{5}$$

X is a original watermark, X^* is a extracted watermark. In this paper, we use the equation (5) for evaluating similarity between two vectors. If the similarity between the original watermark and the extracted watermark is higher than a threshold, we could assert the copyright.

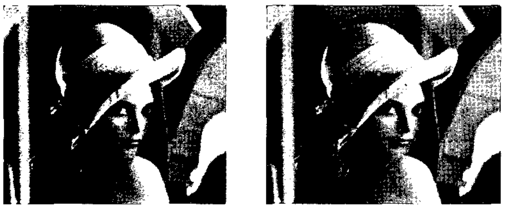
IV. EXPERIMENTAL RESULTS

In this paper, the proposed method is implemented by using Pentium 1.7 MHz, Window XP and Matlab 5.2. The size of the image is 256×256, and we test various images such as Lena image, Barbara image, Bridge image and Girl image, and etc. We use the watermark as the Gaussian normal distribution (1, 1).

We tested fidelity and robustness for the standard of the performance value. For the test of robustness, we did various filtering (Lowpass filter, Highpass filter, Wiener filter), adding noise, geometric transform (enlarge, reduction, cropping) and the attack of the compression of JPEG, and then we confirm robustness. In addition, for the higher confidence in the proposed algorithm, we test the image which is not embedded watermark by false positive error. We also are compared with other algorithms (Kundur, Wang, Xia, Cox and Kutter).

A. Similarity

We get PSNR to be decided objectively between the original image and the watermarked image, and we calculate fidelity through the equation 5 from the extracted watermark and the original watermark, the value of objective PSNR is maintained over 47dB in the Table 1.



(a) Original image (b) Watermarked image

Fig. 2 Similarity Test

Table 1 Similarity between orignal image and watermarked image

Image	PSNR	Image	PSNR
Lena	47.92	Camera man	47.92
Barbara	47.35	Crowd	46.57
Bridge	47.54	Oleh	46.85
Girl	47.75	Pepper	47.35

B. Robustness

We tested the watermarked image in Lowpass filer, Highpass filter, and Wiener filter. We used Highpass filter that the mask of the 3 x 3 size, [0 -1 0; -1 8 -1; 0 -1 0]/4, and Lowpass filter that the 3 x 3 size of the Gaussian filter, average is 0 and standard deviation is 0.5, and Wiener filter is the 3 x 3 size of the Wiener filter. Wiener filter is less similarity than other filters but it is not influenced to extract the watermark. We tested the watermarked imaged about geometric transform (rescaled a twice enlarged the watermarked image, rescaled a twice reduced the watermarked image, and the 156×156 size of the center cropping). The result is powerful efficiency in the geometric transform and adding noise of Salt & Pepper and Gaussian.

Table 2 Correlation between the original watermark and the extracted watermark

Image	Low pass filter	High pass Filter	Wiener filter
Lena	0.99	0.98	0.70
Barbara	0.99	0.97	0.75
Bridge	0.99	0.99	0.76
Girl	0.98	0.99	0.75

Image	Rescaled enlarge	Center cropping	S&P noise
Lena	0.98	0.88	0.86
Barbara	0.97	0.84	0.86
Bridge	0.99	0.82	0.89
Girl	0.98	0.92	0.83

But, it doesn't matter to decide the existence of watermark because the similarity is over than detection values. However, it is not influence to extract watermark. Compare with Kundur's algorithm which doesn't need the original image, the process get better result in figure 5.

Even though the efficiency of the process is weaker than other algorithms which needed the original image but it is not influence to extract the watermark. In this paper, without the original image, so the process is better than other blind watermarking in comparison. Furthermore, compare with Cox in the same the DCT situation, it can't be extracted under JPEG 10%, the watermark is extracted in the process even the value is low.

The image that is not embedded the watermark is experimented in false positive error. The watermarking algorithm can't be reliable, if the watermark is extracted in false positive error. In this paper, the watermark isn't extracted from the image that not embedded the watermark.

V. CONCLUSIONS

In this paper, we proposed the watermarking considering of human vision character and embedded the watermark in the highest sub-band that has fewer amounts of image data in visual. The process used the wavelet transform by using the RBF. The process considers the character of the image that is adaptive watermarking. Using the clustering data that is used in embedding, the watermark is extracted without the original image. The proposed method was applied not to the whole wavelet coefficients, but to only the wavelet coefficients in the selected node to reduce the time cost. The algorithm is much stronger than the others because unauthorized users can't know the result of training by the RBF.

In the result, the value of objective PSNR is maintained over 47dB, and there is not to significant visual difference in subjective observation. And the proposed algorithm is much efficient than other algorithms.

REFERENCES

[1] M. D. Swanson, M. Kobayashi, and A. TewFik, "Multimedia Data-Embedding and Watermarking Technologies," *In Proceeding of IEEE*, Vol. 86, No. 6, June 1998.

[2] I. Pitas and T. Kaskalis, "Applying Signatures on Digital Images," *In Proceeding of IEEE Nonlear Signal Processing Workshop*, Thessaloniki, Greece, 1995.

[3] C. F. Osborne, R. G. Schyndel and A. Z. Tirkel, "A Digital Watermarking," *International Conference on Image Processing*, November 1994.

[4] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, 1997.

[5] I. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, *Academic Press*, 2002.

[6] M. Kutter, F. Jordan, and F. Bossen, "Digital Signature of Color images using Amplitude Modulation," In Ishwar K. Sethi, editor, *Proceedings of the SPIE Conference on Storage and Retrieval for Image and Video Databases*, Vol. 2952, pp. 518 - 526, San Jose, USA, 1997.

[7] D. Kundur and D. Hatzinakos, "Digital watermarking using Multiresolution Wavelet Decomposition," *In Proceeding of IEEE ICASSP '98*, Vol. 5, pp. 2969 - 2972, Seattle, WA, USA, May 1998.

[8] H. J. Wang, P. C. Su and C. J. Kuo, "Wavelet-based digital image watermarking," *Optics Express 3,* pp. 497, December 1998.

[9] X. G. Xia, C. G. Boncelet and G. R. Arce, "Wavelet Transform based Watermark for Digital Images," *Optics Express 3*, pp. 497, December 1998.

[10] S. Mallat, "Multi-Frequency Channel Decom-position of Images Wavelets Models," *IEEE Trans. on Information Theory,* Vol. 11, No. 7, July 1992.

[11] S. Haykin, Neural Networks: A Comprehensive Foundation, *MacMillan*, 1994.

[12] J. M. Shapiro, "Embedded Image coding using zerotrees of wavelet coefficients," *IEEE Transaction on Signal Processing*, Vol. 41, No. 12, pp. 3445-3462, December 1993.

[13] M. Kutter, "http://www.watermarkingworld.org/," *WatermarkingWorld*, 2000.

[14] T. Kohonen, "Self-Organizing Maps," Berlin: *Springer-Verlag*. First edition was 1995, second edition 1997.

[15] K. I. Diamantaras, and S. Y. Kung, Principal Component Neural Networks, Theory and Applications, *NY: Wiley*, 1996.

[16] R. C. Gonzalez, R. E. Woods, Digital image processing, Second edition, *Prentice Hall*, 2001.

[17] Darpa, Neural Network Study, *AFCEA International Press*, 1988.

Jae-Hyun Cho

Received the B.S. degrees in Dept. of Computer Science from Pusan National Univ., Busan, Korea, in 1986 and the M.S. degrees in Dept. of Computer Science from Soongsil Univ., Seoul, Korea, in 1989, and the Ph.D. degrees in Dept. of Computer Science from Pusan National Univ., Busan, Korea, in 1998, respectively. Since 2001, he has been with School of Computer Information Engineering at Catholic Univ. of Pusan, Korea as an Associate Professor. His research interests include Neural Networks, Image Processing and Human Visual System.