The Multi-Image Copyright-Protection Scheme Based on Neural Network

Chun-Hua Chen[1&2] and Chao-Hsing Hsu[2]
[1] *Institute of Computer Science, National Chung-Hsing University*
250, Kuo Kuang Road, Taichung, 402, Taiwan, R.O.C.
[2]*Department of Electronic Engineering, Chienkuo Technology University*
Changhua 500, Taiwan, R. O. C.
Mail: godsons@ckit.edu.tw

Abstract-*Through the rapid development of computer technology and the popularity of Internet, more and more information is delivered through digital way. Because the digital information has the property of easy copy and rapid delivery, any one can distribute and obtain digital information easily. So, the copyright protection of valuable digital (included digital images) becomes an increasingly important research topic.*

In this paper, we proposed a multi-image copyright-protection scheme based on neural network. Through the use of Neural Network which has the capacity of learning, we can use the multiple original digital images as the input and the copyright pattern as the output. The neural network can learn the relationship between them. Then, some image which is needed to be verified can be as the input of the learned neural network and the output will show the copyright pattern if the image is legal.

Our experiments show that this copyright-protection scheme has robustness. It can resist many different attacks of images, it still output the clear copyright pattern to verify copyright in such conditions. In addition, our scheme does not hide digital watermark (copyright pattern) in the original images actually, so our scheme will not cause the loss of the original images. Finally, our scheme can processes multiple images at a time, it cut down the cost of registration.

Keywords: Neural Network, Digital Watermark, Discrete Wavelet Transform

1. Introduction

The general way to protect copyright of image is the digital watermark. The digital watermark is more and more important in recent years. Many scholars are devoted to the research of digital watermark and the research results are growing rapidly. The digital watermark is the technique which embeds copyright information (like trademark, serial number, logo, seal...) into protected digital media. The purpose of this technique is to forbid the illegal copy, illegal use and illegal distribution of the protected digital images. In general, the watermarking techniques can be classified into two classes. The first is the spatial domain technique and the second is the frequency domain technique. The methods of the first technique are to change the values of the pixels directly for embedding watermark. The advantage of first technique is simple and its efficiency is good. But the disadvantage of first technique is difficult to resist the process or the attack of the images. The methods of the second technique are to transfer the image into frequency domain and then to embed watermark into the image. And then transfer the image which is embedded watermark back into spatial domain. For example, Discrete Cosine Transform (DCT) [1,2] and Discrete Wavelet Transform (DWT) [3-5] belong to the second technique. The second technique can resist the process or the attack of the image more than the first technique. For the purpose of the copyright-protection of digital images, the good watermarking technique should satisfy transparency, robustness, unambiguous, security and blindness [1-5].

Hsu and Wu [1, 3] proposed individually Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) watermarking technique to embed watermark into the low frequency coefficients of DCT or DWT. From the experiments, we can realize that the two methods mentioned above can resist JPEG compression and cropping of the image. But these two methods do not cover other attacks of the image.

Chin-Chen Chang et al. proposed another new technique [4]. First, this new technique randomly permutes the original image and then splits the original image into blocks. Second, it compares the variances of pixels of every block to decide one binary pattern. The last, it take this binary pattern to do a XOR($\oplus$) operation with binary watermark. The result of the XOR operation is the secret key to extract watermark of the original image later. The advantages of

this new technique are no losing of the original image and no needing of the original image when it extract watermark later. Because this new technique do not embed watermark into the image actually, we call it "No Loss Copyright-Protection Scheme". Chin-Chen Chang et al. recently proposed two new techniques [6, 11] of "No Loss Copyright-Protection Scheme".

In this paper, we adopt the essence of the "No Loss Copyright-Protection Scheme". Our Scheme do not embed watermark (copyright pattern) into the image actually. First, it use the Discrete Wavelet Transform (DWT) to catch the characteristic value of the protected image. Second, it use the capacity of learning and adapting of the BPN(Back Propagation Network) neural network [10] to learn the relationship between the protected image and watermark (copyright pattern). So, it can extract the copyright pattern later. Because our scheme do not embed copyright pattern into the image actually, it will not cause a loss of the protected image. It conquers the problem of image loss. So, our scheme is suitable for the high quality images (e.g. Medical images) and carton images which are hard to embed watermark. By the way, in the results of our experiments we verify that our scheme can extract copyright pattern more correct than the scheme in [4]. Finally, our scheme can handle multiple images one time, so it outperforms than the schemes used in [7, 8].

2. Neural Network and Back-Propagation Network (BPN)

Neural Network is a model developed by the research of men's mental and activities of brain. From the network framework point of view, it is composed by many simple connected neurons. From the network function point of view, it is a new method of information process and calculation inspired by biology model. The below figure is the computation model of single neuron.

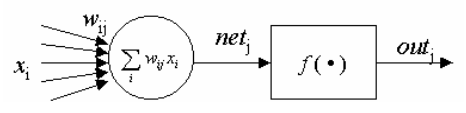

Fig 1 Computation model of neuron

The process of Neural Network can be divided into two phases. The first phase is a learning phase and the second phase is a retrieving phase. In a learning phase, the major work of Neural Network is to decide parameters of system (e.g. W_{ij}: value of link) by training data. In a retrieving phase, the work of Neural Network is to produce corresponding result by testing data.

In the experiments of this paper, we choose Back-Propagation Network (BPN) as the network type of Neural Network. Back-Propagation Network is the most typical network model of Neural Network. It is a supervised learning network which the learning rule of it is based on MSE (min square error) and it use the gradient steepest descent's method to minimize error function. Back-Propagation Network adopts non-linear transformation function, so the values of it's output are continuous values. The learning of Back-Propagation Network can be divided into two passes: the forward pass and the backward pass. The forward pass begins with input layer, it forward and calculate the output values of neurons layer by layer. The backward pass begins with output layer, it backward (layer by layer) the error of previous layer and revise the values of links. This is why this type of neural network is called Back-Propagation Network. The Fig 2 below is Back-Propagation Network with one hidden layer. The left four neurons is the input layer, the middle three neurons is the hidden layer and the right four neurons is the output layer.

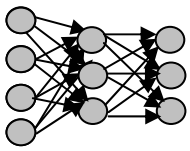

Fig 2 The Back-Propagation Network with one hidden layer

We choose the *S* type function as the transformation function. The *S* type function and it's derivatives are the following:

$$f(net) = \frac{1}{1 + e^{-net}}$$

$$f'(net) = net\ (1 - net)$$

The algorithm of Back-Propagation Network is as below[10]：

(1) Set the parameters of the network and random initial values of the links.

(2) Input the training pairs: input vector X and target output vector T.

(3) Calculate the input net value from input layer to hidden layer.

$$net_j^h = \sum_i w_{ij}^h x_i$$

(4) Calculate the output net value of neuron j of hidden layer.

$$H_j = f(net_j^h)$$

(5) Calculate the input net value of neuron k of output layer.

$$net_k^o = \sum_j w_{jk}^o H_j$$

(6) Calculate the practical output values of

neural network.

$O_k = f(net_k^o)$

(7) Calculate the errors of output layer.

$\delta_k^o = (T_k - O_k) f'(net_k^o) = (T_k - O_k) O_k (1 - O_k)$

(8) Calculate the errors of hidden layer.

$\delta_j^h = f'(net_j^h) \sum_k \delta_k^o w_{jk}^o = H_j (1 - H_j) \sum_k \delta_k^o w_{jk}^o$

(9) Update the values of links of output layer (η is the learning rate chosen by us).

$w_{jk}^o = w_{jk}^o + \eta \, \delta_k^o \, H_j$

(10) Update the values of links of hidden layer.

$w_{ij}^h = w_{ij}^h + \eta \, \delta_j^h \, x_i$

(11) Calculate the error (mean square error).

$E = \frac{1}{2} \sum_k (T_k - O_k)^2$

(12) Repeat step 2 to step 11 until the convergence of neural network

3. The Multi-Image Copyright-Protection Scheme

The multi-image copyright-protection scheme proposed in this paper can be split into two phase. In the phase I, we do two jobs. First, we catch the characteristic values of the protected images and the attacked images of protected images by Discrete Wavelet Transform (DWT), see Fig 3. Second, we use the characteristic values of images as the input and copyright patterns as the output, so that the neural network can learn the relationship between them. In the phase II, we take some image (for verifying the copyright) as the input of learned neural network in Phase I. If the output of the neural network is clear copyright pattern, then we can judge the copyright of the image.

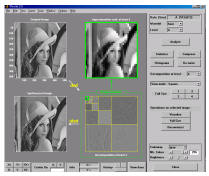

Fig 3 The Lena original image and DWT of it

Detail and statements of our schema are as below:

3.1 Phase I ：Preprocessing and Learning

We suppose protected images are 256 × 256 gray level images (8 bits per pixel) and copyright pattern is a 32 × 32 binary image (8 bits per pixel).

Step 1: Input multiple images which are desired to protect.

Step 2: Transfer protected images (including the attacked images of protected images) through four times DWT transformations.

Step3: Learning the relationships between protected images and the copyright pattern by BPN network.

Step 4: Saving the network parameters and the values of links.

Step 5: Registration copyright of the protected images (by transformation the values obtained in step 4) on some certification center.

3.2 Phase II ： Verifying Copyright of Some Image

Step 1: Input some image X which is planed to verify and suppose the copyright pattern is W.

Step 2: Transfer the image through four times DWT transformations.

Step 3: Input the result of step 2 to the learned neural network obtained by Phase I and Obtain the result W'.

Step 4: To judge the copyright of the image.

If the image X is the protected image, then the image W' will be the same as copyright pattern W and if the image X is some attacked image on protected image then the image W' will be very similar to copyright pattern W. But if the image X is not the protected image, then the image W' will be not similar to copyright pattern W.

4. Experiments and Discussions

To verify the robustness of our copyright protection scheme, we do some experiments described below. In our experiments, we use a PC Intel 586(RAM 1GB) for simulating platform, and C++ 5.0 for writing interface program and MATLAB 6.5 as the neural network simulating tool. In the first group of experiments, we choose gray level image Lena (Fig 4), Airplane (Fig 5) and Tower (Fig 6) as our protected images and a Qoo (Fig 7) graph as the copyright pattern. In the second group of experiments, we choose gray level image Airplane (Fig 5) and Tower (Fig 6) as our protected images and a seal graph (Fig 8: Chinese words that mean the name of our department and our school) as our copyright pattern. The size of above protected images is 512 × 512 and the size of copyright pattern is 32 × 32. We use the PSNR value as evaluating standard of image quality of test image. The definition of PSNR value is as below:

$$PSNR = 10 \log_{10} \frac{E_{\max}^2 \times H_X \times W_X}{\sum [x_{ij} - x_{ij}']^2}$$

The E_{max} is the maximum of every pixel in the test image. For example, the E_{max} is 255 in gray level image. The x_{ij} represents the coefficient of the pixel on (i,j) position of the original image and x'_{ij} represents the coefficient of the pixel on (i,j) position of attacked image of original image. If the value of PSNR is bigger, then the similarity of these two images is higher. And if the value of PSNR is bigger then 30dB, the loss of the image is not aware by human's vision.

Fig 4 Original Image I : Lena

Fig 5 Original Image Ⅱ: Airplane

Fig 6 Original Image Ⅲ: Tower

Fig 7 The first copyright pattern

Fig 8 The second copyright pattern

For the quality measurement of extracted copyright pattern through Phase II, we use Bit Correct Ratio (BCR). The definition of BCR is as below.

$$BCR = \frac{\sum_{i=1}^{W_H}\sum_{j=1}^{W_w}\overline{w(i,j)\oplus w'(i,j)}}{W_H \times W_w}\times 100\%$$

The w(i,j) is represented the coefficient on (i,j) position of original copyright pattern and the w'(i,j) is represented the coefficient on (i,j) position of extracted copyright pattern. The sign $\oplus$ is represented the XOR operation. If the BCR value is closer to 1 (100%), the quality of the extracted copyright pattern is better.

4.1 The first group of experiments

We use the protected images Lena, Airplane and Tower as input training groups of neural network (the copyright pattern Qoo as output).

Protected Images — Lena, Airplane and Tower

Image JPEG Compression — ratios of compression are 10%, 30%, 50%, 70% (Lena10, Airp30, Tower50, Lena70…)

Image Blurring — blurring the images (Lena_hblur, Airp_hblu, Tower_hblu)

Image Noising — adding noise to images (Lena_noise, Airp_ noise, Tower_ noise…) Lena_mnoise represents adding more noise to the Lena image…

Image Scaling — shrinking the images to 1/2 or 1/4 size and then enlarge to original size (Lena_scale2, Lena_scale4, Airp_scale2 …)

The results of the first group of experiments are shown by Fig 9 and Table 1 bellow.

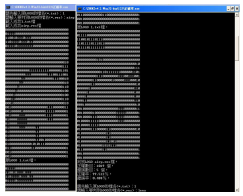

Fig 9 The example of verifying phase
(The left side of Fig 9 is the original copyright pattern, the right side of Fig 9 is the copyright pattern extracted form the verified image. The BCR value is 99.5%)

Table 1 The result of using three original images and 27 testing images for verifying

Testing images	PSNR	BCR (Bit Correct Ratio)	Have learning ?
Lena	Original Ⅰ	90.527 %	Yes
Lena10	31.17	91.797 %	No
Lena30	35.71	90.039 %	No
Lena50	37.55	92.383 %	No
Lena70	39.32	91.699 %	No
Lena_hblur	33.97	90.430 %	No
Lena_mnoise	16.62	87.793 %	No
Lena_noise	22.68	90.430 %	No
Lena_scale2	36.93	89.453 %	No
Lena_scale4	29.85	89.453 %	No
Airp	Original Ⅱ	99.512 %	Yes
Airp10	30.38	99.512 %	No
Airp30	34.89	99.512 %	No
Airp50	36.78	99.512 %	No
Airp70	38.58	99.512 %	No
Airp_hblu	31.99	99.512 %	No
Airp_mnoise	16.80	99.414 %	No
Airp_noise	22.77	99.512 %	No
Airp_scale2	32.91	99.512 %	No
Airp_scale4	27.63	99.512 %	No

Table 1 continue

Testing images	PSNR	BCR (Bit Correct Ratio)	Have learning ?
Tower	Original III	92.090 %	Yes
Tower10	28.85	91.113 %	No
Tower30	32.58	91.895 %	No
Tower50	34.57	91.895 %	No
Tower70	36.81	91.797 %	No
Tower_hblu	10.36	94.141 %	No
Tower_mnoise	17.09	90.625 %	No
Tower_noise	22.74	91.699 %	No
Tower_scale2	29.48	91.602 %	No
Tower_scale4	25.43	91.309 %	No

4.2 The second group of experiments

We use protected images Airplane and Tower as input training groups of neural network (the copyright pattern Fig8 as output).

The results of the second group of experiments are shown by Fig 10 and Table 2 bellow.

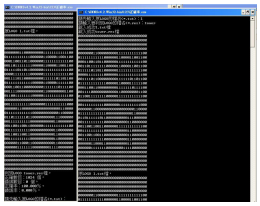

Fig 10 The example of verifying phase
(The left side of Fig 10 is the original copyright pattern, the right side of Fig 10 is the copyright pattern extracted form the verified image. The BCR value is 100%)

Table 2 The result of using two original images and 18 testing images for verifying (table can be seen in right upper side)

Testing images	PSNR	BCR (Bit Correct Ratio)	Have learning ?
Airp	Original II	89.648 %	Yes
Airp10	30.38	90.527 %	No
Airp30	34.89	90.625 %	No
Airp50	36.78	89.551 %	No
Airp70	38.58	90.039 %	No
Airp_hblu	31.99	89.648 %	No
Airp_mnoise	16.80	88.867 %	No
Airp_noise	22.77	88.770 %	No
Airp_scale2	32.91	90.723 %	No
Airp_scale4	27.63	90.527 %	No
Tower	Original III	100 %	Yes
Tower10	28.85	100 %	No
Tower30	32.58	100 %	No
Tower50	34.57	100 %	No
Tower70	36.81	100 %	No
Tower_hblu	10.36	92.578 %	No
Tower_mnoise	17.09	100 %	No
Tower_noise	22.74	100 %	No
Tower_scale2	29.48	100 %	No
Tower_scale4	25.43	100 %	No

4.3 Discussion

From the above two group of experiments, we can know that many test images (image processed from original image) can still be extracted clear copyright pattern. So, the multi-image copyright-protection scheme proposed in this paper is robust. Now we consider another condition, if we choose some image which is not registered before as a test input, will the scheme output some copyright pattern? To know the answer of the question, we take an image boat (see Fig 11) for the test. In this test, our scheme can not produce any clear copyright pattern.

Fig11 Some image (boat) not registered

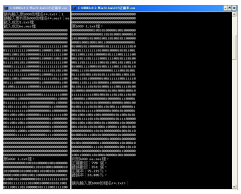

Fig 12 The result of Fig 11 as an input
(The left side of Fig 12 is the original copyright pattern, the right side of Fig 12 is the copyright pattern extracted form the verified image – boat. We can not see clear copyright pattern in the right side.)

Maybe readers still have a question. If some one stole the images of a company, and used the scheme proposed by this paper to set up the learning capability and verifying capability of these images. Then, how the judiciary decides who owns the images when there is a dispute of copyright. For solving this problem, Voyatz and Pitas[9] proposed the idea that to solve thoroughly the copyright protection problem of digital images, we must get the help from the trusted third party (e.g. certification center). So,

we add the step 5 in phase I for registration image copyright on some certification center. S. Katzenbeisser proposed another solution [12] for this problem, he suggest the use of public key technique. Through the encryption, no one else can steal the images and the copyrights of the images. Finally, we compare the scheme proposed in this paper to other related schemes.

Table 3 The comparisons between schemes of image copyright protection

	Robustness	Having loss ?	Number of images processed
Schemes in [1, 3]	good	Yes	one
Schemes in [4, 6]	excellent	No	one
Schemes in [7, 8]	excellent	No	one
Scheme in this paper	excellent	No	multiple

5. Conclusions

In the results of our experiments, we verify that our scheme can resist many classes of attacks (or processes). Our scheme can extract the copyright pattern of high Bit Correct Ratio (BCR) in our experiments. And it will not extract the copyright patterns form the images which do not register in advance (see experiment result in Fig. 12). Because our scheme do not embed copyright pattern into the image actually, it will not cause a loss of the protected image. Finally, this scheme can process multiple images at one time, so it can reduce the cost of registration on some certification center.

Reference

[1] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing*, vol. 8, no. 1, pp. 58-68, Jan., 1999.

[2] Min-Shiang Hwang, Chin-Chen Chang, Kuo-Feng Hwang, "Digital Watermarking of Images Using Neural Networks," *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548-555, Jan., 2000.

[3] Chiou-Ting Hsu and Ja-Ling Wu, "Multiresolution Watermarking for Digital Images," *IEEE Transactions on Circuits and System-II: Analog and Digital Signal Processing*, vol. 45, no. 8, pp. 1097-1101, August, 1998.

[4] Chin-Chen Chang, Kuo-Feng Hwang and Min-Shiang Hwang, "A block based digital watermarks for copy protection of images," in *Fifth Asia-Pacific Conference On Communications /Fourth Optoelectronics And Communications Conference*, Beijing, China, October 1999.

[5] M.J. Tsai, K.Y. Yu, and Y.Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking," *IEEE Transactions on Consumer Electronics*, vol. 46, no.1, pp. 241-245, Feb., 2000.

[6] C.C. Chang, K.F. Hwang, and M.S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics," *IEE Proceedings-Vision Image and Signal Processing*, vol. 149, no. 1, pp. 43-50, Feb., 2002.

[7] Gwoboa Horng, Chun-Hua Chen, Bean-Cheng Tzeng, Tzung-Her Chen, "A Robust and losses Copyright-Protection Scheme Based on Neural Network", *Proceedings of the 7th Conference on Artificial Intelligence and Applications (TAAI2002)*, Wufon, Taiwan, pp. 579~584, Nov., 2002.

[8] Gwen-Hua Chen , Gwoboa Horng, Tzung-Her Chen, "A Robust Copyright-Protection (Digital Watermark) Scheme Based on Neural Network," *SCI 2003 Proceedings* , Orlando, USA, vol. 15, pp. 345-349, July, 2003.

[9] G. Voyatzis and I. Pitas, "Protecting Digital-Image Copyrights: A Framework," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 18-24, Jan.-Feb., 1999.

[10] Jeng-Hung Chou, "Neural network — Theory and Implement", Sung Gang Book Corporation, Taiwan, 1996.

[11] C.C. Chang, and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognition Letters*, vol. 23, no. 8, pp. 931-941, June, 2002.

[12] S. Katzenbeisser, "On the Design of Copyright Protection Protocols for Multimedia Distribution Using Symmetric and Public-Key Watermarking," in *12th International Workshop on Database and Expert systems Applications, Fifth International Query Processing and Multimedia Issues in Distributed Systems Workshop, IEEE Computer Society Press*, pp. 815-819, Sept., 2001.