ISSN 2186-5647

Adaptive Digital Watermarking using Fuzzy Inference System and Human Visual System

China University of Technology ○Yin, Te-Lung

1. Introduction

Today, the use of the Internet has grown rapidly. However, transmitting information on computer networks is not safe and the valuable data is easy to be stolen. So, it is the reason why information security is an important issue now in our world. The research of digital watermarking becomes an interesting topic consequently and one of its applications is the copyright protection.

Transform-domain methods such as the Fourier transform, discrete cosine transform, or wavelet transform are based on spatial transformation, and process the coefficients in the frequency domain for hiding data [3]. The secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency portion is more likely to be suppressed by compression. How to select the best frequency portions of the image for watermark is another important and difficult topic. After the inverse transformation, the hidden data will be scattered around the spatial image. Thus, the transform-domain method is more robust than the spatial-domain method against compression, cropping and jittering. The robustness is maintained at the price of imperceptibility in the transform-domain. To avoid distortion of the image quality and increase the survival of watermark, there are many requirements for a well-designed watermark. The requirements for watermarking scheme are described as follows.

● *Imperceptibility*

The host image or original image should not be visibly degraded by the watermark. In other words, we must ensure that an unauthorized user does not perceive the existence of the watermark. Imperceptibility ensures the excellent perceptual quality of the protected image.

● *Robustness*

The hidden watermark must survive image processing or operations such as clipping, filtering, enhancement, and so on. The watermark should be retrievable by lossy compression techniques such as JPEG, which is used for transmission and storage. It also must against the malicious attack that denotes the manipulation of destroying or removing the watermark.

● *Capacity*

In watermark, trade-offs exist between the capacity and the degree of immunity of the original image from modification. By constraining the cover image degradation, a watermarking scheme can operate with either high capacity or high resistance to modification .

In this paper, we use the Human Visual System (HVS) model and lead in the fuzzy inference system (FIS, shown as Fig. 1) for adapting the watermark strength to each image. This provides a maximum power subject to the imperceptibility constraint.

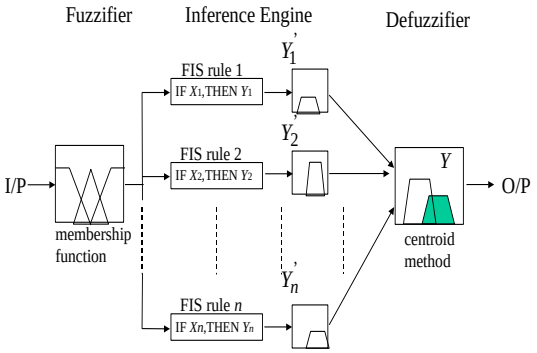

Fig. 1. Fuzzy inference system (FIS).

In the HVS, there are two properties: (1) luminance sensitivity: the brighter the background is, the larger the embedded signal could be, and (2) frequency sensitivity: the higher the frequency is,

the larger the embedded signal could be. We use the DC coefficient in the DCT of an image as luminance sensitivity. The frequency sensitivity is estimated by quantizing the DCT coefficients of an image using the JPEG quantization table. Then, we compute the number of non-zero coefficients as the frequency sensitivity.

Our FIS can take account of human knowledge in HVS. The human visual perception of luminance and frequency can be represented by a number of fuzzy-set values. From these fuzzy representations, the FIS characterizes the function of how to control the transparency. That depends on the transform of image sensitivity to fuzzy associations.

2 Watermark embedding

The watermark is a sequences of random number that length is *n* and have the normal distribution *N*(0,1), i.e., $W = \{w_i, 0 \le i < n\}$. Three random numbers of the watermark sequences are embedded in low frequency coefficients of each block.

The watermark embedding process is given in Fig. 2. The original image is decomposed into non-overlapping 8x8 blocks, and the DCT is performed for every block. Then, the luminance sensitivity and frequency sensitivity are computed as the input of FIS. The transform function between sensitivity and membership is sigmoid function. Consider a fuzzy association for intelligent inference of an adaptive watermark.

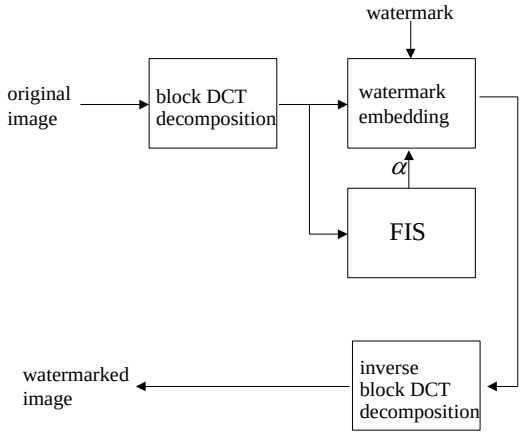

Fig. 2. Watermark embedding process.

The FIS rules fo basic knowledge are:

Rule1: If the image is dark and smooth, then keep the amount of embedding information small.

Rule2: If the image is dark and texture, then keep the amount of embedding information moderate.

Rule3: If the image is bright and smooth, then keep the amount of embedding information moderate.

Rule4: If the image is bright and texture, then keep the amount of embedding information large.

Let:

x: the luminance sensitivity in fuzzy set; membership of *L*, $\mu(L)$.

y: the frequency sensitivity in fuzzy set; membership of *F*, $\mu(F)$.

z: the inference result.

A_1 : "DARK" in the fuzzy set.

A_2 : "BRIGHT" in the fuzzy set.

B_1 : "SMOOTH" in the fuzzy set.

B_2 : "ROUGH" in the fuzzy set.

C_1 : "SMALL" in the fuzzy set.

C_2 : "MODERATE" in the fuzzy set.

C_3 : "LARGE" in the fuzzy set.

Then the basic HVS knowledge can be described as IF-THEN rules in the inference system as follows:

INPUT: x is A' AND y is B'

R^1: IF *x* is A_1 AND *y* is B_1,
THEN *z* is C_1.

R^2: IF *x* is A_1 AND *y* is B_2,
THEN *z* is C_2.

R^3: IF *x* is A_2 AND *y* is B_1,
THEN *z* is C_2.

R^4: IF *x* is A_2 AND *y* is B_2,
THEN *z* is C_3.

CONCLUSION: *z* is C'.

We use the centroid method to defuzzify the inference results in the defuzzifier process. The output α_k's of FIS is used to as the weights of the watermark.

3. Watermark detection

The watermark detection process is given in Fig. 3. The weights α_k's are again computed from the original image by convolving the same FIS as that used in the watermark embedding process. Then, the original image and corrupted images are transformed using the DCT. The embedded coefficients are subtracted and divided by the weights α_k's to extract the corrupted watermark. The watermark detection process

can be described as:

$$D_k = X_k - X_k^*, \quad (1)$$

$$w^* = \bigcup_k (D_k / \alpha_k), \quad (2)$$

where the X_k^* is the DCT coefficients in block k of the corrupted image and the w^* is the corrupted watermark that formed by combining with all k blocks' sub-watermarks.

The watermark detection is performed by computing the correlation between w^* and w as:

$$\rho = \frac{w^* \cdot w}{\sqrt{w \cdot w}}, \quad (3)$$

where ρ is a correlation measurement. If the measurement is larger than a threshold, it means that the corrupted watermark is correct.

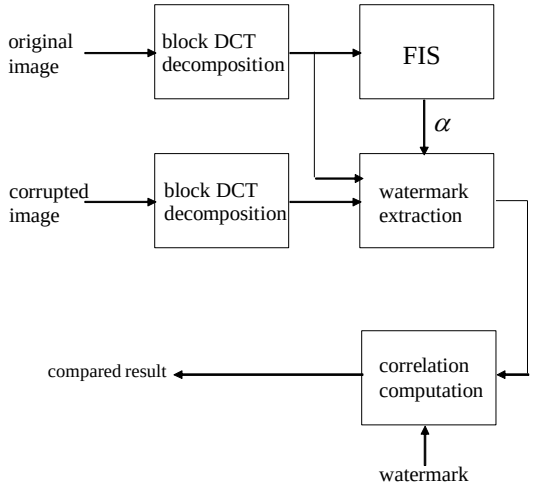

Fig. 3. Watermark detection process.

4. Experimental results

The above watermarking scheme has been tested on the image Lena as Fig. 4. The watermark is a random number sequences that length is 1000. Fig. 5 show the adaptive weights corresponding to the blocks in the original image. In Fig. 5, it is generated by our method that is smoother. The watermarked image is shown as Fig. 6 and the image transparency is not affected. We generate 1000 test watermarks and the 500th is the correct watermark. The response due to the correct watermark is much stronger than that of incorrect watermarks as shown in Fig. 8. The image quality in our watermarked image is better. Then, compress the watermarked images in different quality factor. The lower quality factor value corresponds to greater compression. The detector responses in our method are still good. In the above experiments, the embedding watermark defenses the distortion, so it is robust.

Fig. 4. Original image of size 2565256,

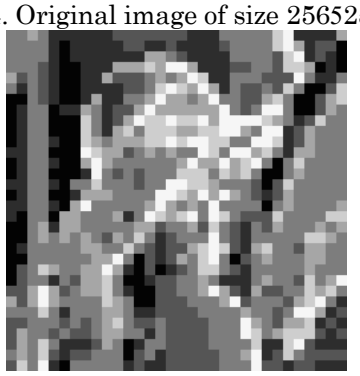

Fig. 5. Perceptual parameters of our method

Fig. 6. The watermarked image.

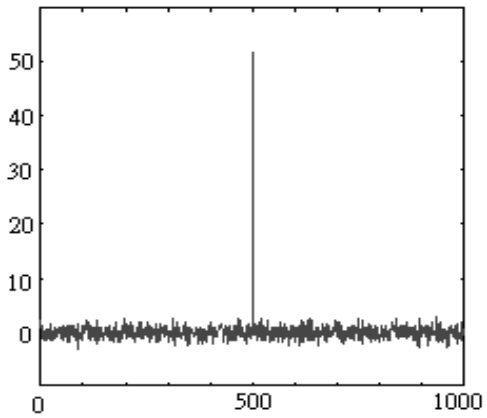

Fig. 7. Watermark detector response.

5. Conclusions

In this paper, an adaptive watermarking

scheme based on the human visual model and the fuzzy inference system is proposed. By using the human visual model, the watermark can be adapted to different images that provide a maximum and suitable power watermark subject to the imperceptibility constraint.

The main contributions of our adaptive watermark scheme are that it provides the advantage of fuzzy logic inference that extracts the human's intelligence. And it applies the adjustment of watermark strength smoother and more compatible to the variation of human visual model. The capacity of the watermark can be larger, and it is hence more robust and imperceptible.

References

1) I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

2) J. Huang and Y. Q. Shi, "Adaptive image watermarking scheme based on visual masking," IEE Electronics Letters, vol. 34, no. 8, pp. 748-750, Apr. 1998.

3) C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," IEEE Journal on Selected Areas in Communications, vol.16, no. 4, pp. 525-539, May 1998.