中正嶺學報 第三十二卷 第二期 民國 93.5.
JOURNAL OF C.C.I.T., VOL.32, NO.2, MAY, 2004

短文 Short Note

Robust Digital Watermarking Using Fuzzy Inference Technique

Der-Chyuan Lou, Te-Lung Yin, and Ming-Chang Chang

Department of Electrical Engineering
Chung Cheng Institute of Technolog
National Defense University
Tahsi, Taoyuan, Taiwan
e-mail: dclou@ccit.edu.tw

ABSTRACT

Digital watermarking has been proposed for copyright protection in our digital society. In this paper, a digital watermarking scheme based upon human visual mask and fuzzy logic technique is proposed. Fuzzy logic approach is employed to obtain the different strengths of watermark by the local characters of image like brightness sensitivity and frequency sensitivity in our proposed method. In our experiments, this scheme provides a more robust and transparent watermarks.

***Keywords**:* watermark, copyright protection, fuzzy inference system

模糊推論技術應用於強韌數位浮水印之研究

婁德權　尹德龍　張明昌

國防大學中正理工學院電機工程學系

摘　　要

在網際網路逐漸普及應用，數位資料的傳遞變得簡單快速，因此保護資料安全日益重要。數位浮水印技術，是在媒體資訊之中隱藏一段著作權資訊，用來證明該媒體之合法權益，以避免在未被授權的情況下，電子文件被非法任意散佈及盜用。本論文結合模糊理論與人類視覺模式，應用在影像數位浮水印技術上。其目的在建構兼俱強固性與透明性的影像數位浮水印技術，藉此解決影像數位浮水印之問題。

關鍵字：數位浮水印、著作權保護、模糊推論系統

文稿收件日期 90.2.12; 文稿修正後以短文接受日期 93.1.9.
Manuscript received Feb. 12, 2001; revised as short paper Jan. 9, 2004.

I. INTRODUCTION

Today, the use of the Internet has grown rapidly. However, transmitting information on computer networks is not safe and the valuable data are easy to be stolen. So, it is the reason why information security is an important issue now in our world. There are many applications about multimedia protections such as secret information delivery [1, 2], secret image store [3], image authentication [4, 5] and watermarking [6-21]. The research of digital watermarking becomes an interesting topic consequently and one of its applications is the copyright protection. Digital watermark strategies fall into two major categories: spatial-domain and transform-domain techniques.

Many techniques have been proposed in the spatial-domain, such as the LSB (least significant bit) insertion method [19, 22], the patchwork method, and the texture block coding method [23]. The spatial-domain technique processes the location and luminance of the image pixel directly. The LSB insertion method hides the watermark into the original image by replacing the least significant bits of the pixels in the original image. For the human visual system (HVS), the small changes in gray values are regarded as noise. The LSB method has the disadvantage that the least significant bits may be easily circumvented. It is possible to destroy the exiting code using modifications, such as randomly flipping the lower bits or lossy compression.

Transform-domain methods such as the Fourier transform [16], discrete cosine transform [6, 7, 9, 10, 12, 13, 17, 24], or wavelet transform [16] are based on spatial transformation, and processes the coefficients in the frequency domain for hiding data. 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.

Research involving watermark has become an interesting topic. 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.

a. 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.

b. 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 be able to resist against the malicious attack that denotes the manipulation of destroying or removing the watermark.

c. 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, an adaptive watermarking scheme based on the HVS model and lead in the fuzzy inference system (FIS) for adapting the watermark strength to each selected DCT (discrete cosine transform) coefficient is proposed. This provides a maximum power subject to the imperceptibility constraint. The rest of this paper is organized as follows. In Section 2, some significant previous works are introduced. The proposed method for adaptive watermarking is described in Section 3. The embedding and extraction processes of the watermark are described in Section 4. In Section 5, the experimental results are given. Advanced discussions about the proposed method are given in Section 6. Section 7 concludes this paper.

II. PREVIOUS WORKS

A well-known frequency-domain watermark scheme was introduced by Cox *et al.* [10] in 1997. Cox *et al.* proposed a spread-spectrum watermark scheme. They used a spread-spectrum-like method to insert watermark into the perceptually most significant spectral components of the signal. The watermark is a sequence of real numbers *X* = $x_1,\ldots,x_n$ with a normal distribution *N*(0,1) that has zero mean and a variance of one. The watermark is inserted into the original image *V* to produce the watermarked image V'. It is described as:

$$v_i' = v_i + \alpha x_i\,, \tag{1}$$

$$v_i' = v_i(1 + x_i)\,, \tag{2}$$

$$v_i' = v_i + e^{\alpha x_i}\,, \tag{3}$$

where v_i refers to the selected DCT coefficient of image *V* and α is the strength value of the watermark *X*. The Eq. (1) may not be suitable when the v_i varies violently. The other two equations, Eq. (2) and Eq. (3) are more adaptive to the variation of v_i. The selection of strength value α had not been discussed by Cox *et al.* By this scheme, Cox *et al.* spread the watermark over broadband so it is imperceptible in any frequency beam.

However, how to select the best strength value α of the watermark for hiding is an important and difficult topic. Many researches try and apply the knowledge of human visual system to the watermarking scheme. Cox *et al.*'s scheme can be improved by introducing the adaptive strength value α_i for different spectrum component v_i. The α_i can be adapted by using the human visual model to determine the bound of watermark strength. This allows us to provide the maximum strength watermark, which gives consideration to imperceptibility and robustness. The degree of visual immunity from the watermarking modification can be constrained and the degree of watermark robustness can be increased.

In 1998, Huang and Shi [13] proposed an adaptive spread-spectrum watermark scheme based on human visual system. It was adaptive in the strength of watermarks by accounting the human visual mask: brightness sensitivity and texture sensitivity. The brightness sensitivity is estimated by the DC components in the DCT domain. The texture sensitivity is estimated by quantizing the DCT coefficients using the JPEG quantization table and calculating the numbers of non-zero coefficients. All blocks are clustered into three classes: (1)dark and weak texture, (2) bright and strong texture, and (3) remaining situation. To embed the watermark *W*, it can be described as:

$$\begin{aligned} &X_k^{'}(u,v) = X_k(u,v) + \alpha_k w_i, \\ &\text{for } 3k \le i < 3(k+1) \\ &\text{and} \\ &(u,v) \in \{(0,1),(1,0),(1,1)\}, \qquad (4) \end{aligned}$$

where $X_k(u,v)$ refers to the *k*th block DCT coefficient, and α_k is an adaptive weight of watermark in the *k*th block. Three numbers of the watermark sequences are embedded in low frequency coefficients of each block. For the α_k of each block, it has only one of three levels that is described as $\alpha_k \in \{Class_i \mid i = 1,2,3\}$. However, it could not satisfy the image visual model exactly and smoothly.

In 1999, Kim *et al.*'s [20] proposed a watermarking method using the human visual system based on wavelet transform. The number of watermark elements are proportional to the energy contained in each wavelet transform bands. To estimate the characteristic of the image, the changing rate of a sinusoidal pattern per subtended visual angle in cycles per degree is calculated. The result is used as the visual weight of watermarks in each wavelet transform band.

In 2000, Chen et al's [21] proposed an adaptive watermarking scheme. This scheme embeds a binary image as watermark in DCT approach. The watermarked image is imperceptible by human visual system. It uses a feature-based method to locate the watermark positions during embedding and extracting. The feature-based method uses the Sobel edge-detector to obtain the gradient magnitude and this result is proportional to the amount of watermark bits.

In this paper, we propose a watermarking method that is based on the fuzzy inference system to extract the human knowledge in the HVS. In this method, it allows us to provide the suitable strength of watermarks. The watermarks are embedded adaptively according to the estimation of the FIS based on the HVS. As a result, our watermarking scheme is more robust and imperceptible.

III. RESOLVING THE HUMAN VISUAL SYSTEM BY FUZZY INFERENCE SYSTEM

In the HVS, two properties can be employed in the watermarking scheme: (1) luminance sensitivity: the brighter the background is, the larger the embedded signal could be [24], and (2) frequency sensitivity: the higher the frequency is, the larger the embedded signal could be [25]. 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 non-zero coefficients as the frequency sensitivity.

The 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 perceptual sensitivity to fuzzy associations. Then the fuzzy association is used as the suitable weight of watermark.

A. The Fuzzy Inference System

Fuzzy theory holds that all things are matters of degree. It also reduces black-white logic and mathematics to special limiting cases of gray relationships.

In the classical crisp set, an element either belongs to or does not belong to the set. Oppositely, the fuzzy set is a generalization of an ordinary set in that it allows the degree of membership for each element to range over the unit interval [0, 1]. The membership function of a fuzzy set maps each element to its range space, which is set to the unit interval. The difference between fuzzy and crisp set is that the fuzzy set has an infinite number of membership functions may represent it, while the crisp set always has unique membership functions. The main benefits of fuzzy set are that it can be adjusted for maximum utility in a given situation and it includes higher expressive power, more desirable ability of modeling real-world problems, and better tolerance for imprecision.

The basic ideal of the fuzzy inference system is to assimilate the “expert experience”. The input-output relationship of a human operator in controlling a process is described by a gathering of fuzzy inference rules. The FIS allows simple and more human approaches to a decision or inference design due to its ability to determine outputs for a given set of inputs without using conventional, mathematical models. The FIS solves the inference and decision works like the human being. Using set of inference rules and membership functions, the FIS converts linguistic variables into numeric values. The FIS shown as Fig. 1 works via the following four components: a fuzzifier, a fuzzy inference engine, a fuzzy rule base, and a defuzzifier [26, 27, 28]. The details about the operations are described as follows.

(1) Fuzzifier: A fuzzifier performs the function of fuzzification which tranforms measurement data into valuation of a subjective value. The fuzzifier maps input crisp points to memberships of fuzzy sets. The input data is denoted as *x*, and μ is the membership of *x*. The *x* in a universe of discourse *U* is characterized by *T*(*x*) ={ $T_x^1, T_x^2, ..., T_x^k$ }. The membership functions used in a FIS are usually

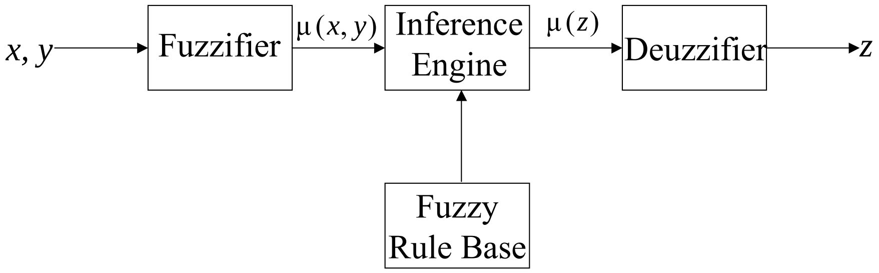


Fig. 1. Fuzzy inference system (FIS).

functions such as triangular function, trapezoid function, sigmoid function, and radial-basis function.

(2) Fuzzy rule base: The fuzzy rule base consists of a collection of fuzzy IF-THEN rules. It provides a natural framework to incorporate fuzzy IF-THEN rules from human experts.

$$\begin{aligned}&R^i : \text{ IF } x \textit{ is } A_i,\ldots, \text{ AND } y \text{ is } B_i,\\ &\text{THEN } z \text{ is } C_i \text{ , for } i=1, 2,\ldots, \text{n},\end{aligned} \quad (5)$$

where *x* and *y* are the input variables and *z* is the output variable. *A*, *B*, and *C* are the membership functions in the fuzzy set.

(3) Fuzzy inference engine: the fuzzy inference engine use the fuzzy IF-THEN rules to determine a mapping from fuzzy sets in the input to the output based on fuzzy logic principles. This collection of fuzzy rules characterizes the simple input-output relation of the system. Membership functions are combined using an inference method based on the compositional rule of inference for approximate reasoning. The inference output is found using the Max-Min inference techniques that are the most popular methods in inference. The general form of inference processes with multi-input variables and single-output variable can be represented as:

$$\text{INPUT} : x \textit{ is } A',\ldots, \text{AND } y \text{ is } B',$$

$$\begin{aligned}&R^1 : \text{ IF } x \textit{ is } A_1,\ldots, \text{AND } y \text{ is } B_1,\\ &\text{THEN } z \text{ is } C_1 \text{ ,}\end{aligned}$$

$$\vdots$$

$$\underline{\begin{aligned}&\text{ALSO } R^i : \text{ IF } x \textit{ is } A_i,\ldots,\\ &\text{AND } y \text{ is } B_i,\ \text{THEN } z \text{ is } C_i\end{aligned}}$$

$$\text{CONCLUSION} : \quad z \text{ is } C' .$$

(4) Defuzzifier: Defuzzification is a mapping from a space of fuzzy actions into a space of nonfuzzy actions. The defuzzification strategy is aimed at producing a nonfuzzy action that best represents the possibility distribution of an inferred fuzzy action.

B. The Estimation of HVS Model

There are two parameters that will be emulated by the HVS, and they are used as the input data for the FIS to calculate the adaptive weight α_k for a watermark. The luminance sensitivity is estimated by the following formula:

$$L_k = \frac{X_{DC,k}}{\overline{X}_{DC}}, \qquad (6)$$

where $X_{DC,k}$ denotes the DC coefficient of the DCT for block *k* and $\overline{X}_{DC}$ is the mean value of all DC coefficients in an image. The frequency sensitivity is estimated by quantizing the DCT coefficients of an image using the JPEG quantization table. The quantization results are round to the nearest integer. Then, we compute the number of non-zero coefficients as the frequency sensitivity [13]. The frequency sensitivity is estimated by the following formula:

$$F_k = Acc\{Round[X_k(u,v)/Q(u,v)]\}, \qquad (7)$$

where *Acc* is an accumulator that accumulates the numbers of non-zero integer, *Round*[*R*] takes the rounded integer of *R* and *Q* is the JPEG quantization table, $X_k(u,v)$ refers to the *k*th block of DCT coefficients.

C. The Estimation of FIS

The luminance sensitivity L_k and the frequency sensitivity F_k are taken as the input measured data of the FIS for estimating the adaptive weight α_k. The transform function between sensitivity and membership is a trapezoidal function. It is shown as Fig. 2 that the sensitivity values are mapping to the membership value in a fuzzy set.

Consider a fuzzy association for intelligent inference of an adaptive watermark by HVS model, the 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 rough, 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 rough, then keep the amount of embedding information big.

The rules shown above are corresponding to R^1 to R^4. And we have the following variables defined as:

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: “BIG” in the fuzzy set.

Then the basic HVS knowledge can be described as IF-THEN rules in the inference system as follows and the diagrammatic representation of inference processes is shown as Fig. 3.

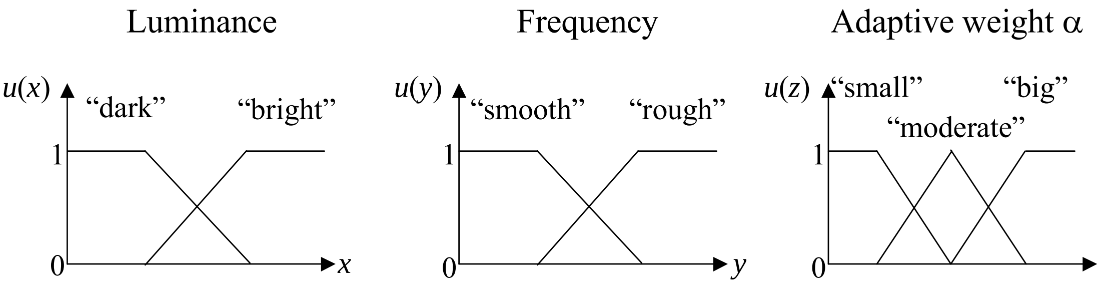


Fig. 2. The membership function mapping input/output variables to fuzzy set.

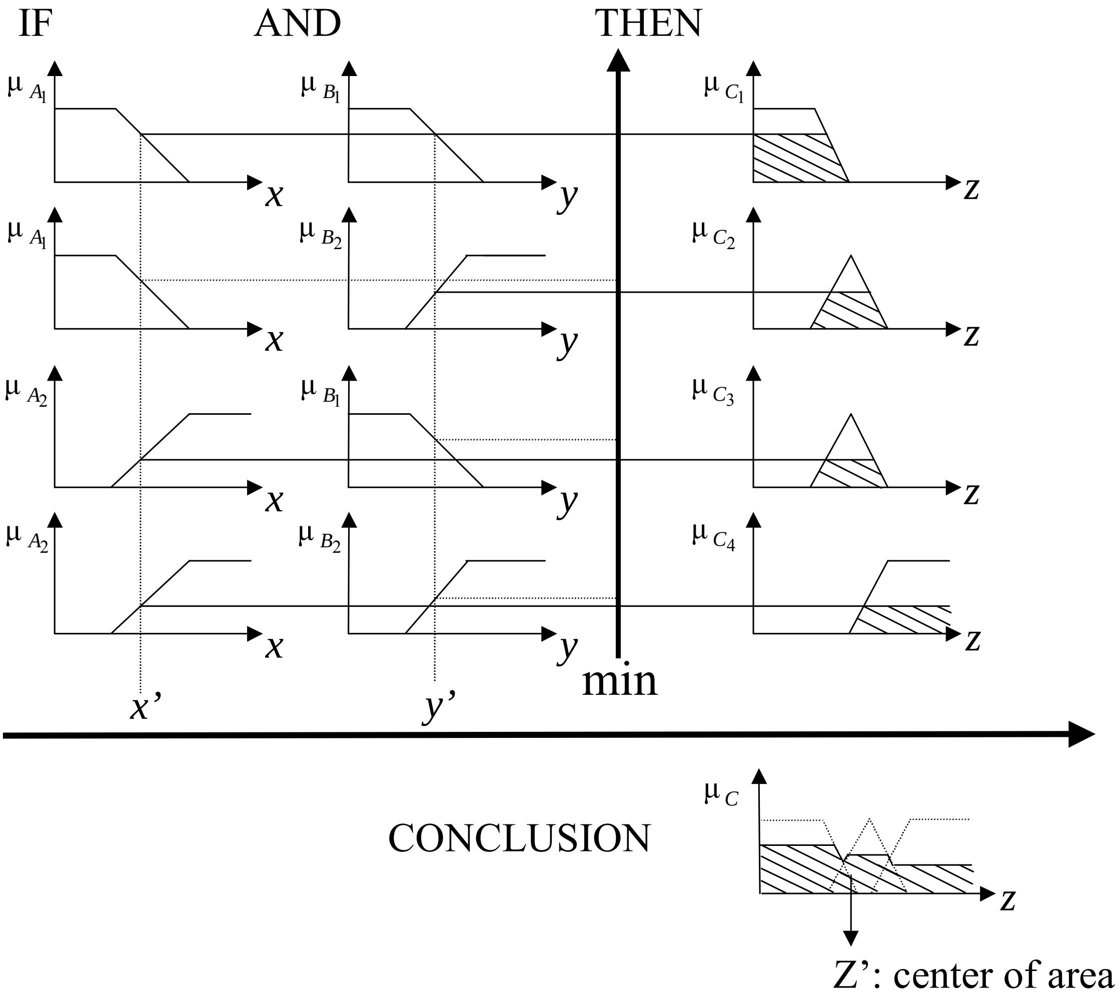


Fig. 3. The fuzzy inference process.

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 $C^{'}$.

The centroid method is used to defuzzify the inference results in the defuzzifier process. The output fuzzy set C can be defuzzified with the centroid technique to produce an exact element of output. The inferred values of the action from numbers of fuzzy inference rules are computed by the following formula:

$$z = \frac{\sum_{i=1}^{n} \mu_c(z_i) \cdot z_i}{\sum_{i=1}^{n} \mu_c(z_i)}, \tag{8}$$

where n is the quantization level, z_i is the output at level i, and μ_c is the membership value in the fuzzy set C. The infered result z is used as the adaptive weight α_k of a watermark which coresponds to the kth block image.

IV. THE PROPOSED WATERMARKING SYSTEM

A. The Watermark Embedding Process

The watermark in our proposed method is a sequences of random number that its length is n and have the normal distribution $N(0,1)$, i.e., $W = \{w_i, 0 \le i < n\}$. The original image is decomposed into non-overlapping blocks of 8×8 and the DCT is computed for each blocks. The DCT coefficients are recorded into zig-zag scan such as the JPEG compression algorithm. To embed the watermark W, it can be described as follows.

$$\begin{aligned} &X'_k(u,v) = X_k(u,v)(1+\alpha_k w_i) \\ &\text{for } 3k \le i < 3(k+1) \\ &\text{and } (u,v) = (0,1),(1,0),(1,1), \end{aligned} \tag{9}$$

where $X_k(u,v)$ refers to the kth block of DCT coefficients, and α_k is the adaptive weight of watermark in the kth block. Each block is embedded two elements of the watermark sequence. The corresponding watermark sequences are embedded in three lowest frequency coefficients of each block, $X(1,0)$, $X(0,1)$ and $X(1,1)$, except the DC component, $X(0,0)$.

The watermark embedding process is shown as Fig. 4. The original image is decomposed into non-overlapping 8×8 blocks, and the DCT process is performed for every block. Then, the luminance sensitivity and frequency sensitivity are computed as the input of the FIS. The output α_k 's of the FIS is used to as the weight of the watermark.

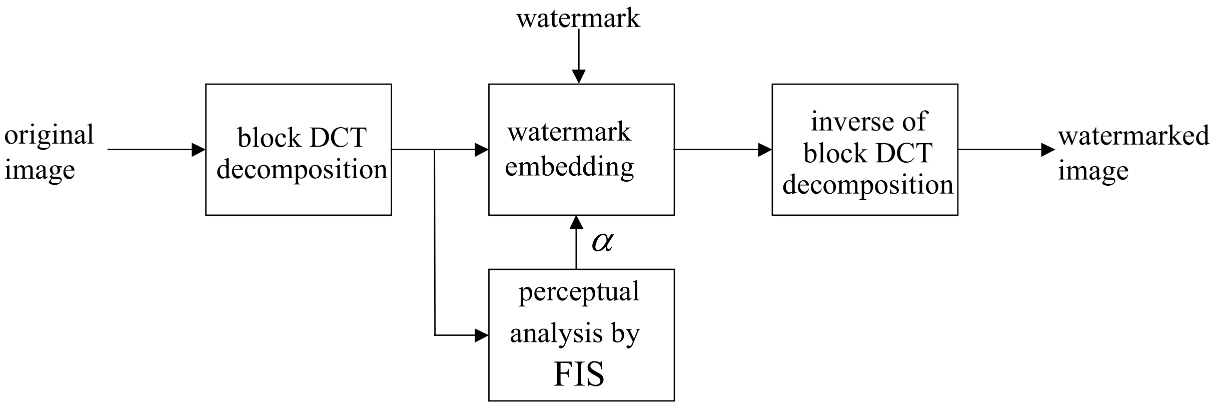


Fig. 4. The watermarking embedding process.

B. The Watermark Detection Process

The watermark detection process is shown as Fig. 5. 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 the 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 performed as follows.

$$w_k^*(u,v) = (X_k(u,v) - X_k^*(u,v)) \big/ \alpha_k X_k(u,v)$$
$$\text{for } (u,v) = (0,1),(1,0),(1,1), \qquad (10)$$

$$w^* = \bigcup_k w_k^* , \qquad (11)$$

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

The watermark detection process computes the correlation between w^* and w as:

$$\rho = \frac{w^* \cdot w}{\sqrt{w^* \cdot w^*}}, \qquad (12)$$

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

V. EXPERIMENTAL RESULTS

The proposed watermarking scheme has been tested on the images as Fig. 6(a). The watermark is a random number sequences that its length is 1000 and have the normal distribution $N(0, 1)$. In the Cox *et al.*'s method, we use the Eq. (2) and the parameter $\alpha = 0.1$. Firstly, we test the imperceptibility of our proposed method. The watermarked image using our proposed method is shown as Fig. 6(b). The transparency of all watermarked images is not affected. Our method

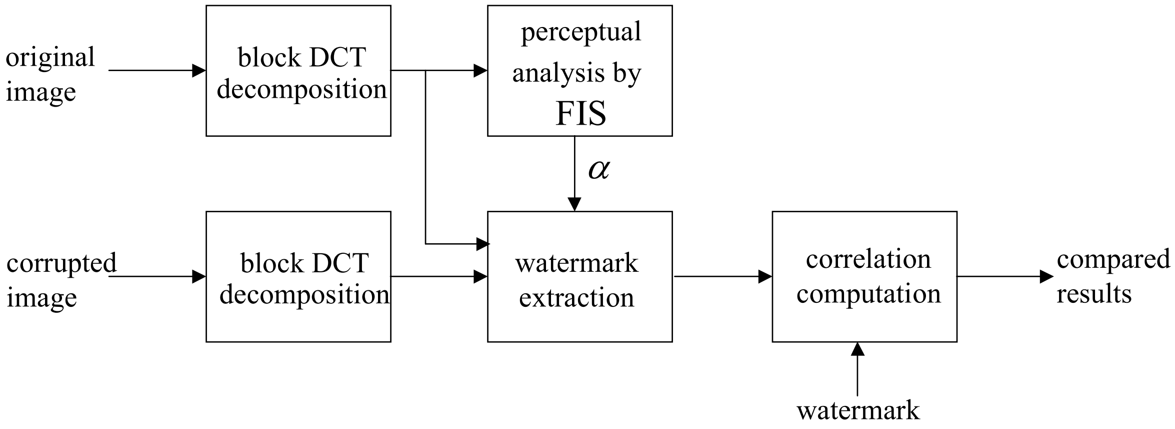


Fig. 5. The watermark detection process.

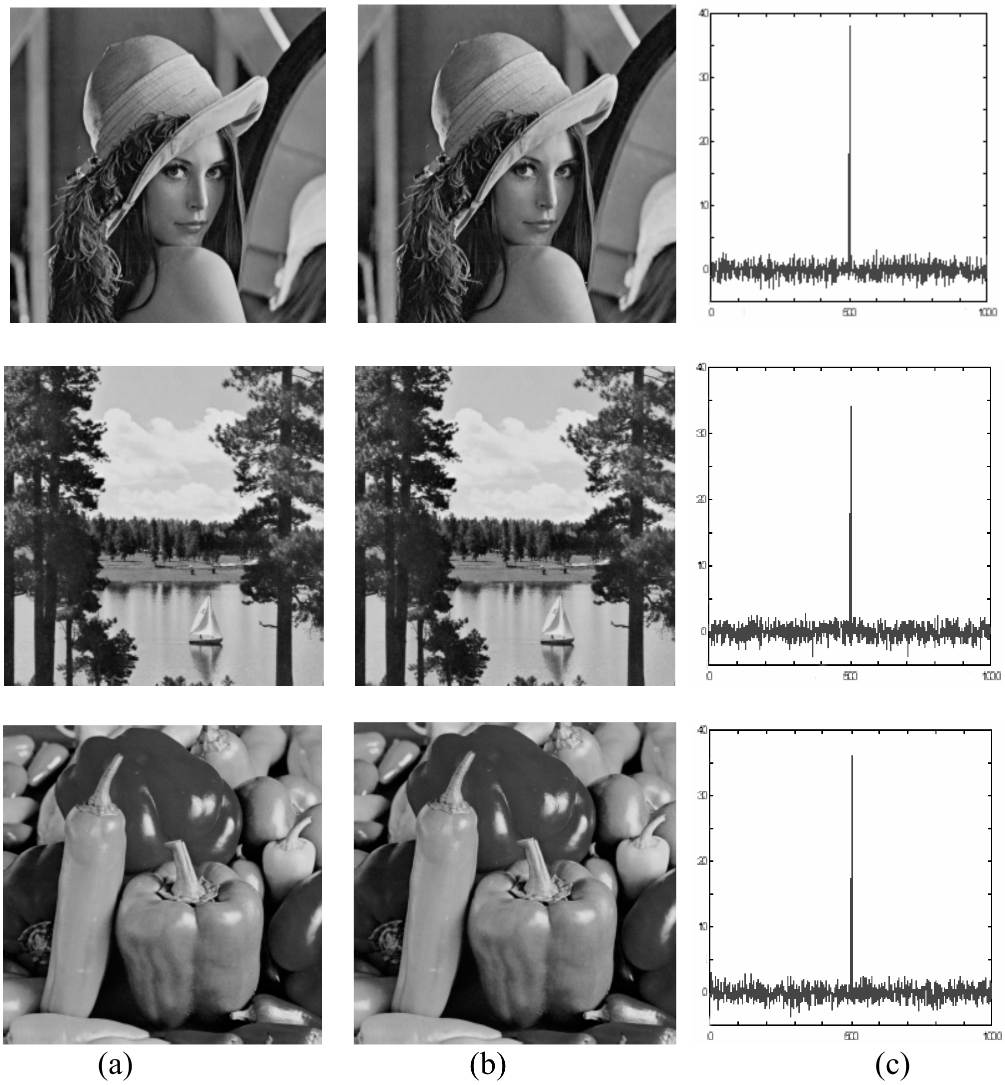


Fig. 6. The watermarked results: (a) original images of size 256□256, (b) watermarked images by our method, (c) the. responses of the watermark detector to 1000 randomly generated watermarks and only the 500th is the correct watermark.

demonstrates the same image quality as the original images. For the similarity measure, 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. 6(c). Then, the capacity of watermarking method is compared. Figs. 7(a), 7(b), and 7(c) show the weights corresponding to the blocks in the original images. They are generated by Cox *et al.*'s method, Huang-Shi's method, and our proposed method, respectively. In the Cox *et al.*'s method, the weight is static that shown as Fig. 7(a). The weights of the other two methods are adaptive by the perceptual character of the original images. In Fig. 7(b), there are only three levels in the Huang-Shi's method. Fig. 7(c) is generated by our proposed method that is smoother than the Huang-Shi's method. The difference images between the watermarked image and the original image exhibit the embedded watermark are shown as Fig. 8. Fig. 8(a) are the difference images using the Cox *et al.*'s scheme, Fig. 8(b) are the difference images using Huang-Shi's scheme, and Fig. 8(c) are the difference images using our proposed scheme. The Cox *et al.*'s scheme could embed small amount of watermarks. In this aspect, our scheme shows larger capacity for watermark. However, the image quality has difference. The values of peak signal to noise ratio (PSNR) are 34.4 dB for Cox *et al.*'s method, 41.5 dB for Huang-Shi's method, and 42.1 dB for our method, respectively. They are compared with the original image (Fig. 6(a) top) and the watermarked image (Fig. 6(b) top). It means less influence of perceptivity but more amounts of watermark by our method. Hence it satisfies the capacity requirement.

Finally, Fig. 9 shows the correlation results after different JPEG compressions by comparing our method, Cox *et al.*'s method and Huang-Shi's method. The tested image is Fig. 6(b) top. The image quality in our watermarked image is better. The watermarked images are compressed in different quality factor. The lower quality factor value corresponds to the greater compression. The detector responses in our method are still better than those of Cox *et al.*'s method and Huang-Shi's method. Figs. 10(a), 10(b), 10(c), 10(d), and 10(e) shown some attacks against the proposed watermarking scheme, namely such as distorted by Gaussian-noise, blurred, cropped, scaled, and brightened. The tested image is top of Fig. 6(b). The experimental results shown as Figs. 10(f), 10(g), 10(h), 10(i), and 10(j) demonstrated the robustness of the proposed watermarking scheme. The responses of detector are 12.5, 18.6, 21.4, 17.2, and 15.8, respectively. In the above experiments, the embedding watermark defenses the distortion; hence it is robust and imperceptible.

VI. DISCUSSIONS

In Section V, we show that the proposed fuzzy method has better response than the α-based DCT-domain watermarking schemes proposed in refs. [11] and [13]. The other DCT-domain watermarking schemes such as the cocktail watermarking scheme [29] are not included in our experiments due to that they are based on another approaches. We also show that the watermark embedded with the proposed method can survive various image-processing operations. It is worthwhile to note some special-purpose attacks. Among them, the LR attack [30] may be the most aggressive one.

The LR attack operator is based on the results of multiple applications of the Laplacian operator [31]. Generally, it can be seen as a band-pass filter. As described in [30], most of the DCT-based watermarking schemes embed the

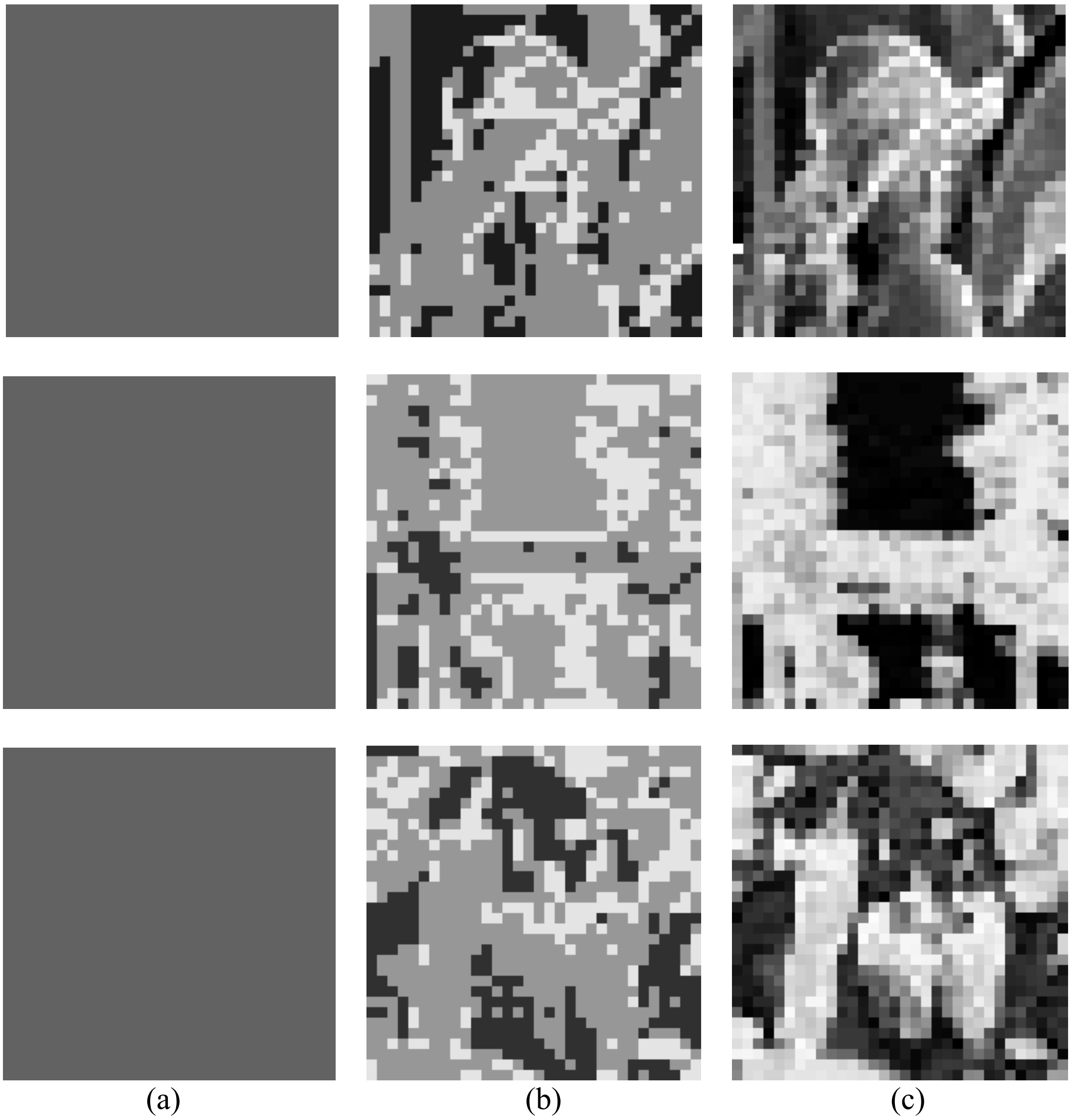
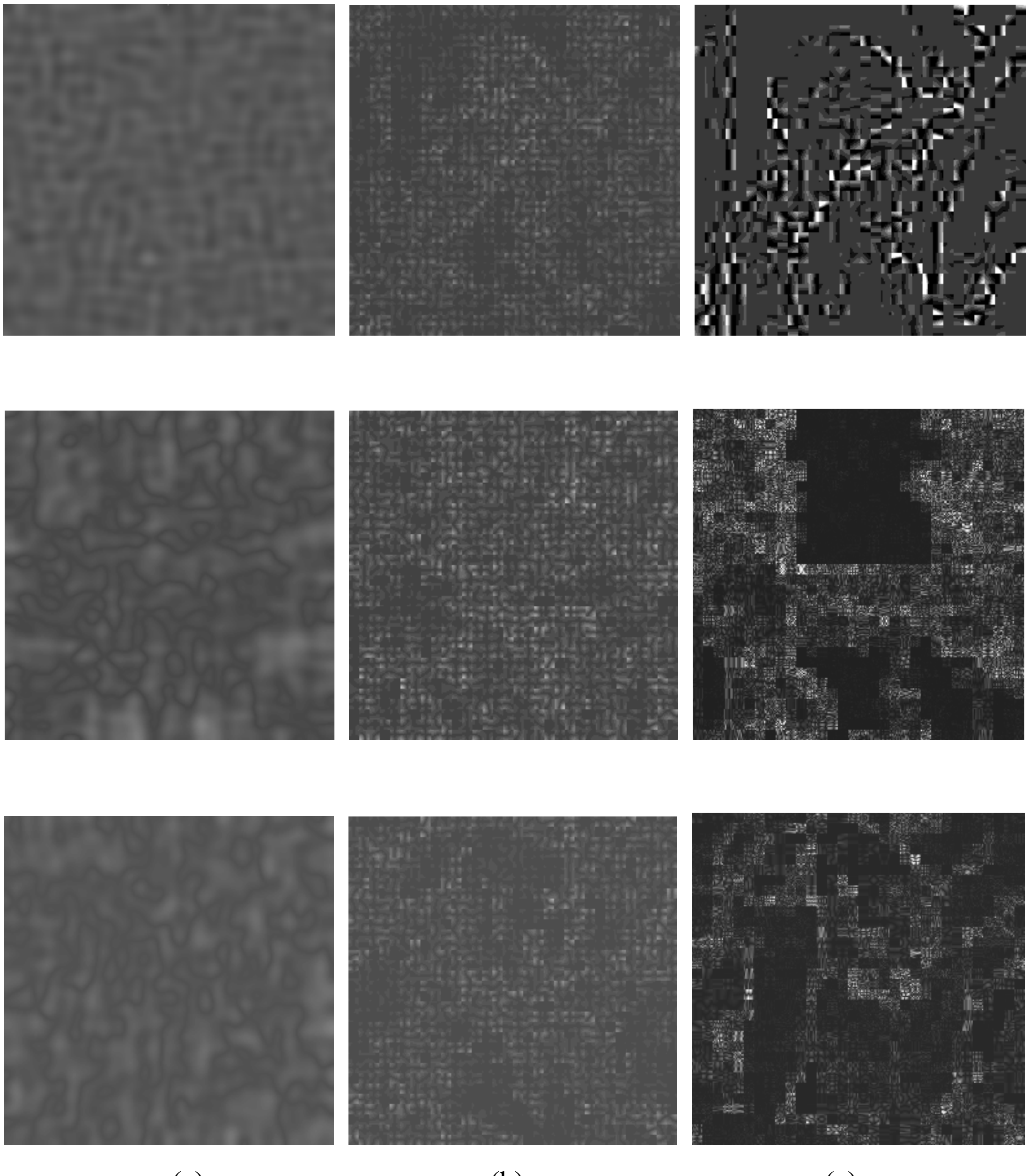

(a) (b) (c)

Fig. 7. The weight map of test images which use (a) Cox et al.'s scheme: static weight α = 0.1, (b) Huang-Shi's scheme: three levels only, (c) our scheme: it is smoother and more exact than Huang-Shi's scheme.



(a) (b) (c)

Fig. 8. The difference images between the original image and the watermarked image, which use (a) Cox et al.'s method, (b) Huang-Shi's method, and (c) our proposed method.

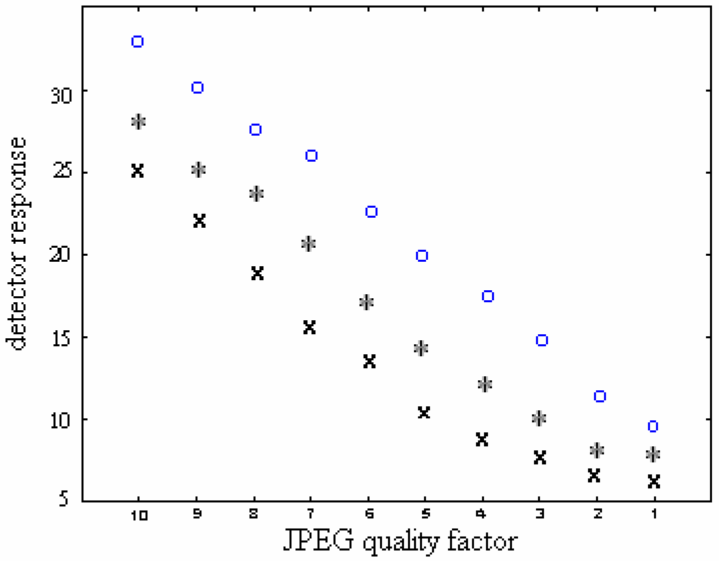
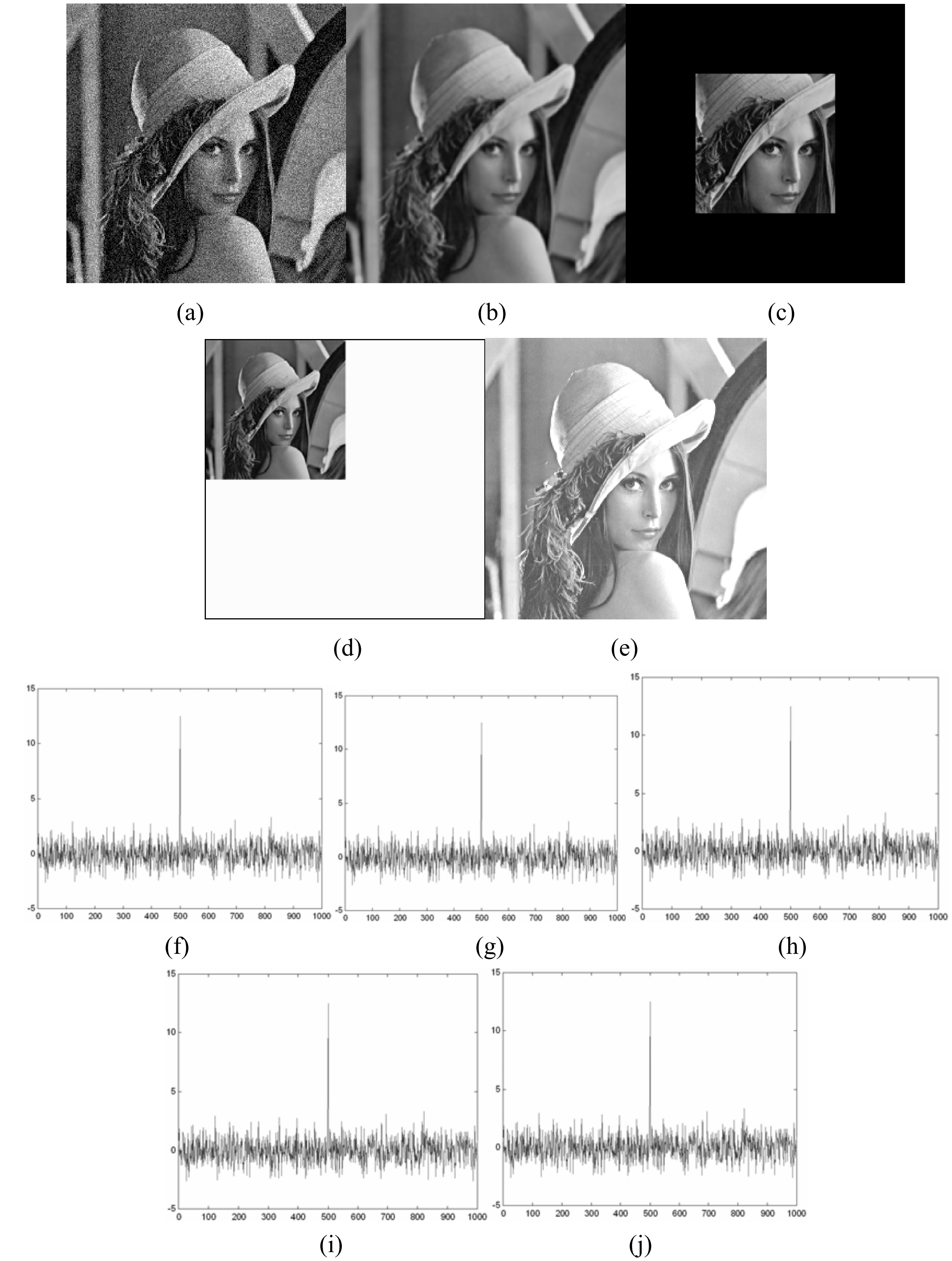


Fig. 9. Comparison of the detector response with Cox et al.'s method (symbol 'x'), Huang-Shi's method (symbol '*'), and our proposed method (symbol 'o'), which in the JPEG compression.



(a) (b) (c)

(d) (e)

(f) (g) (h)

(i) (j)

Fig. 10. Attacks for the watermarked image: (a)gaussian noised, (b)blured, (c)cropped, (d)scaled, (e)brightened, (f ~ j)the detector responses of (a ~ e), respectively.

watermark in the mid-band DCT coefficients will be defeated by the LR attack. To survive such an aggressive attack, our proposed method embeds the watermark in the lower DCT coefficients and strengthens the embedded watermark by fuzzy control. Another benefit of using fuzzy control is the transparency of the embedded watermark remains while the watermark is strengthened. The experimental results demonstrated in Section V have shown that the watermark embedded with our proposed method has good transparency. A benchmark called *chechmark* [32] is adopted to test the effectiveness of the proposed method against the LR attack. The watermarked image used in Section V is corrupted by the LR attack, and the response of the detector is 10.2. It is clear that the proposed method can survive the LR attack.

VII. CONCLUSIONS

The spread-spectrum watermark method proposed by Cox et al. has a weakness that the perceptual model is not taken account. For the reason of imperceptibility constraint of the watermark, this scheme must embed the low strength watermark to avoid degrading the image quality. Unfortunately, it reduces the robustness of the watermark.

In this paper, an adaptive watermarking method 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 results of our adaptive watermark method are the following: our method provides he advantages of fuzzy logic inference on extracting the human's intelligence. And it also improves both the Cox et al.'s method and Huang-Shi's method such that applies the adjustment of watermark strength more smooth and more compatible to the variation of human visual model. Hence, the capacity of the watermark can be larger, and it is hence more robust and imperceptible.

REFERENCES

[1] Lou, D.-C. and Liu, J.-L., "Steganographic Method for Secure Communications," Computers & Security Vol. 21, No. 5, pp. 449-460, 2002.

[2] Lou, D.-C. and Sung, C.-H., "A Steganographic Scheme for Secure Communication Based on Chaos and Euler Theorem," to appear in IEEE Transactions on Multimedia. (Accepted, No: MM10288)

[3] Lou, D.-C. and Yin, T.-L., "Spatial Database with Each Picture Self-Contained Multiscape and Access Control in a Hierarchy," The Journal of Systems and Software, Vol. 56, No. 2, pp. 153-163, 2001.

[4] Lou, D.-C. and Liu, J.-L., "Fault Resilient and Compression Tolerant Digital Signature for Image Authentication," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 31-39, 2000.

[5] Lou, D.-C. and Yin, T.-L., "Adaptive Digital Watermarking Using Fuzzy Clustering Technique," IEICE Transactions

on Fundamentals of Electronics, Communications, and Computer Sciences, Vol. E84-A, No. 8, pp. 2052-2060, 2001.

[6] Lou, D.-C. and Yin, T.-L., “Robust Digital Watermarking for Image Authentication,” Journal of Chung Cheng Institute of Technology, Vol. 30, No. 1, pp. 13-26, 2001.

[7] Barni, M., Bartolini, F., Cappellini, V., and Piva, A., “A DCT-Domain System for Robust Image Watermarking,” Signal Processing, Vol. 66, No. 3, pp. 357-372, 1998.

[8] Brassil, J., Low, S., Maxemchuk, N., and O’Gorman, L., “Electronic Marking and Identification Techniques to Discourage Document Copying,” IEEE Journal on Selected Areas in Communications, Vol. 13, No. 8, pp. 1495-1504, 1995.

[9] Burgett, S., Koch, E., and Zhao, J., “Copyright Labeling of Digitized Image Data,” IEEE Communications Magazine, Vol. 36, No. 3, pp. 94-100, 1998.

[10] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T., “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.

[11] Cox, I. J. and Linnartz, J.-P., “Some General Methods for Tampering with Watermarks,” IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 587-593, 1998.

[12] Hsu, C.-T. and Wu, J.-L., “DCT-based Watermarking for Video,” IEEE Transactions on Consumer Electronics, Vol. 44, No. 1, pp. 206-216, 1998.

[13] Huang, J. and Shi, Y. Q., “Adaptive Image Watermarking Scheme Based on Visual Masking,” IEE Electronics Letters, Vol. 34, No. 8, pp. 748-750, 1998.

[14] Hwang, M.-S., Chang, C.-C., and Hwang, K.-F., “A Watermarking Technique Based on One-Way Hash Functions,” IEEE Transactions on Consumer Electronics, Vol. 45, No. 2, pp. 286-294, 1999.

[15] Kundur, D. and Hatzinakos, D., “Digital Watermarking Using Multiresolution Wavelet Decomposition,” Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, part 5 (of 6), Vol. 5, pp. 2969-2972, 1998.

[16] O'Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M., ”Phase Watermarking of Digital Images,” Proceedings of the 1996 IEEE International Conference on Image Processing, Vol. 3, pp. 239-242, 1996.

[17] Tao, B. and Dickinson, B., “Adaptive Watermarking in the DCT Domain,” Proceedings of the 1997 IEEE International Conference on Image Processing, pp. 2985-2988, 1997.

[18] Voyatzis, G. and Pitas, I., “Applications of Toral Automorphisms in Image Watermarking,” Proceedings of the 1996 IEEE International Conference on Image Processing, Vol. 2, pp. 237-240, 1996.

[19] Walton, S., “Image Authentication for a Slippery New Age,” Dr. Dobb's Journal, Vol. 20, No. 4, pp. 18-26, 1995.

[20] Kim, Y.-S., Kwon, O.-H., and Park, R.-H., “Wavelet Based Watermarking Method for

Digital Images Using The Human Visual System," IEE Electronics Letters, Vol. 35, No. 6, pp. 466-468, 1999.

[21] Chen, D.-Y., Ouhyoung, M., and Wu, J.-L., "A Shift-Resisting Public Watermark System for Protecting Image Processing Software," IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp. 404-414, 2000.

[22] Turner, L. F., Digital data security system, Patent IPN WO 89/08915, 1989.

[23] Bender, W., Gruhl, D., Morimoto, N., and Lu A., "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.

[24] Watson, A. B., "DCT Quantization Matrices Visually Optimized for Individual Images," Proceeding of the SPIE Conference on Human Vision, Visual Processing, and Digital Display IV, Vol. 1913, pp. 202-216, 1993.

[25] Jayant, N. S., Johnson, J. D., and Safranek, R. J., "Perceptual Coding of Image Signals," Proceeding of IEEE, Vol. 81, No. 10, pp. 1385-1422, 1993.

[26] Kosko B., Neural Networks and Fuzzy Systems, Prentice-Hall, New Jersey, 1992.

[27] Kosko, B., "Counting with Fuzzy Sets," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. PAMI-8, pp. 556-557, 1986.

[28] Wang, L.-X., Adaptive Fuzzy Systems and Control, Prentice-Hall, New Jersey, 1994.

[29] Lu, C.-S. and Liao, M. H.-Y. "Oblivious Cocktail Watermarking by Sparse Code Shrinkage: A Regional- and Global-Based Scheme," Proceedings of the IEEE international Conference on Image Processing, Vol. III, pp. 13-16, 2000.

[30] Barnett, R. and Pearson, D., "Attack Operators for Digitally Watermarked Images," IEE Proceedings Vision, Image and Signal Processing, Vol. 145, No. 4, pp. 271-279, 1998.

[31] Gonzalez, R. C. and Woods, R. E., Digital Image Processing, Addison-Wesley, New York, 1992.

[32] http://www.watermarkingworld.org/checkmark/checkmark.html