DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4558

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

FUZZY BASED INVISIBLE WATERMARKING

T.R.Vijaya Lakshmi
Dept. of ECE, MGIT
Hyderabad, India

Abstract: Due to the rapid increase in computer and network technology, the need for securing digital information becomes an important target for technology producers; specially researchers. In this work HVS attributes – luminance sensitivity, contrast sensitivity and edge sensitivity are modeled using Fuzzy system to embed a binary watermark image in gray-scale host images. The performance of the presented system is measured with two metrics such as PSNR and SSIM. Four types of attacks are subjected on the watermarked/signed images to test the robustness of the proposed scheme. The presented system focuses on optimizing the trade-off between the imperceptibility and robustness.

Keyword: Fuzzy system, HVS parameters, attacks, imperceptibility.

1. INTRODUCTION

Digital watermarking came to be in great demand when sharing information on the Internet became a usual practice. Sharing files online, you never know if someone uses them without your consent. To prevent unauthorized commerce use of files, one can publish them to the web in the worst quality or don't publish anything worthwhile at all. It isn't a good way to solve the problem of unauthorized use, so, you should look for more effective ways of copyright protection, such as digital watermarking. A digital watermark is a pattern of bits inserted into a digital file – image, audio or video. Such messages usually carry copyright information of the file. But the main difference between them is that digital watermarks are supposed to be invisible or at least not changing the perception of original file, unlike paper watermarks, which are supposed to be somewhat visible.

An invisible watermark is an embedded image which cannot be perceived with human's eyes. Only electronic devices (or specialized software) can extract the hidden information to identify the copyright owner. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity Although the copyright protection is the main field of using digital watermarks, they can also be used for such purposes as advertising (adding company's name and logo as a watermark for promotion rather than for protection) or even adding memo titles to digital photos. It's obvious that only visible watermarks can satisfy these requirements.

Invisible digital watermarking is a process of permanently embedding multimedia content into digital signal carrying information about the ownership and identification of the intellectual property so that the existence of the watermark is virtually unperceivable by human sensory system. Similar to any intellectual property on paper, information published or distributed on a networked environment needs to be safeguarded against piracy and malicious manipulation. Although encryption is possible to provide secured delivery of valuable information by deterring counterfeiters from hijacking the copyrighted information, it fails to control the distribution of the illegal copies of the original work upon decryption by the authorized recipients. The use of invisible digital watermarking schemes to certify the image legitimacy and enable the tracking of the distribution of its permitted copies is a viable solution to this problem.

2. RELATED WORK

Most watermark embedding processes are performed in either spatial domain or transform domain. In spatial domain watermarking schemes [1-3] the watermark image is directly embedded into the host image by changing its pixel values. Both the insertion and extraction processes are relatively simple compared to transform domain watermarking schemes. However, it is more difficult for spatial domain watermarks to achieve imperceptibility because of the need to embed high intensity digital watermark for robustness tends to degrade the image visual quality.

In transform domain watermarking schemes [4-12] transform domain coefficients of the host image are modulated by the watermark information. They have several advantages over spatial domain schemes. First, it is more difficult for attackers to extract the marked information and hence to alter the watermarks since the watermark is irregularly distributed all over the host images. Second, one can select certain bands that possess perceptually significant features to embed the watermark. Third, it is the transform domain coefficients that are modified rather than the pixel values of the host image, making it plausible to reduce the visual artifacts of the marked image even though the watermark is introduced into the selected coefficients that contribute significantly to the host image intelligibility. However, frequency based watermarking schemes are generally susceptible to geometrical transformation attacks. This lost of synchronization can be efficiently detected and the transformation parameters can be recovered using an elegant method proposed in [10] lately for spread-spectrum like transform domain watermarking schemes.

As the host images are often divided into smaller equal size blocks in transform domain watermarking schemes, they can also be vulnerable to counterfeiting attack [13]. The authors in [14] use the security of a proven cryptographic hash function for a block-wise independent digital watermarking scheme to work against the counterfeiting attack.

Unfortunately, their watermarking scheme belongs to the class of a fragile digital watermarking scheme which is not designed to be resilient against even a mild image processing attack. One main weakness of their watermarking scheme is that the risk of rejecting an authentic watermarked image is high even though it has not been maliciously manipulated as noises in the communication channel are likely to corrupt more than the least significant bits of the pixels in transmitting the marked image.

Digital image watermarking techniques which are based on artificial intelligence [15, 16] are available in the literature. Throughout the years many have proposed algorithms for watermarking some of them proposed an algorithm using Fuzzy-Neural system along with super resolution, it uses both Neural Network and Fuzzy Logic for watermark extraction.

The authors in [4] proposed an algorithm based on Fuzzy-Neural system using Discrete Cosine Transform (DCT), it uses 27 fuzzy-bp rules to embed and extract the watermark.

The authors in [1] proposed a watermarking method using Back Propagation Neural Network (BPNN) and Fuzzy Inference System (FIS), and compared both the techniques for robustness against different image processing attacks.

In [16] proposed a watermarking method using Back Propagation Neural Network (BPNN) and Discrete Wavelet Transform (DWT). 2-level DWT is applied to host image.

The authors in [5] proposed an adaptive watermarking algorithm performed in the wavelet domain which exploits Human Visual System (HVS) and a Fuzzy Inference System (FIS) for medical images.

3. PROPOSED METHODOLOGY

The human visual system can perform a number of image processing tasks in a manner vastly superior to anything we are presently able to do with computers. In this paper we consider three HVS features namely, edge blocks of the image to be watermarked, the effect of variance across the blocks available in the host image and the computed values of the block intensity. The HVS based watermarking is expected to give good quality imperceptibly signed images.

This work focuses on optimizing the trade-off between the twin parameters of image watermarking: imperceptibility and robustness. We thus, propose a grayscale image watermarking scheme using the hybrid Fuzzy by taking into account the HVS characteristics of the gray-scale host images. For this purpose we employ three different characteristics of the Human Visual System (HVS) to embed and extract the watermark from four different gray-scale host images of size 256 X 256. These images are Cameraman, Pepper, Office, Autumn and Football.

Motwani have implemented a MAMDANI type Fuzzy Inference System (FIS) which uses as its input the HVS characteristics namely brightness, texture and edge sensitivities of the gray-scale image. The output of this inference system is successfully used to embed the watermark in the host image in the DWT domain. This FIS uses a set of 27 inference rules which are primarily based on the following facts:

(1) The eye is less sensitive to noise in those areas of the image where brightness is high or low.

(2) The eye is less sensitive to noise in highly textured areas, but among these, more sensitive near the edges.

(3) The eye is less sensitive in the regions with high brightness and changes in very dark regions.

The HVS characteristics – luminance sensitivity, contrast sensitivity and edge sensitivity are fed to a Fuzzy inference system as inputs. The Fuzzy inference system is driven by the same set of 27 inference rules as proposed by Motwani. This network produces a weighting factor as its output.

Another key aspect is the decision to perform these operations on 8x8 blocks. These dimensions may seem somewhat arbitrary, and that is in part because they are. However, there are also a few reasons to support this decision. First, if the patch sizes were larger, then it is possible that the image would have larger color gradients between these blocks. It's helpful to think about the masking step as basically averaging together the values in the block before it's returned back to the viewer. If there are finer differences in an image between smaller blocks of pixels, this process won't capture those differences well. However, this would seem to indicate that an even smaller block size, such as 4x4 or 2x2 should be used. For each block, you have to take the DCT, multiply by the mask, and take the inverse DCT. With more blocks, this process would take longer. As we'll see with experimental results later, it is also harder to compress an image to the same accuracy while achieving smaller file sizes when you're using smaller blocks. Therefore, the 8x8 block size approach has emerged as the dominant way to split up the image.

The human eye is subtle to different spatial frequencies, so the effect of noise in some areas of the image cannot be noticed by the human eye because of the same reason, in the human sensitivity of human eye to many frequencies is given by the frequency sensitivity. The effect of the imperceptibility of noise on a constant background is calculated by visual system model these areas are identified and the watermark is placed in these areas. The luminance sensitivity, texture sensitivity in this HVS model is also used in many insertion and detection algorithms of the watermark.

A. HVS parameters

a. Luminance sensitivity (L_k): Brightness is proved to be effective towards masking detectable noise on a continual background. The brighter the background is, the higher the size of noise can be i.e. embedded signal.

The luminance sensitivity can be calculated by using the formula:

$$L_k = \frac{Y_{DC,k}}{\overline{Y_{DC}}} \quad (1)$$

Where $Y_{DC,k}$ is the DC quantity of the DCT of the k^{th} chunk $\overline{Y_{DC}}$ *i*s the average of all DC components of a definite image.

b. Contrast sensitivity (F_k):

If we split the image into 8x8 chunks and DCT is applied to each chunk, a 8x8 matrix will be formed of DCT components for each chunk. This matrix is separated into three parts, high-frequency (HF) components, low frequency (LF) components, and medium-frequency (MF) components. In the 2D DCT matrix's upper left corner

symbolizes low frequency component while the lowest right corner is the high frequency components. Image can be distorted if low frequency components are modified. Alternatively, since the compression process causes the DCT components to be detached in high frequencies, watermark cannot be embedded in high frequency components. So the central frequency components are utilized to embed the watermark. The normalized variance is computed to find the contrast sensitivity as defined by

$$C_k = statxture(k) \tag{2}$$

c. Edge Sensitivity (T_k):

The areas in an image can be divided into smooth, texture, and edge chunks. Texture areas are rough in nature and can withstand noise, i.e. noise cannot be noticed in these areas as it would also be mixed with the texture. The texture sensitivity is expected by rounding off the DCT components of cover image by means of the Joint Photographic Experts Group (JPEG) quantization table. The output is approximated to adjacent integers and then the non-zero numbers are counted, this routine is calculated utilizing:

$$T_k = graytres(k) \tag{3}$$

B. Fuzzy linguistic terms for three input attributes

The following fuzzy linguistic terms associated with luminance (brightness) sensitivity, contrast sensitivity and edge sensitivity are computed. Note that each linguistic variable consists of three fuzzy sets.

1. Luminance sensitivity has dark, medium and bright levels.
2. Contrast sensitivity has low, medium and high levels and
3. Edge sensitivity has small, medium and large levels.

This is done to decompose these parameters into fuzzy equivalent variables to constitute the fuzzy inference rules. These fuzzy sets are represented in LR type. Table 1 illustrates the LR-type fuzzy number equivalents for the associated attribute values.

Table 1: LR-type fuzzy number equivalents for associated attributes

Attributes	Fuzzy set	LR-Type Fuzzy Number
Brightness Sensitivity	Dark	(0, 0.001, 0.5)
	Medium	(0.5, 0.25, 0.25)
	Bright	(1, 0.5, 0.0001)
Contrast Sensitivity	Low	(0, 0.001, 0.5)
	Medium	(0.5, 0.25, 0.25)
	High	(1, 0.5, 0.0001)
Edge Sensitivity	Small	(0, 0.001, 0.5)
	Medium	(0.5, 0.25, 0.25)
	Large	(1, 0.5, 0.0001)

The final outcome of application of the fuzzy rules is the suitable output of the expert system and is given by one of the five crisp output values namely: Least (0.0), Less (0.25), Average (0.5), Higher (0.75) and Highest (1.0).

C. Watermark embedding

In the present simulation, we use four gray-scale host images represented by (I) to demonstrate watermark embedding. These images are Cameraman, Pepper, Office, and Pepper. The watermark (X) embedded in I is a binary image of size m × m pixels. Fig. 1 depicts the block diagram of the proposed watermark embedding scheme. The formula for embedding the watermark used in the present work is given by Eq. (4).

$$LL3' = LL3 * ((k * O'' * X) + 1) \tag{4}$$

Where LL3 is the 3–level DWT low frequency region of the host image, O'' is the crisp output of Fuzzy, X is the original watermark, k is the watermark scaling coefficient and LL3' is the DWT low frequency region of the signed image. The scaling coefficient, k, is optimized to be 0.07 for the binary watermark. The watermark embedding procedure is given in Algorithm 1. Perceptible quality of the watermarked images is quantified by PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index Measure).

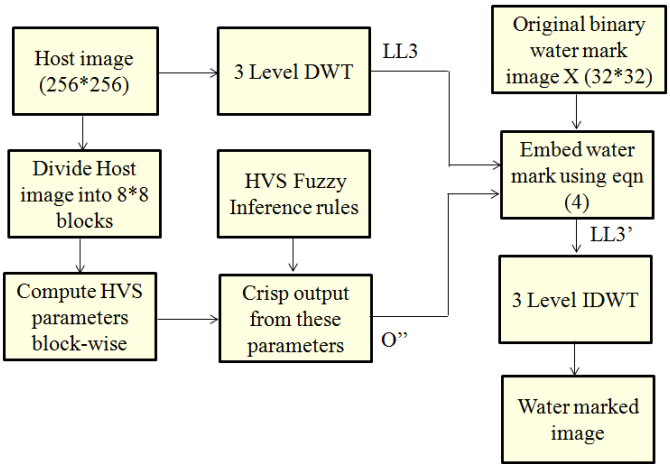

Fig.1 Proposed scheme to embed watermark

Quality assessment of the signed images (I') is done by computing two full reference quality assessment metrics PSNR and SSIM given by Eqs. (5) and (6) respectively.

$$PSNR = 10log_{10}(\frac{I_{MAX}^2}{MSE}) \tag{5}$$

where I_{max} is the maximum possible pixel value of the image I and MSE is the mean square error.

Algorithm 1: Steps involved in embedding a watermark

Steps	Watermark Embedding Algorithm
Step 1:	Divide host image into 8x8 size blocks in spatial domain and compute DCT of all blocks.
Step 2:	Compute luminance sensitivity, contrast sensitivity and edge sensitivity of all blocks of the host image using Eqs.(1)–(3) respectively.
Step 3:	Train the Fuzzy network using 27 Fuzzy inference rules derived from HVS model and retain weight set.
Step 4:	Convert block wise above computed three parameters into their equivalent LR type fuzzy numbers and supply them as input to the trained Fuzzy to obtain the crisp output (O'').
Step 5:	Apply three-level DWT on the original image to obtain the sub-band LL3.
Step 6:	Embed the watermark using the formula given in Eq. (4).
Step 7:	Compute three-level IDWT to obtain watermarked (signed) image.

$$SSIM = \frac{(2\mu_{I'}\mu_I + C_1)(2\sigma_{II'} + C_2)}{(\mu_I^2 + \mu_{I'}^2 + C_1)(\sigma_I^2 + \sigma_{I'}^2 + C_2)} \quad (6)$$

where μ_I and $\mu_{I'}$ are mean intensity or luminance component of image signals x and y respectively, C_1 and C_2 are constants.

D. Watermark Extraction

The extraction procedure is inverse of that of embedding and is informed in the present work. Fig.2 depicts the block diagram of the watermark extraction scheme. The formula for extracting the watermark used in the present work is given in Eq. (7).

$$X^* = (LL3'' - LL3)/(k * wO'') \quad (7)$$

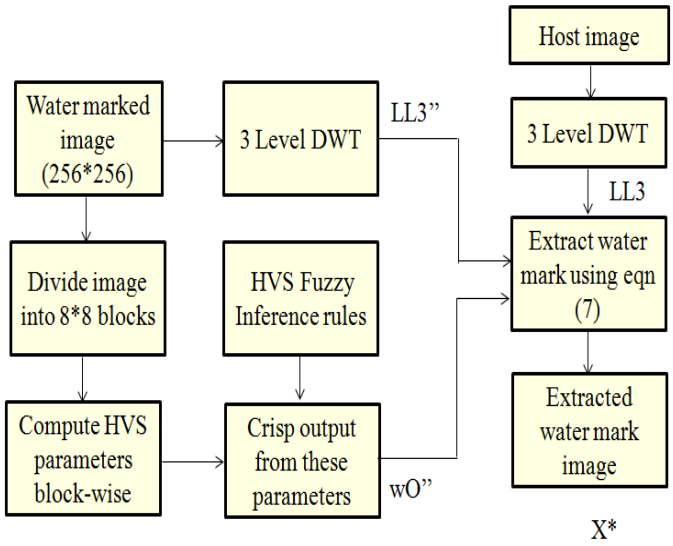

Fig.2 Proposed scheme to extract watermark

To examine the issue of robustness of the proposed embedding scheme, the watermarked images are subject to four different image processing attacks. They are Gaussian noise, Salt and pepper noise, Wiener filter and Motion Blur.

4. RESULTS AND DISCUSSIONS

This section presents results obtained by carrying out the embedding and extraction of watermark into four standard gray-scale host images. These images are Cameraman, Peppers, Office, and Football of size 256 × 256 which are shown in Fig. 3(a-d). The binary watermark of size 32×32 to embed on the host images is shown in Fig. 3(e).

Fig. 4 depicts the signed images obtained by embedding the binary watermark in host images of Fig. 3(a–d) respectively. The computed values of PSNR and SSIM are mentioned on top of these signed images. These values indicate that their visual quality is good. Fig. 4(e) depicts watermark recovered from signed image of Fig. 3(a).

To examine the robustness of the proposed embedding scheme, four different image processing operations are executed on all four signed images of Fig. 4(a–d). These attacks are namely: (1) Gaussian Noise (2) Salt and Pepper Noise (3) Wiener Filtering and (4) Motion blur. Table 2 compiles the computation results obtained from signed images after executing these attacks.

A careful observation of these results indicates the following points:

(i) High computed values of PSNR and SSIM indicate that signed images have good imperceptibility.

(ii) The plot of PSNR for signed and attacked Cameraman images with respect to k is shown in Fig. 5.

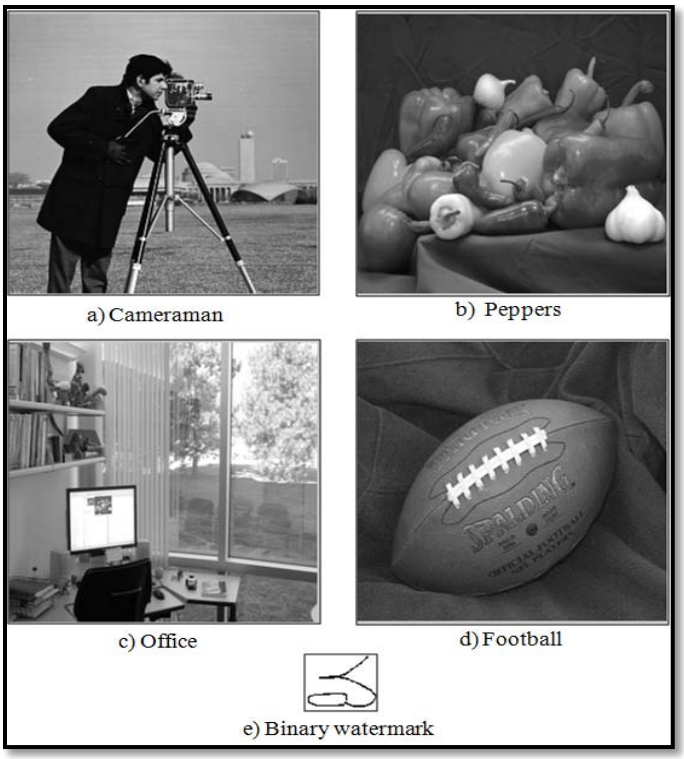

Fig. 3 (a-d) Various host images (e) Binary watermark

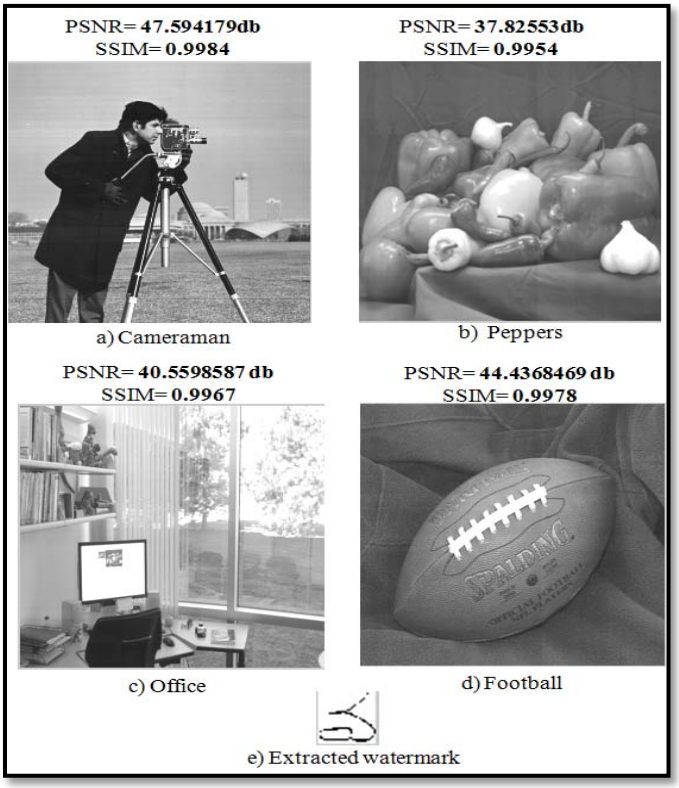

Fig. 4 (a-d) Signed/watermarked images (e) Extracted watermark

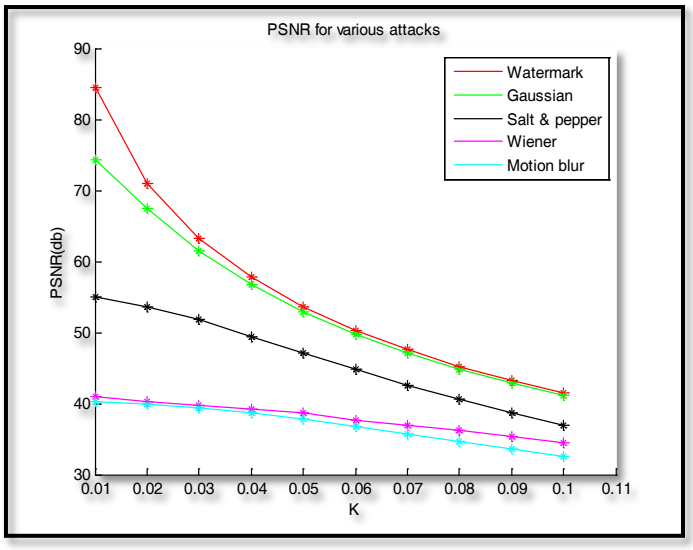

Fig. 5 PSNR for various attacks

Table 2: PSNR values for attacked Cameraman, Peppers, Office and Football images

Attack	Image	PSNR (dB)
Gaussian noise	Cameraman	47.158934
	Peppers	37.869668
	Office	40.521388
	Football	44.316785
Salt and Pepper noise	Cameraman	42.617799
	Peppers	34.560201
	Office	37.137331
	Football	41.51899
Wiener filtering	Cameraman	36.904100
	Peppers	31.269289
	Office	35.566558
	Football	34.654473
Motion blur	Cameraman	36.904100
	Peppers	31.269289
	Office	35.566558
	Football	34.654473

5. CONCLUSION

This work presents a image watermarking technique which involves three basic characteristics of the HVS model namely – Luminance, Contrast Sensitivity computed using block variance and Edge sensitivity computed using block threshold value. These HVS characteristics are modeled using Fuzzy inference system to implement watermarking. The major contribution of the proposed scheme is the application of Fuzzy expert system for gray-scale image watermarking. To examine the robustness of the proposed algorithm, four different image processing attacks are executed over signed images. Experimental results show that the proposed scheme yields high values of PSNR, which indicate that the signed and attacked images have good perceptible quality. The watermark is also extracted from the signed and attacked images using Fuzzy. Thus, the proposed algorithm is found to be extremely suitable for practical real time applications.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Syst. J., vol. 35, no. 3&4, pp. 313–336, 1996.

[2] C. Dautzenberg and F. M. Boland, "Watermarking Images," Dept. Electron and Elect. Eng., Trinity College Dublin, Tech. Rep., 1994.

[3] R. G. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in Proc. IEEE Int. Conf. Image Process., vol. 2, Nov. 1994, pp. 86–90.

[4] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," Signal Process., vol. 66, no. 3, pp. 357–372, 1998.

[5] C. H. Chang, M. Zhang, and Z. Ye, "A content-dependent robust and fragile watermarking scheme," in Proc. 2nd IASTED Int. Conf. Visualization, Imaging and Image Processing, Sep. 2002, pp. 201–206.

[6] C. H. Chang, Z. Ye, and M. Zhang, "Fuzzy-ART based digital watermarking scheme," in Proc. IEEE Asia Pacific Conf. Circuits and Systems, vol. 1, APCCAS-2002, Dec. 2002, pp. 425–426.

[7] J. J. Eggers and J. K. Su, "A blind watermarking scheme based on structured codebooks," in Proc. IEE Secure Images and Image Authentication Colloq., London, U.K., 2000, pp. 4/1–4/21.

[8] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[9] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," IEEE Trans. Image Process., vol. 8, no. 1, pp. 58–68, Jan. 1999.

[10] E. Izquierdo, "Using invariant image features for synchronization in spread spectrum image watermarking," in EURASIP J. Appl. Signal Process., vol. 4, 2002, pp. 410–417.

[11] C. Rey and J. L. Dujelay, "Blind detection of malicious alterations on still images using robust watermarks," in Proc. IEE Secure Images and Image Authentication Colloquium, London, U.K., Apr. 2000, pp.7/1-7/6.

[12] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," in Proc. Int. Congress IPR for Specialized Information, Knowledge and New Technologies, Vienna, Austria, Aug. 1995, pp.242–251.

[13] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," IEEE Trans. Image Process., vol. 9, no. 3, pp. 432–441, Mar. 2000.

[14] P.W.Wong and N. Memon, "Secret and public key image watermarking schemes of image authentication and ownership verification," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[15] O. B. Adamo, Saraju P. Mohanty, E. Kougianos, and M. Varanasi, "VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Camera," Proc. In IEEE International Conference SOC, pp. 141-144, 2006.

[16] G. A. Carpenter, S. Grossberg, and D. B. Rosen, "Fuzzy ART: An adaptive resonance algorithm for rapid, stable classification of analog patterns," in Proc. Int. Joint Conf. Neural Networks, 1991, pp. 411–416.