ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 3, June 2012

Blind and Robust Watermarking for Self-Authentication of Images Using Integer Wavelet Transform

G.Himaja, B.Mala Konda Reddy, K.V. Phani Raju

***Abstract*— A robust watermarking scheme is proposed for self-authentication of images based on second-generation wavelets (lifting- based integer wavelet transforms). Procedures that can recover the hidden mark without the use of the original unmarked data are defined as blind decoding. The process of watermarking is carried out by comparing the adjacent coefficients in the LL1 band. The scheme has the capability of providing both robustness and self-authentication of the watermarked images. The watermarking scheme gives peak signal to noise ratio (PSNR) in excess of 45dB due to the use of integer-to-integer transform. The experimental results show that the watermark embedded with the proposed algorithm is robust and self-authenticated under different attacks such as compression, filtering and rotation.**

***Index Terms*— Integer wavelet transform, blind watermarking self authentication, lifting scheme**.

I. INTRODUCTION

Digital watermarking, or data hiding, a more general alternative term, is a process to hide data into cover media such as images, audio clips or video streams. It can be used as a way to transport information secretly or to protect the integrality of the cover medium itself. Digital image watermarking can be visible or invisible. In the case of invisible digital watermarking, no visual artifact is expected in the marked ones (which are referred to as stego-images as well). Although the difference between a stego-image and its original one is imperceptible by human eyes, the stego-images are different to the original ones because of the manipulations exerted to the original image during the watermark embedding process. However, in some scenarios, for example, satellite images or medical images, the original ones are so precious or subtle that people wish the original pictures can be recovered without any distortion after the hidden data have been extracted.

Manuscript received June 2,2012.

G.Himaja, *Electronics and communication Engineering, JNTU,Kakinada/ BVSR Engineering College, (e-mail: himajaratnam@gamil.com). Ongole, India, 9985780137*

B.Mala Konda Reddy, *Electronics and communication Engineering, JNTU,Kakinada/ BVSR Engineering College, Ongole, India, 9492338958(e-mail: bmalakondareddy@gmail.com).*

K.V. Phani Raju *Electronics and communication Engineering, JNTU,Kakinada/ BVSR Engineering College, Ongole, India, 9704771004 (e-mail: venkata.phaniraju75@gmail.com).*

Wavelet transform has been commonly used to embed watermark in images [1–4]. Watermark can be added in the selected wavelet coefficients by quantization [1], but it does not consider the human visual system since all the sub-bands are watermarked, due to which perceptible distortion occurs in the watermarked images. Maximum likelihood detection scheme by modeling the discrete wavelet transform coefficients using the Laplacian probability density function has also been considered [2]. A new modulation scheme was proposed [5, 6], which uses half of the watermark positively embedded and the other half negatively, but thei design does not include the security issues and geometric attacks. Recently, lifting-based second-generation wavelet transforms have been proposed by Sweldens [7]. The lifting scheme requires three phases for its implementation, namely: split phase, predict phase and update phase. The 5/3 filter bank is an important class of biorthogonal filter where all filters have finite impulse response and linear phase. The 5/3 filter bank also belongs to a special class of integer-to- integer filter banks that maps integers to integers, allowing exact recovery of input signal by avoiding rounding off errors. This property makes the 5/3 filter bank an ideal choice for lossless compression in the JPEG2000 standard [11]. The structure of 5/3 filter bank is relatively simple as a result prediction and update steps for this filter bank are straight forward. Due to its property of integer-to-integer transformation, it has recently being used for image watermarking applications [8–11].

II. PROPOSED IMAGE WATERMARKING SCHEME

In this scheme the host image is processed using 2-level 5/3 integer wavelet transform (IWT) to get the integer coefficients. The watermark image is embedded in LL1 sub-band (shown in Fig. 1); because the perceptual distortion at low frequencies is less and hence strong watermark can be embed [11]. After watermark embedding, we have to perform the inverse IWT.

In the watermark extraction process, first the watermarked image is processed using the 2-level 5/3 IWT. Then the watermark image is extracted from the LL1 sub-band (shown in Fig. 2).Finally the cross correlation and the normalized cross correlation is calculated between original watermark image and extracted watermark image.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 3, June 2012

A) Watermark embedding

Let $O_{x,y}$, original host image and $W_{x,y}$, be the watermarked image pixel intensity, respectively. $C_{x,y}$, and $C1_{x,y}$ be the wavelet coefficient before and after embedding, i.e. in the LL1 sub-band. Let the black and white watermark image be W_i, and its size is [m, n].
The W_i is converted into a vector of [1, m*n]

$$W\_em = [w_1, w2 \ldots w_k], \quad k = m*n$$

The watermark embedding involves the following steps

1) If W_em(k)=1, check $C_{x,y} > C_{x,y+1}$. If the condition is correct then,

$$C1_{x,y} = C_{x,y}$$
$$C1_{x,y+1} = C_{x,y+1}$$
Else
$$C1_{x,y} = C_{x,y} + \alpha$$
$$C1_{x,y+1} = C_{x,y+1}$$

Here α is minimum allowable difference the adjacent coefficients in LL1 band.

2) If W_em(k)=0, check $C_{x,y} > C_{x,y+1}$. If the condition is correct then,

$$C1_{x,y} = C_{x,y}$$
$$C1_{x,y+1} = C_{x,y+1} + \alpha$$
Else
$$C1_{x,y} = C_{x,y}$$
$$C1_{x,y+1} = C_{x,y+1}$$

An advantage of using the above method is less degradation in perceptual quality due to its small change in the transformed coefficient values. Finally applying inverse 2-level IWT, the watermarked image with modified pixel intensity $W_{x,y}$ is generated as shown in Fig. 1.

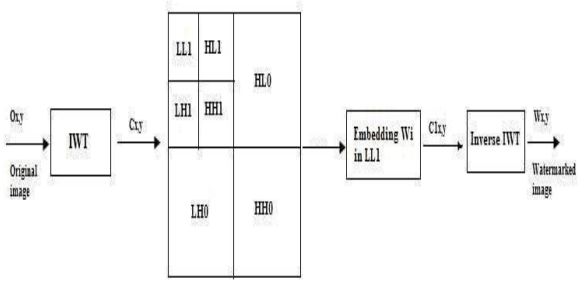

Fig.1. Scheme for embedding watermark

B) Watermark extraction

The watermarked image $W_{x,y}$ is first decomposed by 2-levels using 5/3 IWT and coefficients ($C2_{x,y}$) are obtained. Let W_ex be the extracted watermark vector of size [1, m*n].

The watermark extraction process is also carried out in LL1 band as follows

If $C2x,y > C2_{x,y+1}$
W_ex(k) = 1
Else
W_ex(k) = 0; k=1,2…..m*n

Now the correlation between embedded watermark vector and extracted watermark vector is calculated, it is denoted by χ, which is known as Authentication-Cum-Robustness function.

$$\chi = W\_em \ominus W\_ex$$

Where Θ denotes the correlation value between W_em and W_ex. If it is equal o 1 then the image is self- authenticated. For robustness measure of the pro- posed watermarking scheme, different tests were carried out and the results are discussed in the next section. A normalized cross-correlation coefficient (NCC) is also calculated between W_em and W_ex. The extracted watermark image can be displayed by converting the vector W_ex to a matrix of [m, n]

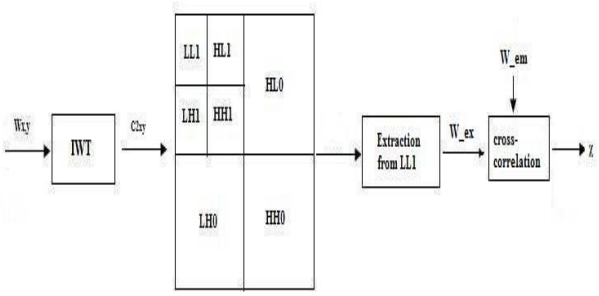

Fig.2. Scheme for image watermark extraction

III. RESULTS

The proposed scheme has been tested using the following values. The host image is the Lena image (256 × 256) and the watermark image is of 32 × 32, shown in fig.3 (a) and 3(b). Here α is taken as 10;

(a) (b)

Fig.3(a).Original host image;3(b). original watermark image

The host image is processed using 2-level 5/3 integer wavelet transform (IWT), shown in fig.4 and the image after watermark embedding is shown in fig.5.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 3, June 2012

Fig.4. 2-level IWT of host image

Fig.5. Host image after watermark embedding

The Peak-Signal-To-Noise Ratio (PSNR) is calculated between the original and watermarked host images. By using this scheme we can get the PSNR in excess of 45dB. Different attacks were applied on to the watermarked image. The following fig.6 shows the extracted watermark images after different attacks.

	
JPEG 75%	**Noise variance**
	
Rotation	**Mean filter**
	
Median filter	**Cropping**

Fig.6. Extracted watermarks after attacks

The Cross correlation and the NCC factors are calculated between original and extracted watermark vectors. These are listed in the following Table.1 for various attacks,

Attack types	Robustness Attacks	χ	NCC
JPE G	75	0.9464	0.9735
Noise variance	0.01	0.91	0.9694
Rotation	0.25°	0.7357	0.8215
Mean filter	3*3	0.9241	0.5204
Median filter	3*3	0.9241	0.5204
Cropping	1%	0.7039	0.397

Table1. Results for Robustness and NCC

The goal of our project is to develop a watermarking scheme for robustness and self-authentication that can withstand a certain degree of image compression and resist a series of attacks. The above result shows that the proposed scheme can sustain the attacks more efficiently as compared to the Amit Bohra scheme [11].

IV. CONCLUSION

In this paper, a blind robust watermarking is proposed with self-authentication capability. It uses IWT, which requires less computation as compared to techniques based on conventional discrete wavelet transform. The main advantage of this scheme is its self-authentication capability along with robust watermarking while maintaining high perceptual quality. From the results obtained it is evident that the proposed scheme can resist the attacks efficiently.

REFERENCES

[1] Kundur D, Hatzinakos D. Towards a telltale watermark techniques for tamper-proofing. Proc IEEE Int Conf Image Process 1998;2:409–13.
[2] Ng TM, Garg HK. Maximum-likelihood detection in dwt domain image watermarking using Laplacian modeling. IEEE Signal Process Lett 2005;12(4):285–8.
[3] Bao P, Xiaohu M. Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans Circuits Syst Video Technol 2005;15(1):96–102.
[4] Vizireanu DN, Preda, RO. A new digital watermarking scheme for image copyright protection using wavelet packets. In: 7th international conference on telecommunications in modern satellite, cable and broadcasting services, vol. 2, 2005. p. 518–21.
[5] Lu CS, Liao, HY. Oblivious cocktail watermarking by sparse code shrinkage: a regional and global-based scheme. In: Proceedings of international conference on image processing proceedings, vol. 3, 1987. p. 13–6.
[6] Lu CS, HYL, Sze CJ. Combined watermarking for image authentication and protection. In: Proceedings of IEEE international conference on multimedia and expo, vol. 3, 2000. p. 1415–8.
[7] Sweldens W. The lifting scheme: a construction of second generation wavelets. SIAM J Math Anal 1998;29(2):511–46.
[8] Yuan Y, H D, Liu D. An integer wavelet based multiple logo-watermarking scheme. In: 1st international multi-symposiums on computer and computational sciences, vol. 2, 2006. p. 175–9.
[9] Xiaoyun W, Junquan H, G Z, Jiwu H. A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters. In: Proceedings of the conference Australasian information security workshop, vol. 44, 2005. p. 75–80.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 3, June 2012

[10] Liu HM, Liu JF, JWHDRH, Shi YQ. A robust dwt-based blind data hiding algorithm. Proc IEEE Circuits Syst 2002;2: 672–5.
[11]Amit Bohra, OmarFarooq, Izharuddin. Blind self-authentication ofimages for robust watermarking using integer wavelet transform. Int. J. Electron. Commun. (AEÜ) 63 (2009) 703–707