Robust Digital Image Watermarking based on spread spectrum and convolutional coding

TABA Mohamed Tahar[1], BEDDA Mouldi[2], H.D.AL-Sharari[2]
[1]*LAIG Laboratory, Guelma University, Algeria,*
[2] *College of engineering, Al JOUF University, KSA.*

Abstract: *Digital watermarking is a promising technology to embed information as unperceivable signals in digital contents. A copyright protection method for digital image with convolutional coding is proposed in this paper. In this method, the watermark logo is coded with convolutional encoder and fused with noise bits to improve the robustness to malicious attacks including JPEG, noise and geometric attacks such as, cropping and rotation. During extraction, the watermark bits are decoded by Viterbi algotithm decoder, and the extraction procedure needs neither the original image nor the watermark logo. Simulation results show that the proposed method based on the convolutional coding can effectively resist the common malicious attacks, the embedding and extraction performances are quite improve compared to the method based on the direct coding.*

Keywords: *Digital Watermarking, Spread Spectrum, Convolutional Coding,*

I. Introduction

The Internet has brought convenience and innovation. Most users use it to exchange information. The proliferation of digitized media (audio, image, and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid key holders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Therefore, conventional cryptography provides little protection against data piracy, in which a publisher is confronted with unauthorized reproduction of information. Owing to publicity about intellectual property rights, many researchers are aware of the issues of copyright protection, image authentication, proof of ownership, etc; hence, there are many solutions that have been proposed. The watermarking technique is one of these solutions.

A digital watermark is a sequence of characters or code embedded in a digital document, image, video or computer program to uniquely identify its originator and authorized user. This technique embeds information so that it is not easily perceptible; that is, the viewer cannot see any information embedded in the contents...
There are several important essential properties in the watermarking system [1]. First is transparency. The embedded watermark should not degrade the quality of the image and should be perceptually invisible to maintain its protective secrecy. Second is robustness. The watermark must be robust enough to resist common image processing attacks and geometric attacks, and must not be easily removable. Third is security. Only the owner of the image is able to extract the watermark. Fourth is clarity. The identification of the owner of the image cannot be ambiguous. Fifth is blind reproducibility. It may only need secrecy keys [2], or even need neither the original image nor original watermark for extraction.

Many watermarking methods have been proposed [3, 4, 5]. Embedded the watermark into the perceptually significant portion of the whole DCT-transformed image wherein a predetermined range of low frequency components excludes the DC component.

Convolutional coding and viterbi decoding is a Forward Error Correction (FEC) technique to compensate signal loss in wireless communications since wireless communications, which, usually, are with higher packet loss rates and lower transmission rates, are more unreliable than transmissions by wire communications. The convolutional coding adds the redundant information to the signal in a transmission to achieve the objective of error correction and high reliability, and the receiver subsequently uses viterbi decoding to decide the value of the bit which has been transmitted..

In this paper, we propose a watermark protection scheme based on convolutional coding with rate 1/2 for resisting malicious attacks [6, 7]. The watermark logo is spread over the entire image by CDMA spread spectrum techniques [8, 9].
CDMA spread-spectrum techniques is used to scatter the bits randomly throughout the cover image, that can enhance the resistance to attacks. The watermark is transformed from 2D to 1D. For each value of the watermark, a PN sequence is generated using an independent seed. The summation of all of these PN sequences represents the watermark, which is added to the cover image [3**].**

To retrieve the watermark, the same PN generator algorithm is seeded, the correlation with the entire image is computed . If the correlation is high than a threshold, that bit in the watermark is set to “0”, otherwise is set to “1”. The process is then repeated for all the values of the watermark.

This paper is organized as follows: the image protection and verification using the convolutional coding watermark is described in Section 2. The simulation results are given in Section 3. Finally, the conclusions are summed up in Section 4.

II. The Proposed Method (Co-Watermarked)

2.1 Definition:

Spread spectrum (**SS**) communication technologies have been developed since the 1950s in an attempt to provide means of low-probability-of-intercept and anti-jamming communications. Spread Spectrum technique is defined as means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery. Although the power of the signal to be transmitted can be large, the signal-to-noise ratio in every frequency band will be small. Even if parts of the signal could be removed in several frequency bands, enough information should be present in the other bands to recover the signal. Thus, **SS** makes it difficult to detect and/or remove a signal. This situation is very similar to a watermarking system which tries to spread a secret message over a cover image in order to make it impossible to perceive. Since spread signals tend to be difficult to detect and remove. Embedding methods based on Spread Spectrum should provide a considerable level of robustness [10].

The message to be transmitted is first encoded by convolutional encoder Fig.1. This step typically takes a binary input stream and translates it into a binary output stream; the watermark logo is encoded with convolutional encoder with rate 1/2, [6, 7].

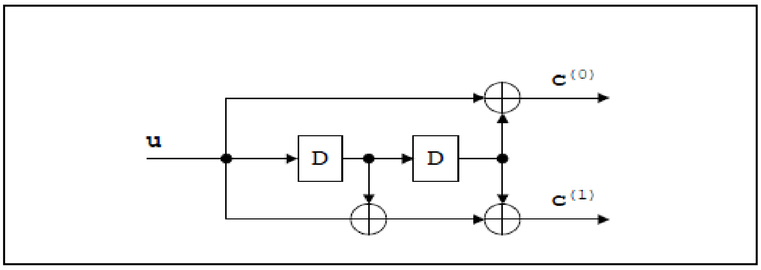


Figure 1. Rate r=1/2 convolutional encoder [6]

The output stream $\boldsymbol{c}^{(j)}$ is found by convolving the input stream $\boldsymbol{u}$ with a generator sequence $\boldsymbol{g}^{(j)}$ as follows:

$$\boldsymbol{C}^{(j)} = \boldsymbol{u} * \boldsymbol{g}^{(j)} \qquad \textbf{(1)}$$

Where the $\boldsymbol{l}^{th}$ element of the output vector is

$$\boldsymbol{C}_{l}^{(j)} = \sum_{k=0}^{m} \boldsymbol{u}_{l-k}\, \boldsymbol{g}_{k}^{(j)} \qquad \textbf{(2)}$$

This step will increase the robustness of the overall watermarking application. The resulting encoded message is then modulated by a pseudorandom sequence produced by a pseudorandom number generator using *a secret key* as seed [3]. The resulting random-looking signal is then added to the cover image **Fig.2.**

The receiver demodulates the noisy signal to a possibly corrupted encoded message. Finally, this message is decoded by the Viterbi decoder to produce the received message [6, 7].

In order to raise secrecy and confusion of a watermark, and to make the embedded information more difficult to be detected by attackers, convolutional coding and CDMA are used. The proposed watermarking scheme is robust for application in copyright protection. The detailed description of the algorithm for the image protection and verification is stated as follows.

2.2 Watermark embedding

The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudorandom noise pattern to the luminance values of its pixels. Many methods are based on this principle [3],

[4], [10]. In general, the pseudorandom noise pattern consists of the integers {-1, 0, 1}. The pattern is generated based on a key using seeds or linear shift registers.

The only constraints are that the energy in the pattern is more or less uniformly distributed and that the pattern is not correlated with the host image content. To create the watermarked image ***Iw(x,y),*** the pseudorandom pattern ***W(x, y)*** is multiplied by a small gain factor ***k*** and added to the host image ***I(x, y)***, as illustrated in **Fig. 3**

$\boldsymbol{I_w(x,y) = I(x,y) + k * W(x,y)}$ ***(3)***

We generate the protection key through the encoded watermark logo $\boldsymbol{C^{(j)}}$ fused with the noise bits which gives ***W(x,y)*** (**Fig.3**).

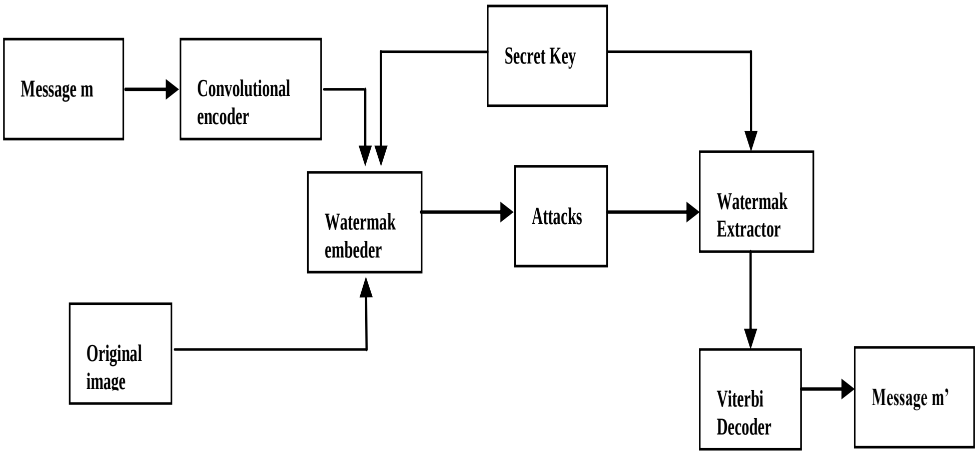


Figure.2. Convolutional Spread spectrum watermarking model

The process of convolutional encoding the message and then watermarking it, we called co-watermarking (convolutional coding+ watermarking). In the equation (3), ***k*** represents the gain factor.

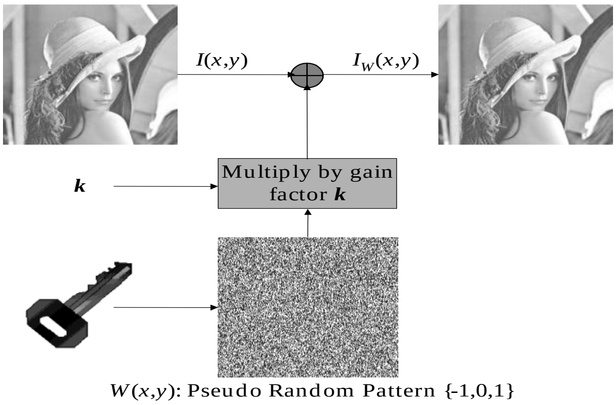

I(x,y)
I_W(x,y)
k
Multiply by gain factor k
W(x,y): Pseudo Random Pattern {-1,0,1}

Figure.3. Spread spectrum digital watermarking

2.3 Watermark detection

To detect the watermark**,** we calculate the correlation between the watermarked image ***I_w(x,y)*** and the pseudorandom noise pattern *W*(*x*, *y*). In general, ***W(x,y)*** is normalized to a zero mean Pseudorandom before correlation. Patterns generated using different keys have very low correlation with each other. Therefore, during the detection process the correlation value will be very high for a pseudorandom pattern generated with the correct key and would be very low otherwise. This is shown in **Fig. 4**, the correlation values of some pseudorandom patterns generated using seeds varying between 0 and 1000 to the watermarked image. It can be seen that the correlation is very high when the correct seed (100) is used, while the correlation was very low when the wrong seeds are used.

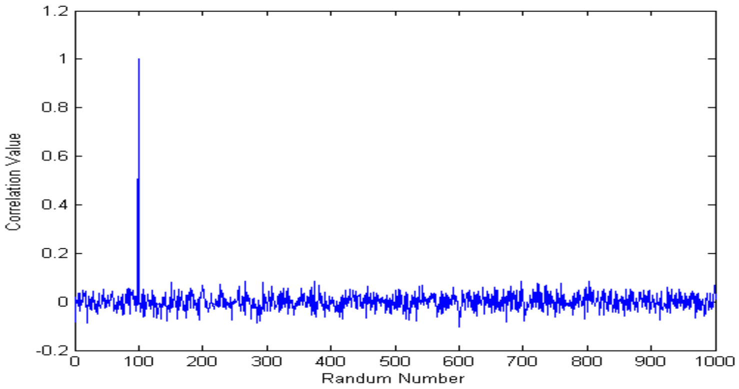


Figure 4. Watermark detector response to 1000 randomly generated watermarks. Only one watermark at 100 is detected

In Spread Spectrum watermarking scheme the detection of binary valued watermark data depends on the decision variable ***C_{ri}*** obtained by evaluating the correlation coefficient between the watermarked image ***Iw*** and the code pattern ***W***, which is generated through the secret key. The computation of ***C_{ri}*** is obtained*:*

$$c_{ri} = \frac{\sum_m \sum_n (I_w - \mu_w)(W - \mu_p)}{\sqrt{[\sum_m \sum_n (I_w - \mu_w)^2][\sum_m \sum_n (W - \mu_p)^2]}} \qquad \textbf{(4)}$$

Where μ_w = mean (I_w), and μ_p = mean (P).

During the detection process, it is common to set a threshold ***Tr*** to decide whether the watermark is detected or not. Correlation values are calculated between the watermarked image with the corresponding code pattern ***W***. Therefore, for each bit of message vector, a correlation value is obtained and we have ***Mw*** *correlation* values ***Cr_i***, where i=1,2, ..M_w. From these correlation values, we calculate an overall mean correlation value ***Tr*** **(eq. 1.5)** that is used as the threshold for watermark decoding (**Fig.5**).

$$T_r = \frac{1}{M_w} \sum_{i=0}^{W_H - 1} C_{ri} \qquad \textbf{(5)}$$

The decision rule for the decoded watermark bit is as follows: When Cri ≥ ***Tr***, the extracted bit is '**0**' and When Cri < ***Tr***, the extracted bit is '**1**'.

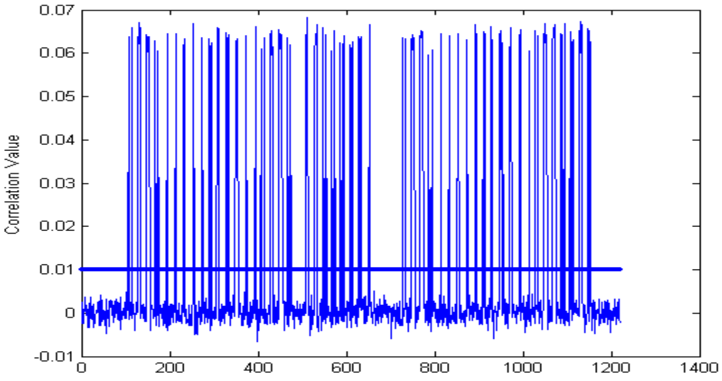


Figure 5 - Choice of Threshold by Mean

Value, for “LAIG LAB” logo In this case threshold T=0.01
In the verification process, no original image is needed. The extracted logo is then decoded by a Viterbi decoder [6,7]

III. Experimental Results and discussion

To evaluate the quality between an attacked image and the original image, we use the peak signal-to-noise ratio (PSNR). The PSNR is formulated as follows:

$$PSNR = 10 * log_{10} \frac{255*255}{\frac{1}{I_H I_W}\sum_{x=0}^{I_H-1}\sum_{y=0}^{I_W-1}[i(x,y)-i'(x,y)]^2} \qquad \textbf{(6)}$$

Where $\boldsymbol{I_H}$ and $\boldsymbol{I_W}$ are the height and width of the image, respectively, and i(x,y) and i'(x,y) are the gray level coefficients located at coordinate (x,y) of the original image ***I*** and the watermarked image ***I'***, respectively.
QAfter extracting the watermark, the **N**ormalized **C**orrelation **C**oefficient (**NC**) is computed using the original watermark and the extracted watermark to judge the existence of the watermark in order to measure its correctness. It is defined as follows:

$$NC = \frac{1}{W_H * W_w}\sum_{i=0}^{W_H-1}\sum_{j=0}^{W_w-1} W_{ij}\, W'_{ij} \qquad \textbf{(7)}$$

Where, W_H and W_W are the height and width of the watermark. $\boldsymbol{W_{i,j}}$ and $\boldsymbol{W'_{i,j}}$ are the values located at coordinate ***(i,j)*** of the original watermark ***W*** and the extracted watermark ***W'***. We use, in our experiments, the Lena image (512 x512 pixels, 8 bits/pixel) as cover image. The size of the binary watermark logo is 61x20 pixels **(Fig.6).**

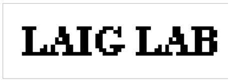
Cover image	Watermark logo
	

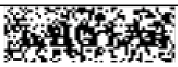
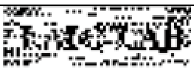
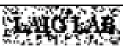
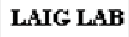
Fig.6. Cover image and watermark logo

To show the effectiveness of the proposed method (co- watermarked), a comparative experiments are conducted between the proposed method and the direct watermarked (Shoemaker [3])

In the following experiments we consider, in Tables 1 and 2, the impact of the gain factor *k* on the quality of the extracted watermark. It is remarkable that the quality of extracted logo is enhanced by the proposed method; the given proposed method with (PSNR= 26.5408 and k=0.5) is very closer to that given by the direct method with (PSNR=28.3007 and k =1)

The figure 7 shows the Normalized Correlation coefficient for "LAIG LAB" logo in function of Signal to Noise Ratio (SNR), we conclude that the proposed method is very robust against noise compared to the direct method(Shoemaker [3]), we have attained NC=1 for only SNR=5dB, since for the direct method, the watermark logo still undetectable ; also, we consider both geometric and non-geometric attacks. Non-geometric attacks include JPEG compression (Tables 3 and 4), JPEG is one of the most used formats in the Internet and digital cameras. The JPEG quality factor Q is a number between 1 and 100 and associates a numerical value with a particular compression level. When the quality factor is decreased from 100, the image compression is improved, but the quality of the resulting image is significantly reduced.
Tables 3 and 4, represents the results obtained with JPEG attack. The quality factor Q of the JPEG compression is set to 30 and 60, and the watermark logo "LAIG LAB" is extracted completely by proposed method.
In figure 8 and 9 , the variation of the normalized correlation coefficient (NC) function of JPEG compression for different values of Q , figure 8 (with out noise) and figure 9 (with noise SNR= 5dB).
The results obtained show the remarkable difference between the two methods, by the proposed method NC attains value 1 from Q=30, but for the direct method NC close to 1 at Q=90 for the case with out noise.
With noise the proposed method still considerably better than the direct method**.**
We also use other geometric attacks such as cropping combined with Gaussian noise (Table 5), and (Table 6) we use rotation attack with noise. The experimental results represented by figures 9, 10 and 11 show that the proposed method "Co-watermarking" outperforms the ones derived in [3,4]; the watermark logo can still be recognized clearly.

Table.1. Effect of Gain factor **k**

	Gain factor k=0.25 without noise		Gain factor k=0.5 without noise	
Method	watermarked Image	Co-watermarked Image	watermarked Image	Co-watermarked Image
PSNR	40.1884	32.5381	34.2994	26.5408
Extracted watermark				
NC	0.6177	0.7763	0.7296	1

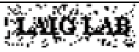
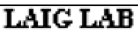
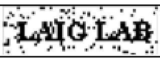
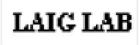
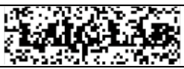
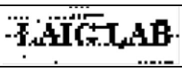
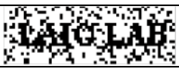
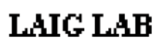
	Gain factor k=0.75 without noise		Gain factor k=1 without noise	
Method	watermarked Image	Co-watermarked Image	watermarked Image	Co-watermarked Image
PSNR	30.7833	23.0256	28.3007	20.5563
Extracted watermark				
NC	0.8307	1	0.8998	1

Table.2. Gain factor **k= 1** + Gaussian noise

	Gain factor k=1 + Noise snr=0 dB		Gain factor k=1 + Noise snr=5dB	
Method	watermarked Image	Co-watermarked Image	watermarked Image	Co-watermarked Image
PSNR	**5.5927**	**5.3767**	**10.5607**	**10.0890**
Extracted watermark				
NC	**0.6693**	**0.9416**	**0.7539**	**1**

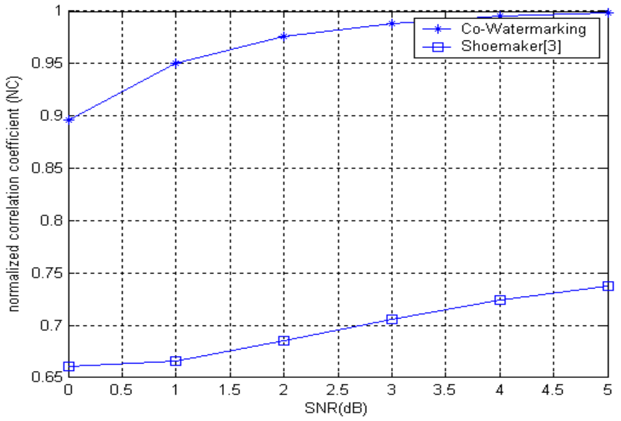


Figure 7. NC in function of SNR for "LAIG LAB" logo

Table 3: watermarking attack with JPEG compression: quality Q=30 and Q=60.

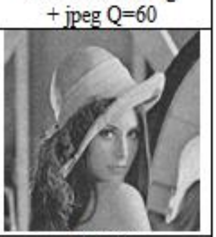
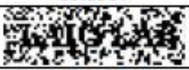
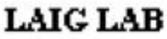
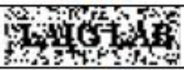
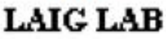
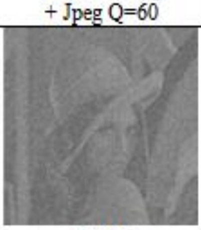
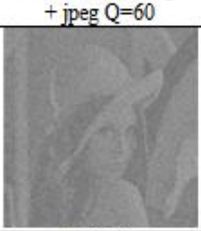
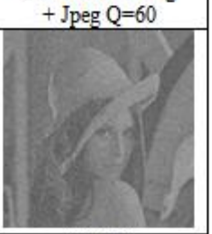
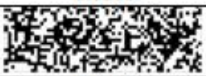
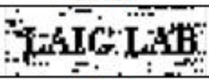
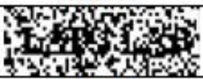
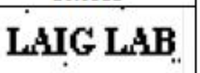
	Without noise		Without noise	
Method	Watermarking + Jpeg Q=30	Co-Watermarking + Jpeg Q=30	Watermarking + Jpeg Q=60	Co-watermarking + jpeg Q=60
				
PSNR	30.8357	22.2115	29.8578	20.0563
Extracted watermark				
NC	0.6391	1	0.7140	1

Table 4: watermarking attack with JPEG + Noise

	With noise SNR= 0 dB		With noise SNR= 5 dB	
Method	Watermarking + Jpeg Q=60	Co-watermarking + jpeg Q=60	Watermarking + Jpeg Q=60	Co-Watermarking + Jpeg Q=60
				
PSNR	5.6205	5.3623	10.5801	10.0511
Extracted watermark				
NC	0.5759	0.8920	0.6255	0.9951

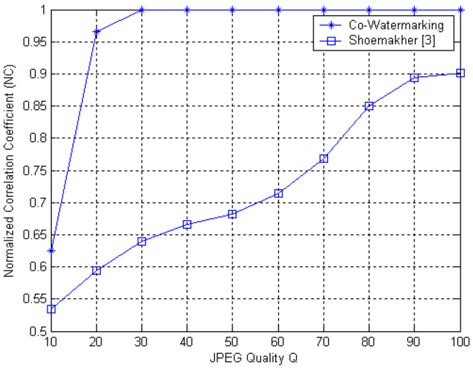


Figure 8. Normalized Correlation Coefficient in function JPEG quality without noise

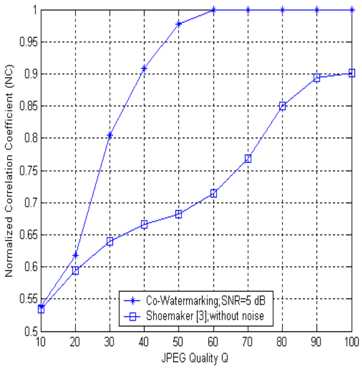


Figure 9. Normalized Correlation Coefficient in function JPEG quality with noise(SNR=5 dB) for co-watermarking only

Table 5: watermarking attack with cropping+Noise

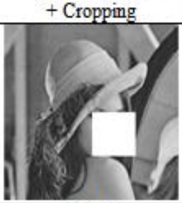
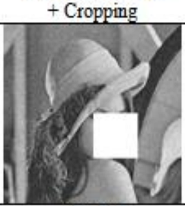
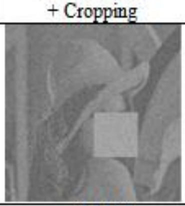
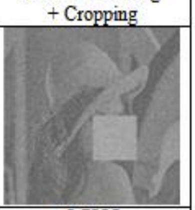
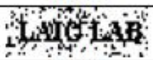
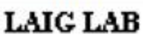
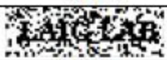
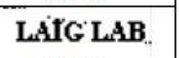
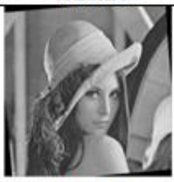
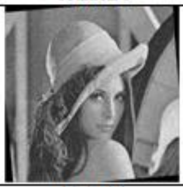
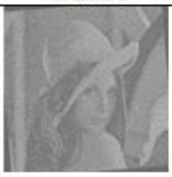
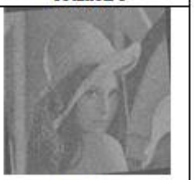
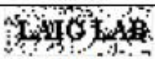
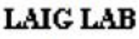
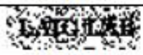
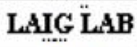
	Without noise		With Gaussian noise : SNR=5dB	
Method	Watermarking + Cropping	Co-watermarking + Cropping	Watermarking + Cropping	Co-watermarking + Cropping
				
PSNR	16.7351	15.5173	9.0899	8.7885
Extracted watermark				
NC	0.8395	1	0.6926	0.9874

Table 6: watermarking attack with rotation 5°

	Without noise		With Gaussian noise : SNR=5dB	
Method	Watermarking + rotation 5°	CO-watermarking + rotation 5°	Watermarking + rotation 5°	CO-watermarking + rotation 5°
				
PSNR	19.9333	17.6486	10.2691	9.8516
Extracted watermark				
NC	0.8385	1	0.7160	0.9922

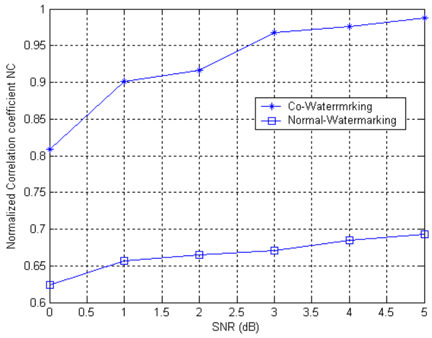


Figure 10. Normalized Correlation Coefficient in function of SNR for cropping attack

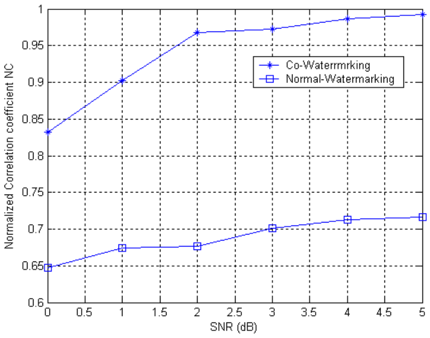


Figure.11. Normalized Correlation Coefficient in function of SNR for 5 degree rotation attack.

IV. Conclusion

In this paper, the simulation shows that the result given by proposed method “convolutional spread spectrum watermarking” is considerably better then that given by the direct method , also the proposed method is robust against the common attacks, and is also strong enough to resist the geometric attacks and noise by the combination of spread spectrum and convolutional coding where the polynomial for convolutional coding and the code for generating PN code are unknown, while the retrieval watermark logo is still recognizable.

The main limitations of spread spectrum co-watermarking in the spatial domain remain on its limited capacity.

References

[1] Wei-Hung Lin a et al, “Image copyright protection with forward error correction”, Expert Systems with Applications: An International Journal. Vol. 36 Issue 9, November, 2009.

[2] Ganic, E., & Eskicioglu, A. M. (2004). “Robust DWT-SVD domain image watermarking: Embedding data in all frequencies”. In Proceedings of the international multimedia conference multimedia and security, Magdeburg (pp. 166–174).

[3] Chris Shoemaker “Hidden Bits: A Survey of Techniques for Digital atermarking”. Available: http://www.vu.union.edu/~shoemakc/, June 2011.

[4] Langelaar, G. C., Setyawa, I., and Lagendijk, R. L. “Watermarking digital image and video data: A state-of-the-art overview”. IEEE Signal Processing Magazine, vol.17, pp 20-46. September 2000.

[5] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). “Secure spread spectrum watermarking for multimedia”. IEEE Transactions on Image Processing, 6,1673–1687.

[6] Matthew C. Valenti, “Channel coding for IEEE 802.16e mobile WiMAX,” roceedings of IEEE International Conference on Communications, ICC 2009, Dresden, Germany, 14-18 June 2009.

[7] http://www.iterativesolutions.com/, 0ctober 2011.

[8] Luis Pérez-Freire and Fernando Pérez-González Spread, “Spread spectrum watermarking security”. *IEEE Transactions on Information Forensics and Security*, 4(1):2-24, March 2009.

[9] F. Cayre, C. Fontaine, and T. Furon, “Watermarking security: theory and practice,” *IEEE Transactions on Signal Processing*, vol. 53, no. 10, October 2005.

[10] Stefan Katzenbeisser, Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, 2000, ARTECH HOUSE, INC.