Journal of Signal and Image Processing
ISSN: 0976-8882 & E-ISSN: 0976-8890, Vol. 2, Issue 2, 2011, pp-36-41
Available online at http://www.bioinfo.in/contents.php?id=48

A DWT BASED MULTI LEVEL DIGITAL WATERMARKING TECHNIQUE FOR IMAGES

RAHUL PATHAK[1], ABHISHEK KATARIYA[1], TOMAR G.S.[2] AND PRAJAPAT K.K.[1]
1Department of Electronics & Comm. Engineering, Sri Balaji College of Engg. & Tech., Jaipur (Raj.), India
2Director, MIR Lab, Gwalior (M.P.), India
*Corresponding author. E-mail: rahul_vn_pathak@yahoo.co.in, abhishek_katariya@rediffmail.com, gstomar@ieee.org, kkprajapat2004@rediffmail.com

Received: August 24, 2011; Accepted: September 20, 2011

Abstract—The digital watermarking of still images based on the concept of multiresolution wavelet fusion is proposed. The proposed method for the digital watermarking is based on the two-dimensional discrete wavelet transform. It decomposes original image in DWT domain in to three hierarchical levels and watermarks it with a logo image. The watermark is added to the DWT image according to a certain threshold. The proposed approach embeds a meaningful data in form of a logo image instead of a pseudo-random number sequence, called as image-fusion watermarking. This approach show that a watermark signal can be embedded in high-pass wavelet coefficients without any impact on the image visual fidelity. The results prove that the proposed scheme has an efficient performance in terms of robustness to a variety of attacks.

Keywords—digital watermarking; discrete wavelet transform; pseudo-random number sequence; image-fusion watermarking; high-pass wavelet coefficient

Introduction

Digital contents in the form of text document, still image, motion picture, and music etc. are widely used in our normal life nowadays. Rapidly growing field of digitized images, video and audio has urged for the need of copyright protection, which can be used to produce evidence against any illegal attempt to either reproduce the digital media or to manipulate them in order to change the very identity of them. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques.

Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

Ideal characteristics of a digital watermark have been stated [1]. These characteristics include:

1. Perceptual invisibility.
2. Statistical invisibility.
3. Fairly simple extraction should be.
4. Accurate detection.
5. Robustness to filtering, additive noise, compression, and other image manipulations.
6. Ability to determine the true owner of the image.

A lot of work is being conducted in different branches in this field. Steganography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper detection [2]. Among the two basic modalities for image watermarking encoding: spatial domain techniques and frequency domain techniques, most of the spatial watermarking schemes provide simple and effective ways for embedding an invisible watermark into the cover image, but they are usually not robust to common image alternations. Casting watermarks in the frequency domain can provide more protection under most signal processing and high ratio compression attacks.

In this paper, a new technique for the digital watermarking of still images based on the concept of two-dimensional discrete wavelet transform is intended. It decomposes original image into three hierarchical levels of DWT domain with the Haar wavelet filter, and watermarks it with a logo image instead of a pseudo-random number sequence. This is unlike most previous work, which used a random number of a sequence of bits as a watermark and where the watermark can only be detected by comparing an experimental threshold value to determine whether a sequence of random signals is the watermark. The logo image, generally smaller than the host image, is put into the high frequency band of the host image which has been wavelet transformed.

There are two important advantages of embedding a logo image as watermark data. First, the extracted image can be correlated with the originally embedded image by a human observer, building on the superior pattern-matching capabilities of the human brain. Second, the existence of a visual logo in the questionable image might be much better proof of ownership than a high statistical correlation value.

In this method, embedding can be applied to HL, LH, HH sub-bands at all levels of decomposition and to LL detail at the third level. Thus if a particular kind of noise affects a particular frequency band, then the watermark can be extracted from other sub-band.

Investigation on performances of the proposed technique for the digital watermarking of still images in terms of robustness to a variety of attacks, such as JPEG compression, blurring attack, deblurring attack, rotation by 4 degrees, average filter, salt n pepper noise, and AWGN noise attack has been studied. Experiments show that the corresponding watermark can still be correctly identified at each possible resolution in the wavelet domain.

In the following, we describe the DWT and the proposed watermarking method in detail. One of the main advantages of the discrete wavelet transform (DWT) is to describe more accurately aspects of human vision system (HVS) as compared to DFT and DCT. Therefore, it is imperative to study watermarking schemes in the wavelet transform domain.

WATERMARKING IN THE WAVELET DOMAIN

Transform domain watermarking techniques apply some invertible transform to the host image before embedding the watermark. Then, the transform domain coefficients are modified to embed the watermark and finally the inverse transform is applied to obtain the marked image. The transforms commonly used for watermarking purposes are the discrete cosine transform (DCT), the discrete Fourier transform (DFT), the fractal transform and the discrete wavelet transform (DWT) but there are also approaches dealing with more "exotic" transforms such as the Fresnel transform, the complex wavelet transform (CWT), the Fourier-Mellin transform and others.

Transform domain watermarking algorithms possess a number of desirable properties. Since the watermark embedded in the transform domain is irregularly distributed over the area of local support after the inverse transformation, these methods make it more difficult for an attacker read or modify the mark. For watermarking strategies that depend on the global DCT this means the watermark is spread over the entire image. The wavelet transform or a block-based DCT only affects the local region. Furthermore, the frequency representation of the images allows selecting only certain bands of the host signal for watermarking. The human visual system has been observed to process certain frequency bands individually which led to the development of visual models that try to capture these characteristics.

Algorithms operating in the frequency domain usually add the mark or its spread spectrum signal to a small subset of transform coefficients of the low or medium frequency range [3]. In spread spectrum techniques, a narrowband signal which represents the message to be transmitted is modulated by a broadband carrier signal, which broadens or spreads the original, narrow-band spectrum; hence termed as "spread spectrum".

The low- and mid-frequency components of the image data represent most of the perceptual important information. Therefore, compression schemes and other image processing operations can hardly affect this significant portion of the host image without destroying much of the visual content of the image. Thus, adding the watermark in significant coefficients of the transform domain generally improves robustness. Spatial domain watermarking methods have to indirectly model the low-frequency component of the host image signal, which can be quite complicate to achieve [4]. In the DCT domain, the energy concentrates in the low frequency regions around the upper-left corner. The multi-resolution DWT representation has the low frequency components of the image signal in the approximation sub-band, also located in the upper-left corner, while the high-frequency components are represented in the detail sub-bands at several resolutions. Most energy of the detail sub-bands is situated in edge areas and textured regions.

The main disadvantages of frequency transform domain techniques are their computational cost, and, in the case of a global transform, their problem to adapt the watermark strength to the local image activity, making it more difficult to exploit certain characteristics of the HVS such as masking effects. The later shortcoming can be resolved by using the wavelet transform which provides both, frequency and spatial information of the host image.

Finally, advantages of the DWT are [5, 6]:

1. The wavelet transform is a multi-resolution description of an image. The decoding can be processed sequentially from a low resolution to the higher resolutions.
2. The wavelet transform is closer to the human visual system (HVS) than the DCT, since it splits the signal into individual bands that can be processed independently. Hence, the artifacts introduced by wavelet domain coding with high compression ratio are less annoying than those introduced at the same bit rate by the DCT.
3. The high resolution sub-bands allow locating image features such as edges or textured area easily in the transform domain. Watermarking schemes often put more watermark energy into large DWT coefficients, thus affecting mostly regions, like edges and texture the HVS is not sensitive to.
4. Lower computational cost than the FFT or DCT.

THE PROPOSED WATERMARKING ALGORITHM

A. *Embedding Process*

The proposed wavelet based watermark embedding scheme is shown in fig. 1. The host image (*I*) is decomposed in DWT domain in to three hierarchical levels with a Haar filter. Let the resulting image be I_{DWT}, which is the combination of the 10 sub-bands (LL, HL, LH, HH).

The DWT coefficients, *f* having high entropy values are selected for each block in which the watermark is to be inserted. The number of DWT coefficients depends on total pixel in the watermark. The watermark is added in high value coefficients so that it spreads uniformly all over the image.

The logo image to be watermarked (*W*) is acquired and resized to 50x50 dimension. The signature data becomes a sequence ω_i of length 2500, that is embedded in a suitably selected subset of the DWT coefficients, *f*.

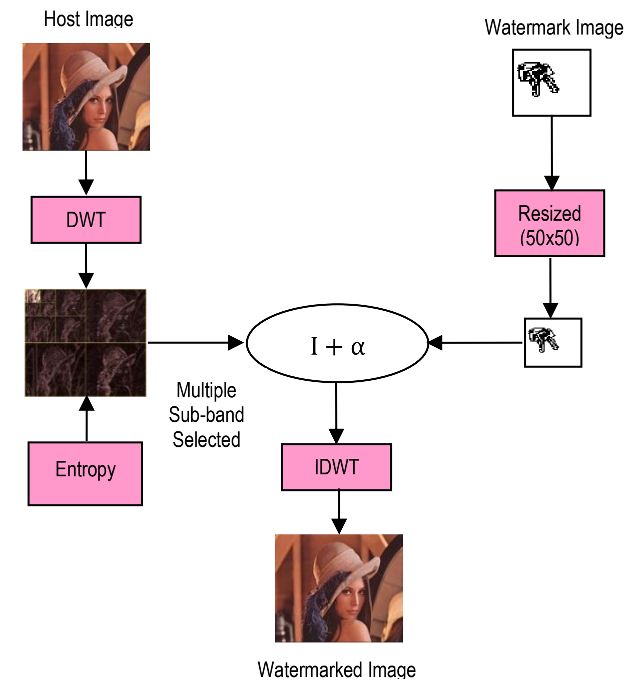

Figure 1. Watermark embedding process

Binary watermark image pixel is embedded by embedding formula:

$$f^{'}(m,n) = f(m,n) + \alpha \cdot \omega_i \qquad \text{when } \omega_i = 1 \quad (1)$$

$$f^{'}(m,n) = f(m,n) - \alpha \cdot \omega_i \qquad \text{otherwise} \quad (2)$$

Here α is weighting factor and is equal to 0.03.
In our method, embedding can be applied to HL, LH, and HH sub-bands at all levels of decomposition and to LL detail at the third level. Thus if a particular kind of noise affects a particular frequency band, then the watermark can be extracted from other sub-band.
The watermarked image is obtained by taking the inverse DWT.

B. *Detection Process*

To obtain the watermark (*W'*), the attacked image (*I'*) and the original image (*I*) is again subjected to third level DWT, resulting into 10 sub-bands (LL, HL, LH, HH).

$$\text{Let} \qquad Y = \text{DWT}(I) \qquad (3)$$

$$\text{and} \qquad Y = \text{DWT}(I') \qquad (4)$$

We subtract the same index of coefficients of sub-band of *Y* (for example LH3 or LH2), by the coefficients of sub-band of *Y'* for the length of watermark.

$$\omega^{'} = 1 \qquad if \qquad Y^{'}_{i(LH3)} - Y^{'}_{i(LH3)} > 0 \qquad (5)$$

$$\omega^{'} = 0 \qquad if \qquad Y^{'}_{i(LH3)} - Y^{'}_{i(LH3)} < 0 \qquad (6)$$

Thus, we obtain the extracted watermark *W'*. The proposed watermark extraction scheme is shown in fig. 2.

Here, the extracted watermark *W'* is a visually recognizable image. However, the subjective measurement is dependent on factors such as views. Therefore, we measure the similarity of original watermark *W* and extracted watermarks *W'* by the normalized correlation (NC) coefficient that is defined as

$$NC = \frac{\sum_i \sum_j \omega_{i,j} * \omega^{'}_{i,j}}{\sum_i \sum_j \omega^2_{i,j}} \qquad (7)$$

The NC belong [0,100]. The higher the NC values, the more similar the embedded watermark is to the extracted one.

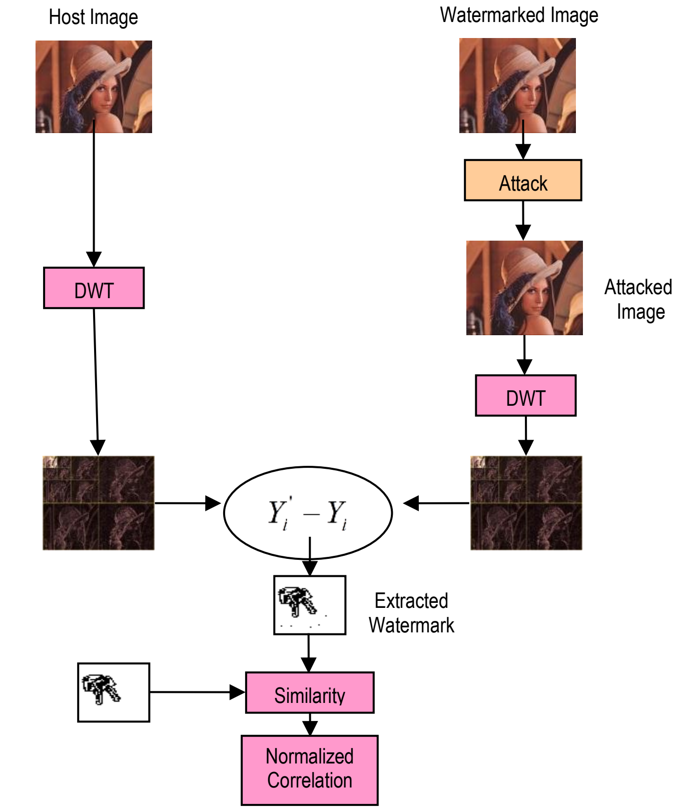

Figure 2. Watermark extraction process

PERFORMANCE EVALUATION

The proposed perceptual watermarking framework is implemented for evaluating both properties of imperceptibility and robustness in a high payload. The 512×512 grey scale Home image, shown in fig. 3 is taken as the host image to embed a 50×50 binary watermark image, shown in fig. 4. For the entire test results in this paper, MATLAB Version 7.0.0.19920 (R14) software is used. Also for computing the wavelet transforms, Haar wavelet is used. The reason for the use of Haar wavelet is that, it is the only known wavelet that is compactly supported, orthogonal and symmetric. Haar wavelets are basically same as Daubechies wavelet db1 (in MATLAB) or Daub4. The compact support of the Haar wavelets enables the Haar decomposition to have good time localization. Specifically, this means that the Haar coefficients are effective for the efficient representation of signals with small support.

The unattacked watermarked image is shown in fig. 5.

Figure 3. Grey scale Home image (host image)

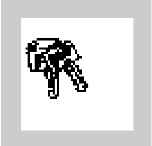

Figure 4. Watermark image

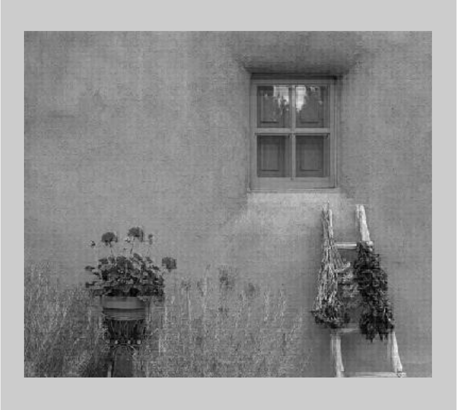

Figure 5. Watermarked image

In our method, embedding can be applied to HL, LH, HH sub-bands at all levels of decomposition and to LL detail at the third level. Here the horizontal sub-band HL at level two and three is represented by CH2 and CH3 respectively. Similarly, the vertical sub-band LH at level three is represented by CV3.

The peak signal-to-noise ratio (PSNR) was used to evaluate the quality of the watermarked image. The PSNR is defined as [6]:

$$PSNR = 10log_{10}\frac{255^2}{MSE}(dB) \qquad (8)$$

Mean-square error (MSE) is defined as:

$$MSE = \frac{1}{mn}\sum_{i-1}^{m}\sum_{j-1}^{n}(h_{i,j} - h'_{i,j})^2 \qquad (9)$$

Where $h_{i,j}$, and $h'_{i,j}$ are the gray levels of pixels in the host and watermarked images, respectively. The larger the PSNR is, the better the image quality is.

The proposed watermarking approach yields satisfactory results in watermark imperceptibility and robustness. The PSNR of the watermarked images produced by the proposed approach is 26.13 dBs, and NC between original watermark image and extracted watermark image is equal to 1. There is no perceptual distortion in the original and watermarked image, which means the scheme has satisfied the criteria that an efficient watermark should be unobtrusive, discreet and easily extracted.

In practice, a watermarked image may be attacked either on purpose or accidentally, so the watermarking system should still be able to detect and extract the watermark. Additive noise, filtering, cropping and compression are the best-known attacks of all attacks. Some of them may be intentional or unintentional, depending on the application. To test the robustness of the proposed algorithm to attacks, we attacked on purpose watermarked image by JPEG compression, additive noise, filtering, rotation, etc., and extracted the watermark image from corrupted watermarked image.

C. *JPEG Compression*

The Home image was watermarked under embedding algorithm then sent through the detector algorithm after JPEG compression. During JPEG compression image data will be lost which will affect the detector's ability to correctly detect the watermark. The image was compressed with quality of 100% to 10%. Hundred being the compressed image having a high quality to 10 being compressed image having a very low quality.

The calculated SNR and correlation coefficients between original watermark and watermarks extracted from various sub-bands with respect to JPEG compression quality factor are shown in Table I.

The extracted watermarks from various DWT sub-bands after JPEG compression are shown in fig. 6.

TABLE I. SNR AND NC AFTER JPEG COMPRESSION ATTACK

S. No.	JPEG Compression Ratio	SNR	NC of CH2	NC of CH3	NC of CV3
1.	Q.F – 100%	26.10	**100**	**100**	**100**
2.	Q.F –80%	24.70	**99.68**	**99.95**	**100**
3.	Q.F – 50%	23.50	88.97	**98.04**	**96.95**
4.	Q.F – 30%	22.82	63.46	**82.87**	**85.51**
5.	Q.F – 10%	21.19	18.82	33.94	39.36

Figure 6(a). Extracted watermarks for JPEG Q.F.=100%

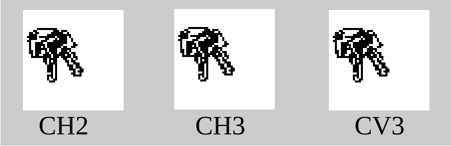

Figure 6(b). Extracted watermarks for JPEG Q.F.=80%

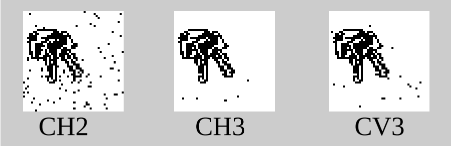

Figure 6(c). Extracted watermarks for JPEG Q.F.=50%

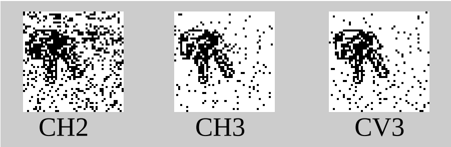

Figure 6(d). Extracted watermarks for JPEG Q.F.=30%

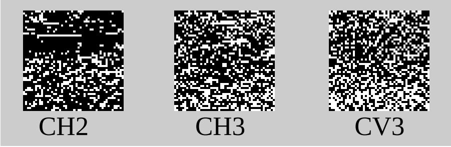

Figure 6(e). Extracted watermarks for JPEG Q.F.=10%

Fig. 7, 8, 9 and 10 show the watermark detection responses graphically.

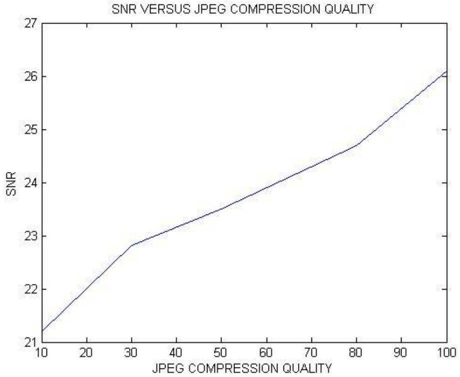

Figure 7. SNR versus JPEG compression Q.F.

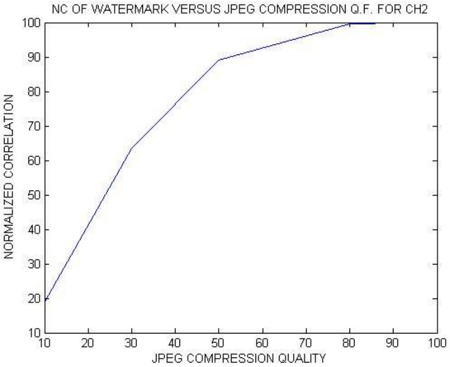

Figure 8. NC of extracted watermark from CH2 w.r.t. JPEG comp. Q.F.

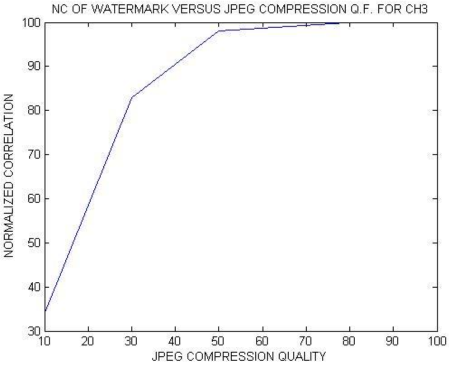

Figure 9. NC of extracted watermark from CH3 versus JPEG comp. Q.F.

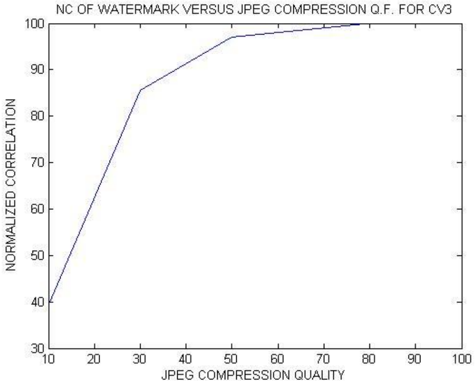

Figure 10. NC of extracted watermark from CV3 versus JPEG comp. Q.F.

D. ***Other Attacks***

The watermarked Home image was sent through the detector algorithm after blurring attack, deblurring attack, rotation by 4 degrees, average filter, salt n pepper noise, and AWGN noise attack. The results of the extracted watermarks are shown in Table II.

The extracted watermarks from various DWT sub-bands after various attacks are shown in the Fig. 11.

TABLE II. SNR AND NC AFTER VARIOUS ATTACKS

S. No.	Attacks	SNR	NC of CH2	NC of CH3	NC of CV3
1.	BLURRED	21.01	23.55	**85.74**	19.73
2.	DEBLURRED	24.68	**98.27**	**99.68**	88.79
3.	ROTATED 4 DEGREE	7.95	9.48	29.85	31.98
4.	AVG FILTERED	22.23	20.09	**84.10**	81.96
5.	SALT N PEPER NOISE	17.61	**92.89**	80.50	80.32
6.	AWGN NOISE	10.64	67.33	66.01	**68.25**

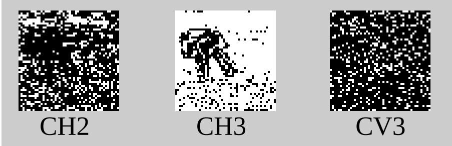

Figure 11(a). Extracted watermarks after blurring attack

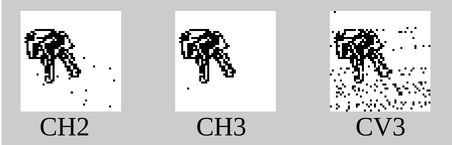

Figure 11(b). Extracted watermarks after deblurring attack

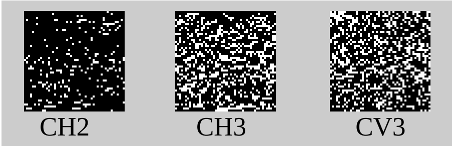

Figure 11(c). Extracted watermarks after rotation by 4 degrees

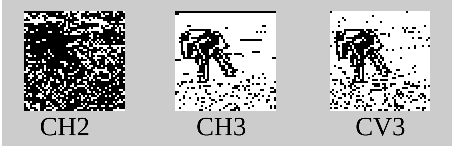

Figure 11(d). Extracted watermarks after average filtering

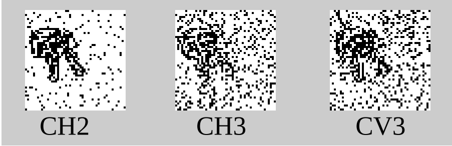

Figure 11(e). Extracted watermarks after salt n pepper noise attack

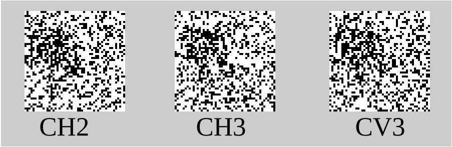

Figure 11(f). Extracted watermarks after AWGN noise attack

The NC between original watermark image and extracted watermark image indicates that the algorithm shows good performances against common signal processing procedures except rotation by 4 degrees.

CONCLUSION

The results shows that this technique can survive JPEG compression and is robust to a variety of other attacks, such as blurring attack, declaring, rotation by 4 degrees, average filter, salt n pepper noise, and AWGN noise attack.

Finally, by showing that the watermarked images are visually identical to their unmarked originals, experimental results have demonstrated the effectiveness of this approach. Therefore, the proposed technique shows excellent promise as it allows the authentication of digital images without preventing their efficient storage.

References

[1] Prasad Manjunatha and Koliwad Shivaprakash (2009) *International Journal of Computer Science and Network Security (IJCSNS),* vol.-9, no.-4, pp. 91-107.

[2] Cox Ingemar J., Miller Matthew L., Bloom Jeffrey A., Fridrich Jessica, and Kalker Ton (2008) *“Digital Watermarking and Steganography”, ISBN 978-0-12-372585-1, Morgan Kaufmann Publishers.*

[3] Cox Ingemar J., Kilian Joe, Leighton Tom, and Shamoon Talal G. (1997) *In Proceedings of the IEEE International Conference on Image Processing, ICIP ’97, vol.-6, pp. 1673-1687, Santa Barbara, California, USA, October .*

[4] Bruyndonckx O., Quisquater Jean-Jacques, and Macq Benoit M. (1995) *In Proceedings of the IEEE International Workshop on Nonlinear Signal and Image Processing, pp. 456- 459, Marmaras, Greece.*

[5] Dugad Rakesh, Ratakonda Krishna, and Ahuja Narendra (1998) *In Proceedings of the IEEE International Conference on Image Processing, ICIP ’98, Chicago, IL, USA.*

[6] Xia X.G., Boncelet C. G. and Arce G. R. (1998) *Optics Express*, pp. 497-511.