A New Robust Blind Copyright Protection Scheme Based on Visual Cryptography and Steerable Pyramid

Azz El Arab El Hossaini[1,2], Mohamed El Aroussi[2], Khadija Jamali[1,2], Samir Mbarki[1], and Mohammed Wahbi[2]

(Corresponding author: Azz El Arab El Hossaini)

Departement of Computer Science, Faculty of Science, Ibn Tofail University, Kenitra, Morocco[1]
Department of Electrical Engineering, Ecole Hassania des Travaux Publics[2]
BP 8108 Oasis-Casablanca, Morocco
(Email: azzelarab@live.fr)

(Received Jan. 31, 2014; revised and accepted Mar. 13 & May 20, 2014)

Abstract

In this paper, we proposed a novel blind digital image copyright protection scheme based on Steerable pyramid transform (SPT) and visual cryptography (VC). Unlike traditional watermarking schemes, the proposed method does not alter the original image by embedding the watermark image. Steerable pyramid transform is performed on the original image, and the low sub-band is selected. The watermark image is divided into two random looking images, called private and public shares using the visual secret sharing scheme and the selected low sub-band features. To reveal the watermark image, the two shares are stacked together while using each share separately reveals no information about the watermark image. A series of attacking experiments are performed on the original image to test the robustness of the proposed method. The experimental results show excellent visual imperceptibility and robustness against a variety of attacks.

Keywords: Copyright protection, robust blind watermarking, steerable pyramid transform, visual cryptography

1 Introduction

Nowadays, the transferring of digital media over the Internet becomes increasingly popular because of its inexpensiveness and efficiency. Moreover, the availability of powerful image processing tools has also made digital media manipulations much easier. These new technologies also bring in serious problems such as unauthorized reproduction and distribution of digital content. To overcome this inconvenient, it is very important for owners of digital content to protect themselves by securing their products to face all these problems. Digital watermarking [2, 30, 34] emerged as a solution for protecting the multimedia data.

By using digital watermarking technique, authors of the digital content can embed additional information called watermark into their digital product by modifying them unnoticeably, in order to protect them. Later authorized persons to prove ownership can extract the embedded information. The embedded watermark should not degrade the visual perception of the host image, and should be resistive to malicious attempts of removal as long as the digital content is still exploitable. A basic digital image watermarking technique consists of a host image, a watermark image, an embedding scheme, and an extraction scheme.

According to the domain in which the watermark is embedded, watermarking scheme could be divided into two categories: spatial domain techniques and frequency domain techniques. Spatial domain techniques [15, 20] are less complex and easy to implement, but they are not robust against various signal-processing attacks as no transform is used in them. In these the watermark is directly embedded into the host image by modifying the pixel values. Most of watermarking techniques proposed in the literature, embed the watermark image into the transform domain like discrete cosine transforms (DCT) [5, 12, 14, 22, 23], singular value decomposition (SVD) [3, 16, 18], discrete Fourier transforms (DFT) [17, 29], and discrete wavelet transforms (DWT) [8, 9, 21, 31]. These techniques provide enhanced imperceptibility and robustness compared to spatial domain techniques. This is due to the fact that the watermark image is irregularly distributed over the host image.

Perceptual transparency, payload of the watermark, robustness and security are the main characteristics to evaluate the performance of a watermarking scheme. (i) Perceptual transparency means that the host image and

the watermarked image cannot be distinguished based on human vision perception. (ii) Payload of the watermark is the amount of information that can be embedded in the host image. (iii) Robustness means that the watermark is resistive to manipulation of data, which may happen during transmission or storage phase. And finally, security refers to the ability to extract the right watermark by the right owner.

In traditional watermarking techniques, it's hard to satisfy all the previous characteristics. This can be achieved by adapting the concept of Visual Cryptography (VC) introduced by Naor and Shamir in 1995 [19]. VC is a simple but perfectly secure way, which uses the Human Visual System to decrypt the secret image without any cryptographic computation. It is described as a secret sharing scheme of digital image; the secret image is encrypted into random looking images called shares using a codebook. After printing these shares on transparencies, each participant gets one. In the decryption process, stacking all or some of the n shares reveals the secret image.

Watermark embedding schemes and watermark concealing schemes are the two categories of copyright protection schemes that we can find in the literature that are based in VC. In watermark embedding schemes, the watermark image is physically embedded into the host image while in the watermark concealing schemes, the watermark is not embedded physically and that could be useful to protect sensitive images since the original image is not altered.

Joo et al. [11] proposed a wavelet-based watermarking scheme that embeds a pseudo-random sequence into the low sub-band. The embedding occurs by selecting visually insensitive locations. During the extraction process, the original image is needed to extract the embedded watermark Hou and Chen [7] proposed a watermarking scheme based on the concept of visual cryptography proposed by Naor and Shamir [19]. The watermark image is divided into two shares. The first share is embedded into the host image by decreasing the gray levels of some specific pixels using a modified VC scheme. The original image and the second share are used during the extraction process. This watermarking method presents two drawbacks: first, it's not robust against geometric attack and second; the first share modifies the host image. Hsuetal. [10] proposed a copyright protection scheme based on VC and sampling distribution of means. The advantages of the proposed scheme are: the host image is not altered and the size of the watermark could be of any size.

In this paper, a novel blind digital image copyright protection scheme based on SPT and VC is presented. For watermark concealing, SPT is performed on the host image and the low sub-band is selected. Features of the selected low sub-band are extracted to construct a binary image using two random vectors. Based on low sub-band features and the VC, the watermark image is divided into two random looking images called private and public shares. The secret share is kept with a certified authority (CA), and the two random vectors are kept by the owner of the digital content. To make a decision about a suspected image, the two random vectors kept by the owner are used to extract SPT low sub-band features to construct the public share. To reveal the watermark image, the constructed public share and the private share kept by the CA are stacked together. Based on the research that we did in the literature of copyright protection schemes, we are the first that combined VC and SPT.

The rest of the paper is organized as follows. The description of SPT and VC is explained in Section 2, followed by the proposed copyright protection scheme in Section 3. In Section 4, the detailed experimental results, and comparative analysis are given. Finally, the conclusions are given in Section 5.

2 Preliminary

2.1 Steerable Pyramid Transform

In signal processing, a signal can be decomposed into sub-bands by a wavelet transform. An important problem with the standard wavelet transform is the lack of the translation and the rotation invariant properties, especially in two-dimensional (2-D) signals. A way to overcome this problem is to replace the standard wavelet transform with a steerable pyramid transform [4, 28]. Translation and rotation invariant properties are very attractive in copyright protection schemes against geometric attacks. For this reason we propose a watermarking scheme based on steerable pyramid decomposition that possesses the desired properties. This decomposition transform is based on angular and radial decompositions, and has the advantage that the sub-bands are translation and rotation-invariant. The steerable pyramid transform typically partitions the input image into low- and high-pass portions, the low-pass portion is also sub-sampled, and the subdivision is repeated recursively on the low-pass portion [28] by a factor of 2 along the rows and columns. If there are k band-pass filters, then the pyramid is overcomplete by a factor of 4k/3.

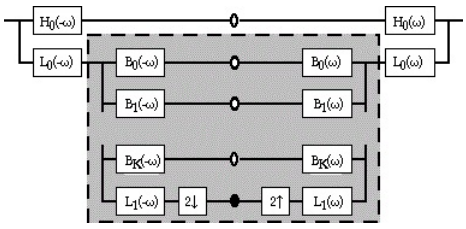

Figure 1: Tree representation of one-level 2D steerable pyramid transform [27]

Figure 1 shows single stage sub-band decomposition carried out by the SPT, where H1 is high pass filter, L0 and L1 are low-pass filters and Bi are oriented band-pass

filters. An example of 3 scales and 4 orientations SPT performed to Lena image is shown in Figure 2.

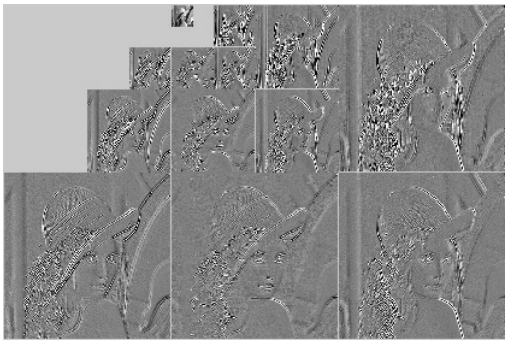

Figure 2: Lena steerable pyramid-based image decomposition using 3 scales and 4 orientations.

In steerable pyramid decomposition, filters are polar-separable in the Fourier domain, the first low- and high-pass filters, are defined as [24]

$$\begin{aligned} L_0(r,\theta) &= L(\frac{r}{2},\theta)/2 \\ H_0(r,\theta) &= H(\frac{r}{2},\theta), \end{aligned}$$

where r, θ are the polar frequency coordinates and L, H are raised cosine low- and high-pass transfer function:

$$\begin{aligned} L(r,\theta) &= \begin{cases} 2 & r \leqslant \frac{\pi}{4} \\ 2cos(\frac{\pi}{2}log_2(\frac{4r}{\pi}))\frac{\pi}{4} < r < \frac{\pi}{2} & \\ 0 & r \geqslant \frac{\pi}{2} \end{cases} \\ B_k(r,\theta) &= H(r)G_k(\theta), k \in [0, K-1]. \end{aligned}$$

$B_k(r,\theta)$ represents the K directional band-pass filter used in the iterative stages, with radial and angular parts, defined as:

$$\begin{aligned} H(r,\theta) &= \begin{cases} 1 & r \geqslant \frac{\pi}{4} \\ cos(\frac{\pi}{2}log_2(\frac{2r}{\pi})) & \frac{\pi}{4} < r < \frac{\pi}{2} \\ 0 & r \leqslant \frac{\pi}{2} \end{cases} \\ G_k(\theta) &= \begin{cases} \alpha_K(cos(\theta - \frac{\pi k}{K}))^{K-1} & \mid \theta - \frac{\pi k}{K} \mid < \frac{\pi}{2} \\ 0 & otherwize \end{cases} \end{aligned}$$

where

$$\alpha_K = 2^{(k-1)}\frac{(K-1)!}{\sqrt{K[2(K-1)]!}}$$

2.2 Visual Cryptography

The proposed copyright protection scheme in this paper is based on Visual Cryptography. VC is an image secret sharing scheme proposed by Naor and Shamir, in which human vision is used to protect the secret message. VC presents a simple but perfectly secure way to protect secret message, by using the human vision system to decrypt a protected message without expensive and complicated decoding. In their approach, the secret image, consisting of black and white pixels, is divided into n shares, and each participant would receive only one share. To reveal the secret image, all or some of the n shares are stacked together while using each share separately reveals no information about the secret image. However, the more the sharing images are, the harder the management is [32].

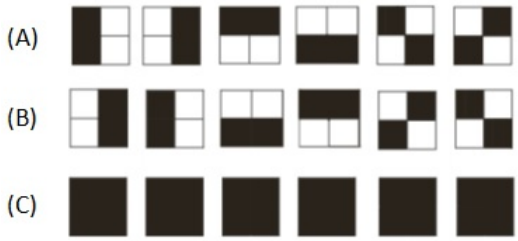

Figure 3: Possible combinations of 2-of-2 visual cryptography of a black share: (a) first share; (b) second share; (c) stacked share.

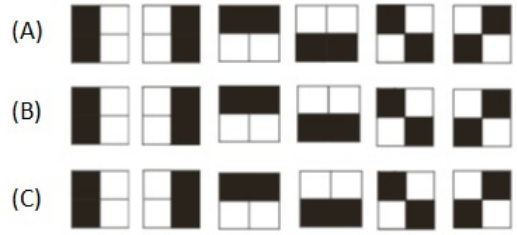

Figure 4: Possible combinations of 2-of-2 visual cryptography of a white share: (a) first share; (b) second share; (c) stacked share.

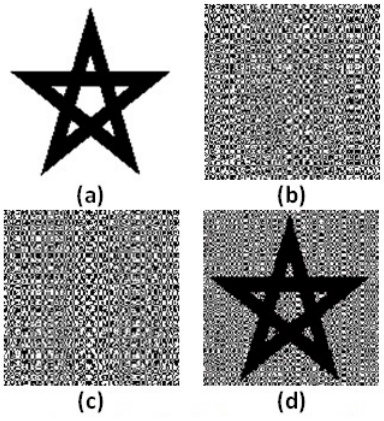

Figure 5: Example of basic 2-of-2 Visual Cryptography: (a) Secret Binary Image; (b) Share1; (c) Share2; (d) Stacked image (share1 and share2).

Possible combinations of the 2-of-2 visual cryptography are shown in Figure 3 and Figure 4. Figure 5 shows an example of basic 2-of-2 Visual Cryptography. In 2-of-2

VC, six pairs of encryption could be used to represent a secret image pixel, and each pixel is replaced by two white pixels and two black pixels to produce random looking shares. The size of the generated shares is 2Nx2N when the size of the secret image is NxN.

3 Proposed Method

This section, describes the proposed copyright protection scheme, which is based on SPT and VC. The proposed scheme consists of two phases: watermark concealing process and watermark extraction process. Unlike traditional watermarking schemes, the proposed method does not alter the original image by embedding the watermark image. Without loss of generality, the host image I is represented by a gray scale image of size M1xM2 and the watermark W is represented by a binary image of size N1xN2. In the proposed scheme steerable pyramid transform with one orientation and one scale is performed on the host image, and the low sub-band LS is selected. Two generated random vectors Vs and Vf of size 1xN1 and 1xN2, respectively, are used to select blocks of size 8x8 within the LS sub-band. The watermark image is divided into two random looking images called private and public shares, using the visual secret sharing scheme and the selected blocks features. To reveal the watermark image, the two shares are stacked together while using each share separately reveals no information about the watermark image. The owner of the digital media keeps the two generated random vectors securely and the private share is registered with a certified authority (CA).

3.1 Watermark Concealing Process

The process of watermark concealing is shown in Figure 6(a) and (b), and the detailed algorithm is given as follows:

Step 1. Perform one scale and one orientation steerable pyramid transform on the host image I of size M_1xM_2, and select the low sub-band LS.

Step 2. Calculate the mean LS_{mean} of selected LS low sub-band.

Step 3. Generate two random vectors Vs and Vf of size 1xN_1, 1xN_2, respectively. Vs and Vf contain integer values from 1 to M/2 -8.

Step 4. Blocks B_{ij} of size 8x8 in location LS(Vf_i,Vs_j) are selected, where $i \in \{1, ...N_1\}$ and $j \in \{1, ...N_2\}$.

Step 5. For each block B_{ij} calculate the corresponding mean M_{ij}.

$$M_{ij} = mean(B_{ij}).$$

Step 6. Calculate the binary image BI of size $N_1 \times N_2$ as

$$BI_{ij} = \begin{cases} 1, & if M_{ij} >= LS_{mean} \\ 0, & if M_{ij} < LS_{mean} \end{cases}$$

Step 7. Construct an empty private share PrS of size $2N_1 \times 2N_2$ and divide it into non-overlapping blocks Bpr_{ij} of size 2×2. The content of each block is calculated as follow.

$$Bpr_{ij} = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & if\ W_{ij} = 0\ and\ BI_{ij} = 1 \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & if\ W_{ij} = 0\ and\ BI_{ij} = 0 \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & if\ W_{ij} = 1\ and\ BI_{ij} = 1 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & if\ W_{ij} = 1\ and\ BI_{ij} = 0 \end{cases}$$

3.2 Watermark Extraction Process

The process of watermark extraction is shown in Figure 6(a) and (c), and the detailed algorithm is given as follows:

Step 1. Perform one scale and one orientation steerable pyramid transform on the claimed image I', and select the low sub-band LS'.

Step 2. Calculate the mean LS'$_{mean}$ of selected LS' low sub-band. The same generated vectors Vs and Vf in concealing process are used to select blocks B'$_{ij}$ of size 8x8 in location LS'(Vf_i,Vs_j), where $i \in \{1, ...N_1\}$ and $j \in \{1, ...N_2\}$.

Step 3. For each block B'$_{ij}$ calculate the correspondent mean M'$_{ij}$.

$$M'_{ij} = mean(B'_{ij}).$$

Step 4. Calculate the binary image BI' of size $N_1 \times N_2$ as

$$BI'_{ij} = \begin{cases} 1, & if M'_{ij} >= LS'_{mean} \\ 0, & if M'_{ij} < LS'_{mean} \end{cases}$$

Step 5. Construct a empty matrix called public share PuS of size $2N_1 \times 2N_2$ and divide it into non-overlapping blocks Bpu_{ij} of size 2×2. The content of each block is calculated as follow.

$$Bpu_{ij} = \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & if\ BI_{ij} = 1 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & if\ BI_{ij} = 0 \end{cases}$$

Step 6. By stacking the private share PrS kept by the CA and the public share PuS, the watermark image W' of size $2N_1 \times 2N_2$ appears.

Step 7. Divide the watermark W' into non-overlapping blocks Wb'$_{ij}$ of size 2×2 and apply the following reduction process to get a reduced watermark W" of size $N \times N$.

$$W''_{ij} = \begin{cases} 1, & if mean(Wb'_{ij}) >= 0.5 \\ 0, & if mean(Wb'_{ij}) < 0.5 \end{cases}$$

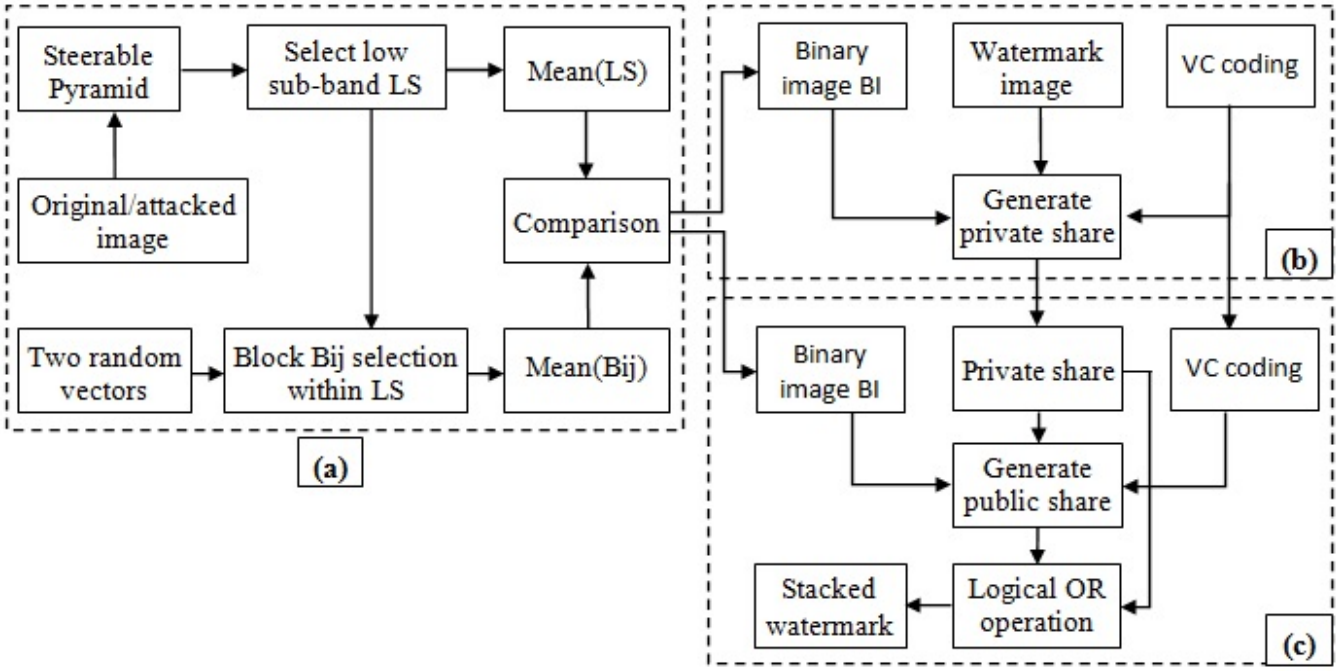

Figure 6: (a) and (b) represent the watermark concealing process; (a) and (c) represent the watermark extraction process.

4 Experimental Results

In this section, we evaluate the performance of the proposed copyright protection scheme by simulating some experiments to demonstrate that the proposed scheme can meet the requirements for copyright protection. Two well-known gray-level images named Lena and Einstein (Figure 7(a)) of size 512×512 are used as the host images and a binary image (Figure 7(b) of size 128×128 is used as a watermark image.

Peak signal to noise ratio (PSNR) is widely applied by copyright protection community for quality assessment. The bigger the PSNR value is, the better the quality of the protected image is. Most proposed scheme in the literature are having a PSNR value around 40dB, which is considered as a good value, and the quality of the protected image is considered to be good too. In the proposed scheme, the protected image has the maximum PSNR value since the host image is not altered by embedding the watermark image into the host image. The PSNR is defined as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}.$$

Where MSE (Mean Square Error) is defined as:

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (I_i - \hat{I}_i)^2.$$

Where N represents the number of pixels in the original (I) and watermarked ($\hat{I}$) image.

Normalized Correlation (NC) and Bit Error Rate (BER) are used as the objective quantitative measure to

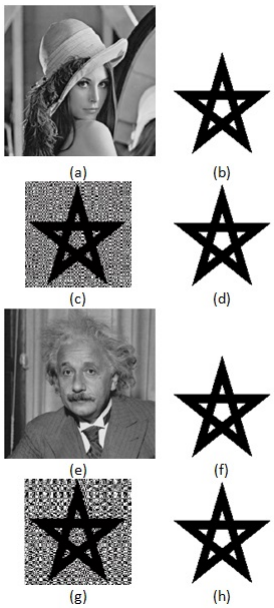

Figure 7: (a) Lena host image; (b) Original watermark; (c) Stacked watermark; (d) Reduced watermark.

compare the original and the extracted watermark image. NC and BER values are between 0 and 1. The bigger NC value is, the better the watermark robustness is, while the lower BER value indicates better robustness. NC and BER are defined as follow:

$$NC = \frac{\sum_{i=1}^{M} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{M} w_i^2} \sqrt{\sum_{i=1}^{M} \hat{w}_i^2}},$$

where M represents the number of pixels in the original (w) and the extracted ($\hat{w}$) watermark image.

$$BER = \frac{\sum_{i=1}^{N} \hat{w}_i \oplus w_i}{N},$$

where w and $\hat{w}$ denote the original watermark and the recovered watermark, respectively, N is the total size of the watermark, $\oplus$ represents the xor operator.

Figure 7(a) shows the protected image Lena under free attack and Figure 7(c) Shows the corresponding extracted watermark obtained by stacking the public share and the private share. The reduced watermark is shown in Figure 7(d). From Figure 7(a) to (d) we can see that the extracted watermark and the original watermark are identical under free attack on the protected Lena image.

Robustness constitutes the most important requirement for copyright protection schemes, and this can be proven by calculating the NC and/or the BER value between the original and the extracted watermark from distorted protected images. In order to evaluate the robustness of the proposed scheme, the protected images are distorted considering image processing and geometric attacks, like Pepper & salt noise, Speckle noise, Gaussian noise, Average filtering, Median filtering, Weiner filtering, Resizing, JPEG compression, Rotation, Cropping, Gamma correction, Histogram Equalization, Sharpening, Increasing contrast, Decreasing contrast, Increasing brightness and Decreasing brightness.

Figure 8 shows the attacked protected images under various attacks and Figure 9, Figure 10, Figure 11 and Figure 12 show the extracted watermark image under various attacks. Detailed results are shown in Table 1 and Table 2 where 100 attacks are simulated.

4.1 Robustness Against Noise Attacks

Robustness to additive noise is the first test to evaluate the proposed copyright scheme. Pepper & salt noise (with density 0.01, 0.02, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5 and 0.6), Speckle noise (with variance 0.01, 0.02, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5 and 0.6) and Gaussian noise (with zero mean and variance 0.01, 0.02, 0.05, 0.1, 0.2, 0.3, 0.4, 0.5 and 0.6) are the three types of noise applied to the protected image. Attacked protected image with Pepper & salt noise (density 0.6), Speckle noise (with variance 0.6) and Gaussian noise (with zero mean and variance 0.6) are shown in Figure 8(a), (b) and (c), respectively. Figure 9(a) to (x) shows the extracted watermarks for all tested noise addition attacks.

Table 1: Obtained NC and BER results after different attacks on the protected Lena and Einstein images

Attacks	Lena		Einstein	
	NC	**BER**	**NC**	**BER**
Pepper & salt noise				
Density=0.01	0.9966	0.0051	0.9944	0.0084
Density=0.02	0.9954	0.0069	0.9923	0.0115
Density=0.05	0.9905	0.0142	0.9866	0.0200
Density=0.1	0.9905	0.0142	0.9733	0.0394
Density=0.2	0.9784	0.0319	0.9504	0.0725
Density=0.3	0.9726	0.0405	0.9137	0.1245
Density=0.4	0.9658	0.0505	0.8731	0.1807
Density=0.5	0.9583	0.0613	0.8402	0.2244
Density=0.6	0.9423	0.0842	0.7964	0.2816
Speckle noise				
var=0.01	0.9964	0.0053	0.9963	0.0056
var=0.02	0.9954	0.0068	0.9940	0.0089
var=0.05	0.9921	0.0117	0.9904	0.0143
var=0.1	0.9887	0.0168	0.9853	0.0218
var=0.2	0.9832	0.0249	0.9786	0.0317
var=0.3	0.9777	0.0331	0.9718	0.0416
var=0.4	0.9719	0.0416	0.9665	0.0494
var=0.5	0.9671	0.0486	0.9588	0.0605
var=0.6	0.9622	0.0557	0.9517	0.0707
Gaussian noise				
M=0 & var=0.01	0.9929	0.0105	0.9878	0.0181
M=0 & var=0.02	0.9905	0.0142	0.9809	0.0283
M=0 & var=0.05	0.9851	0.0220	0.9687	0.0461
M=0 & var=0.1	0.9795	0.0304	0.9470	0.0775
M=0 & var=0.2	0.9685	0.0464	0.9089	0.1312
M=0 & var=0.3	0.9612	0.0569	0.8804	0.1707
M=0 & var=0.4	0.9553	0.0655	0.8585	0.2001
M=0 & var=0.5	0.9486	0.0752	0.8420	0.2218
M=0 & var=0.6	0.9432	0.0829	0.8266	0.2418
Average filtering				
3x3	0.9991	0.0013	0.9996	0.0006
6x6	0.9917	0.0124	0.9935	0.0097
9x9	0.9906	0.0139	0.9929	0.0105
12x12	0.9859	0.0209	0.9872	0.0190
15x15	0.9838	0.0240	0.9829	0.0254
18x18	0.9776	0.0332	0.9775	0.0333
21x21	0.9730	0.0399	0.9732	0.0396
24x24	0.9673	0.0482	0.9664	0.0496
Median filtering				
3x3	0.9983	0.0025	0.9979	0.0031
6x6	0.9899	0.0150	0.9918	0.0122
9x9	0.9920	0.0120	0.9926	0.0110
12x12	0.9865	0.0201	0.9873	0.0189
15x15	0.9853	0.0218	0.9853	0.0218
18x18	0.9821	0.0265	0.9782	0.0323
21x21	0.9771	0.0339	0.9717	0.0418
24x24	0.9718	0.0416	0.9666	0.0492
Weiner filtering				
3x3	0.9991	0.0013	0.9996	0.0006
6x6	0.9962	0.0057	0.9955	0.0067
9x9	0.9955	0.0068	0.9953	0.0070
12x12	0.9921	0.0118	0.9915	0.0126
15x15	0.9912	0.0131	0.9881	0.0176
18x18	0.9869	0.0194	0.9849	0.0223
21x21	0.9837	0.0242	0.9820	0.0267
24x24	0.9797	0.0302	0.9774	0.0334
Resizing				
384x384	0.9998	0.0002	0.9998	0.0002
256x256	0.9997	0.0002	0.9998	0.0002
192x192	0.9993	0.0010	0.9995	0.0007
128x128	0.9982	0.0026	0.9980	0.0029
96x96	0.9971	0.0043	0.9967	0.0049
64x64	0.9929	0.0106	0.9925	0.0112
32x32	0.9728	0.0402	0.9713	0.0424
JPEG compression				
Q=90	0.9996	0.0006	0.9998	0.0003
Q=80	0.9989	0.0016	1.0000	0.0000
Q=70	0.9993	0.0010	0.9988	0.0018
Q=60	0.9986	0.0021	0.9985	0.0023
Q=50	0.9986	0.0021	0.9982	0.0027
Q=40	0.9987	0.0020	0.9981	0.0029
Q=30	0.9976	0.0036	0.9974	0.0038
Q=20	0.9970	0.0045	0.9955	0.0067
Q=10	0.9947	0.0079	0.9937	0.0094
Q=5	0.9853	0.0218	0.9796	0.0302

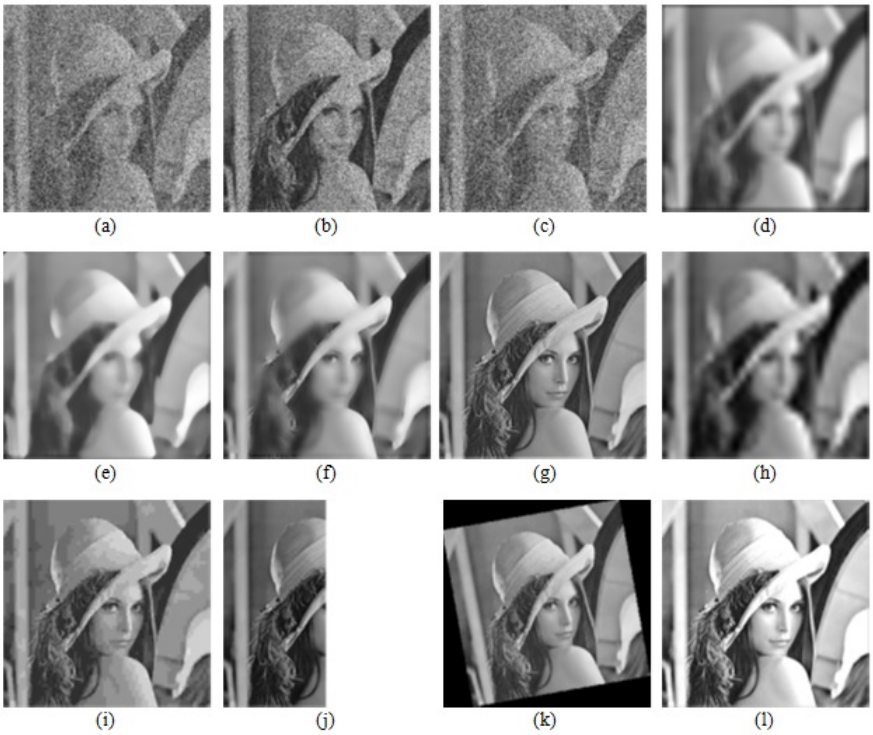

Figure 8: Protected Lena image under attacks (a) Pepper & salt noise (density 0.5); (b) Speckle noise (var=0.5); (c) Gaussian noise (M=0,var=0.5); (d) Average filter (24x24); (e) Median filtering (24x24); (f) Weiner filtering (21x21); (g) Sharpening; (h) resizing (32x32); (i) JPEG compression (Q=5); (j) Cropping 1/4th from the center; (k) Rotation (angle=10); (l) increase contrast by 10%.

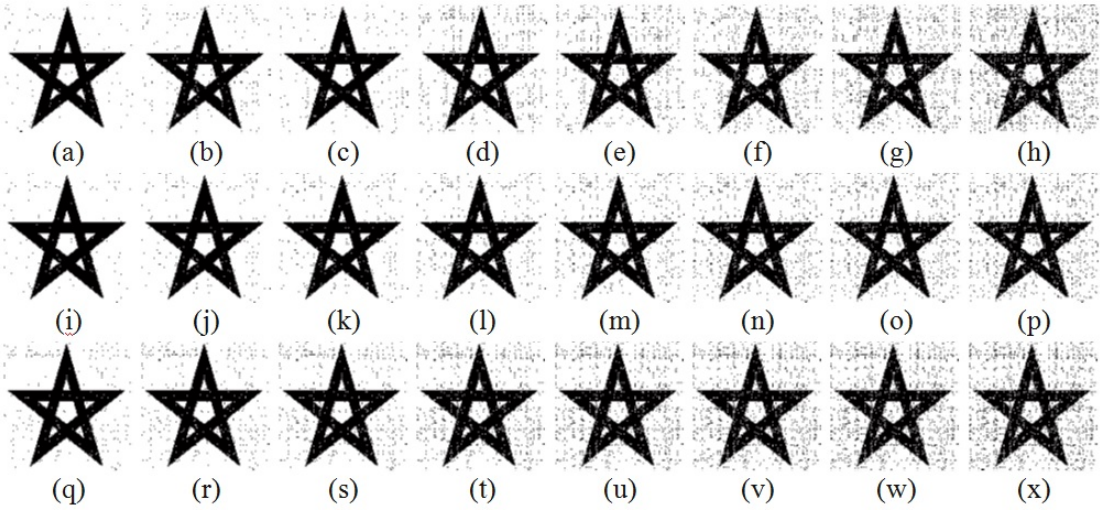

Figure 9: Extracted watermark under attacks (a) Pepper & salt noise (density 0.02); (b) Pepper & salt noise (density 0.05); (c) Pepper & salt noise (density 0.1); (d) Pepper & salt noise (density 0.2); (e) Pepper & salt noise (density 0.3); (f) Pepper & salt noise (density 0.4); (g) Pepper & salt noise (density 0.5); (h) Pepper & salt noise (density 0.6); (i) Speckle noise (var=0.02); (j) Speckle noise (var=0.05); (k) Speckle noise (var=0.1); (l) Speckle noise (var=0.2); (m) Speckle noise (var=0.3); (n) Speckle noise (var=0.4); (o) Speckle noise (var=0.5); (p) Speckle noise (var=0.6); (q) Gaussian noise (M=0,var=0.02); (r) Gaussian noise (M=0,var=0.05); (s) Gaussian noise (M=0,var=0.1); (t) Gaussian noise (M=0,var=0.2); (u) Gaussian noise (M=0,var=0.3); (v) Gaussian noise (M=0,var=0.4); (w) Gaussian noise (M=0,var=0.5); (x) Gaussian noise (M=0,var=0.6).

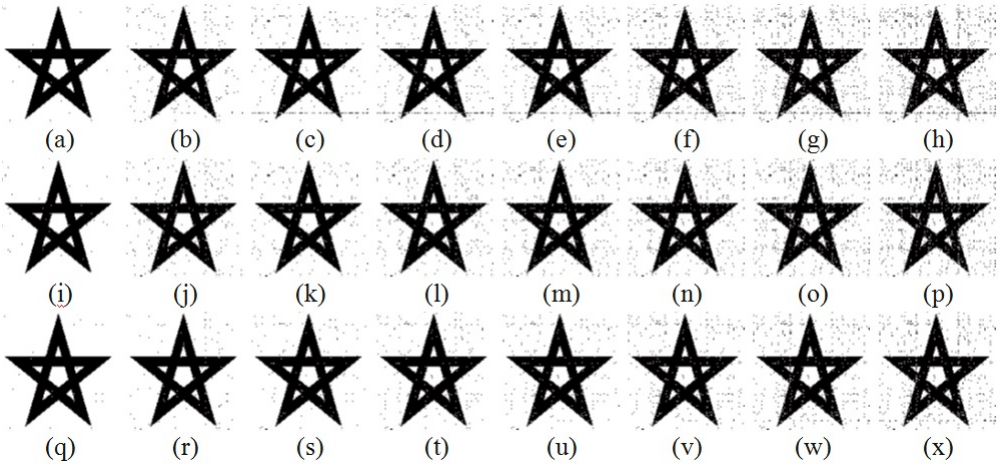

Figure 10: Extracted watermark under attacks (a) Average filtering (3x3); (b) Average filtering (6x6); (c) Average filtering (9x9); (d) Average filtering (12x12); (e) Average filtering (15x15); (f) Average filtering (18x18); (g) Average filtering (21x21); (h) Average filtering (24x24); (i) Median filtering (3x3); (j) Median filtering (6x6); (k) Median filtering (9x9); (l) Median filtering (12x12); (m) Median filtering (15x15); (n) Median filtering (18x18); (o) Median filtering (21x21); (p) Median filtering (24x24); (q) Weiner filtering (3x3); (r) Weiner filtering (6x6); (s) Weiner filtering (9x9); (t) Weiner filtering (12x12); (u) Weiner filtering (15x15); (v) Weiner filtering (18x18); (w) Weiner filtering (21x21); (x) Weiner filtering (24x24).

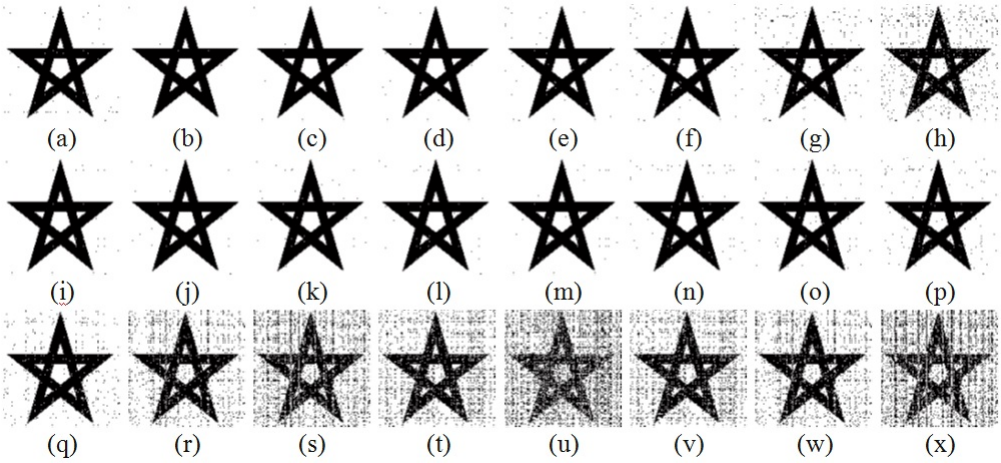

Figure 11: Extracted watermark under attacks (a) Sharpening; (b) Resizing (384x384); (c) Resizing (256x256); (d) Resizing (192x192); (e) Resizing (128x128); (f) Resizing (96x96); (g) Resizing (64x64); (h) Resizing (32x32); (i) JPEG compression (Q=80); (j) JPEG compression (Q=70); (k) JPEG compression (Q=60); (l) JPEG compression (Q=50); (m) JPEG compression (Q=40); (n) JPEG compression (Q=30); (o) JPEG compression (Q=20); (p) JPEG compression (Q=10); (q) JPEG compression (Q=5); (r) Increasing contrast (10%); (s) Increasing contrast (20%); (t) Decreasing contrast (10%); (u) Decreasing contrast (20%); (v) Increasing brightness (10%); (w) Decreasing brightness (10%); (x) Decreasing brightness (20%).

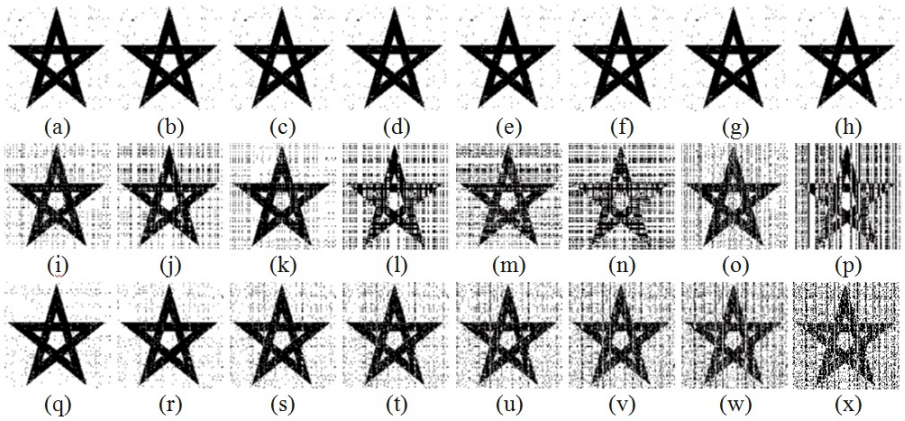

Figure 12: Extracted watermark under attacks (a) Rotation (angle=10); (b) Rotation (angle=20); (c) Rotation (angle=30); (d) Rotation (angle=40); (e) Rotation (angle=50); (f) Rotation (angle=60); (g) Rotation (angle=70); (h) Rotation (angle=80); (i) Cropping 1/4th from the top right corner; (j) Cropping 1/4th from the top left corner; (k) Cropping 1/4th from the bottom right corner; (l) Cropping 1/4th from the bottom left corner; (m) Cropping 1/2th from the top; (n) Cropping 1/2th from the bottom; (o) Cropping 1/2th from the right; (p) Cropping 1/2th from the left; (q) Histogram Equalization ; (r) Gamma correction (0.95) ; (s) Gamma correction (0.9) ; (t) Gamma correction (0.85) ; (u) Gamma correction (0.8) ; (v) Gamma correction (0.75) ; (w) Gamma correction (0.70) ; (x) Gamma correction (0.65).

As we can see the extracted watermarks under noise attacks, are very recognizable even if the protected images being seriously distorted.

4.2 Robustness Against Filtering Attacks

The second test aims to test the robustness against image processing attacks such as filtering. Average filtering (with window 3x3 to 24x24), Median filtering (with window 3x3 to 24x24), Wiener filtering (with window 3x3 to 24x24), and un-sharp filtering are the four types of filter tested on the protected images. Attacked Lena images with Average filtering (24x24), Median filtering (24x24), Wiener filtering (24x24), and un-sharp filtering are shown in Figure 8(d), (e), (f) and (g), respectively. Figure 10(a) to (x) and Figure 11(a) show the extracted watermarks under this four filters attacks and demonstrate the effectiveness of the proposed scheme against filtering attack.

4.3 Robustness Against JPEG Lossy Compression

The protected images were compressed using JPEG lossy compression, which is a common image/video compression standard. Different quality factors (QF) from 90 to 5 are used for the JPEG compression. Compressed Lena image by QF=5 is shown in Figure 8 (i) and extracted watermarks for different QF are shown in Figure 11 (i) to (q). The results demonstrate that the proposed scheme is highly robust to JPEG lossy compression even if the protected image is highly compressed.

4.4 Robustness Against Geometric Attacks

For a specific purpose, an image could be enlarged, reduced, cropped or rotated to fit the desired size or a desired area.

For the resizing attack the size of the protected images is reduced from 512x512 to 384x384, 256x256, 192x192, 128x128, 96x96, 64x64 and 32x32. The 32x32 resized protected Lena image is shown in Figure 8(h) and the extracted watermarks are shown in Figure 11 (b) to (h).

The protected images are attacked also by a rotation attack with different angles of rotation. Extracted watermarks after applying a rotation angle with 10, 20, 30, 40, 50, 60, 70 and 80 degree are shown in Figure 12 (a) to (h).

Moreover, cropping attack is also evaluated by cutting some part of the protected image. Extracted watermarks after cropping 1/4th from the top right corner, the top left corner, the bottom right corner and the bottom left corner of the protected image are shown in Figure 12 (i) to (l), respectively. Extracted watermarks after cropping 1/2th from the top, bottom, right and left of the protected image are shown in Figure 12 (m) to (p).

The obtained results demonstrate the robustness of the proposed scheme under geometric attacks, which are the Achilles heel for many watermarking schemes in the literature.

Table 2: Obtained NC and BER results after different attacks on the protected Lena and Einstein images

Attacks	Lena		Einstein	
	NC	**BER**	**NC**	**BER**
Rotation				
Angle=10	0.9927	0.0109	0.9932	0.0101
Angle=20	0.9931	0.0103	0.9932	0.0102
Angle=30	0.9922	0.0115	0.9923	0.0115
Angle=40	0.9925	0.0111	0.9943	0.0085
Angle=50	0.9929	0.0106	0.9934	0.0098
Angle=60	0.9929	0.0106	0.9929	0.0106
Angle=70	0.9929	0.0106	0.9932	0.0102
Angle=80	0.9931	0.0103	0.9935	0.0097
Cropping 1/4th from				
The top right corner	0.9473	0.0772	0.9701	0.0442
The top left corner	0.9161	0.1208	0.9344	0.0953
The bottom right corner	0.9445	0.0811	0.8861	0.1635
The bottom left corner	0.8575	0.2015	0.8840	0.8840
Cropping 1/2th from				
The top	0.8621	0.1946	0.9032	0.1392
The bottom	0.7966	0.2808	0.7655	0.3214
The right	0.8931	0.1532	0.8559	0.2046
The left	0.7681	0.3154	0.8151	0.2570
Gamma correction				
Gamma=0.65	0.8202	0.2504	0.7168	0.3798
Gamma=0.7	0.8469	0.2156	0.7389	0.3531
Gamma=0.75	0.8786	0.1729	0.7579	0.3292
Gamma=0.8	0.9155	0.1222	0.7813	0.3002
Gamma=0.85	0.9377	0.0908	0.8185	0.2524
Gamma=0.9	0.9556	0.0651	0.8781	0.1735
Gamma=0.95	0.9766	0.0345	0.9407	0.0865
Increasing contrast				
By 10%	0.9444	0.0812	0.8609	0.1965
By 20%	0.8863	0.1625	0.7715	0.3125
Decreasing contrast				
By 10%	0.9218	0.1134	0.8685	0.1868
By 20%	0.8281	0.2408	0.7195	0.3755
Increasing brightness				
By 10%	0.9172	0.1199	0.8838	0.1660
Decreasing brightness				
By 10%	0.9353	0.0942	0.8085	0.2654
By 20%	0.8389	0.2261	0.7272	0.3674
Other attacks				
Histogram Equalization	0.9837	0.0242	0.9656	0.0507
Sharpening	0.9976	0.0036	0.9978	0.0033

4.5 Robustness Against General Image Processing Attacks

Histogram equalization is a popular image processing operation that consists usually of increasing the global contrast of an image. The extracted watermark after performing histogram equalization is shown in Figure 12 (q).

Increasing/Decreasing contrast and brightness is also evaluated in the proposed scheme and the extracted watermarks are shown in Figure 11 (r) to (x).

Gamma correction with different Gamma values is applied to the protected image, which consists of maximizing the use of the bits or bandwidth relative to how humans perceive light and color. Extracted watermarks are shown in Figure 12 (r) to (x).

Based on the extracted watermarks we can conclude that the proposed scheme is highly robust against general image processing attacks.

4.6 Robustness Compared to Other Approaches

The robustness of the proposed copyright scheme compared to six recently related watermarking schemes is tested as well. The comparison includes Lang and Zhang [13], Ranjbar et al. [25], Agarwal et al. [1], Horng et al. [6], Run et al. [26] and Wang et al. [33]. Graphical comparison based on the NC results reported by Run et al. [26] and Wang et al. [33] is shown in Figure 13, which demonstrates the superiority of the proposed scheme. Moreover, the Robusteness limit against attacks for all the schemes included in this comparison is shown in Table 3. These results demonstrate that the robustness of the proposed algorithm is far better and proves superiority over the other existing algorithms.

5 Conclusion

A new robust blind copyright protection scheme based on visual cryptography and steerable pyramid transform is proposed in this paper. Experimental results show that the proposed scheme is highly robust against several image processing and geometric attacks such as Pepper & salt noise, Speckle noise, Gaussian noise, Average filtering, Median filtering, Weiner filtering, Resizing, JPEG compression, Rotation, Cropping, Gamma correction, Histogram Equalization, Sharpening, Increasing contrast, Decreasing contrast, Increasing brightness and Decreasing brightness. Moreover the proposed scheme has the advantage of having the maximum PSNR value since the host image is not altered and that could be useful to protect sensitive images.

References

[1] C. Agarwal, A. Mishra, and A. Sharma, "Gray-scale image watermarking using GA-BPN hybrid net-

Table 3: Robustness limit comparison. '-' means the attacks are not done

	Poposed scheme	Lang and Zhang [13]	Ranjbar et al. [25]	Agarwal et al. [1]	Horng et al. [6]	Run et al. [26]	Wang et al. [33]
Pepper & salt noise (density)	**0.6**	0.1	0.01	-	0.2	-	-
Speckle noise (variance)	**0.6**	0.1	0.01	-	-	-	-
Gaussian noise (variance)	**0.6**	0.03	0.001	0.1	0.05	0.03	0.03
Average filtering	**24x24**	-	-	-	11x11	6x6	7x7
Median filtering	**24x24**	-	3x3	5x5	9x9	7x7	7x7
Weiner filtering	**24x24**	-	3x3	3x3	-	-	-
Scaling Factor	**1/16**	-	1/2	1/2	1/2	1/2	1/2
JPEG compression (QF)	**5**	20	40	10	10	10	10

The bold values is the best

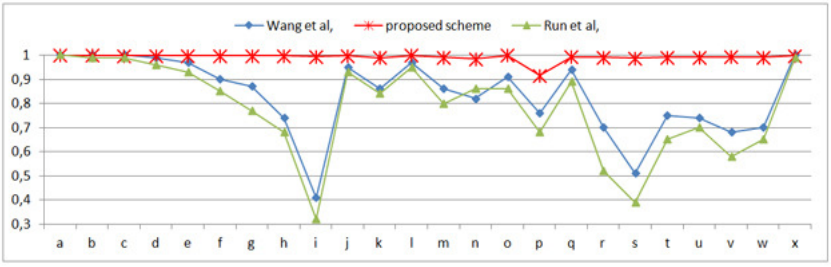

Figure 13: Robustness comparison for our scheme, Wang et al. [33] and Run et al. [26]. (a) JPEG compression Q=80; (b) JPEG compression Q=70; (c) JPEG compression Q=60; (d) JPEG compression Q=50; (e) JPEG compression Q=40; (f) JPEG compression Q=30; (g) JPEG compression Q=25; (h) JPEG compression Q=20; (i) JPEG compression Q=10; (j) Median filtering (3x3); (k) Median filtering (5x5); (l) Average filtering (3x3); (m) Average filtering (5x5); (n) Histogram equalization; (o) Resize (256x256); (p) Cropping (1/4); (q) Gaussian noise (M=0,var=0.01); (r) Gaussian noise (M=0,var=0.02); (s) Gaussian noise (M=0,var=0.03); (t) Rotation (angle=0.25); (u) Rotation (angle=-0.25); (v) Rotation (angle=0.3); (w) Rotation (angle=-0.3); (x) Sharpening.

work," *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, pp. 1135–1146, 2013.

[2] I. Cox, M. Miller, J. Bloom, and M. Miller, *Digital watermarking*, Morgan Kaufmann, 2001.

[3] S. Dogan, T. Tuncer, E. Avci, and A. Gulten, "A robust color image watermarking with singular value decomposition method," *Advances in Engineering Software*, vol. 42, no. 6, pp. 336–346, 2011.

[4] W. T. Freeman and E. H. Adelson, "The design and use of steerable filters," *IEEE Transactions on Pattern analysis and machine intelligence*, vol. 13, no. 9, pp. 891–906, 1991.

[5] J. M. Guo and C. H. Chang, "Prediction-based watermarking schemes using ahead/post AC prediction," *Signal Processing*, vol. 90, no. 8, pp. 2552–2566, 2010.

[6] S. J. Horng, D. Rosiyadi, T. Li, T. Takao, M. Guo, and M. K. Khan, "A blind image copyright protection scheme for e-government," *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, pp. 1099–1105, 2013.

[7] Y. C. Hou and P. M. Chen, "An asymmetric watermarking scheme based on visual cryptography," in *IEEE the 5th International Conference on Signal Processing Proceedings (WCCC-ICSP'00)*, vol. 2, pp. 992–995, 2000.

[8] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875–882, 2001.

[9] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875–882, 2001.

[10] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical engineering*, vol. 44, no. 7, pp. 077003–077003, 2005.

[11] S. Joo, Y. Suh, J. Shin, H. Kikuchi, and S. J. Cho, "A new robust watermark embedding into wavelet DC components," *ETRI Journal*, vol. 24, no. 5, pp. 401–404, 2002.

[12] T. H. Lan and A. H. Tewfik, "A novel high-capacity data-embedding system," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2431–2440, 2006.

[13] J. Lang and Z. Zhang, "Blind digital watermarking method in the fractional fourier transform domain," *Optics and Lasers in Engineering*, vol. 53, pp. 112–121, 2014.

[14] S. D. Lin, S. C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Computer Standards & Interfaces*, vol. 32, no. 1, pp. 54–60, 2010.

[15] J. C. Liu and S. Y. Chen, "Fast two-layer image watermarking without referring to the original image and watermark," *Image and Vision Computing*, vol. 19, no. 14, pp. 1083–1097, 2001.

[16] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, 2002.

[17] W. Lu, H. Lu, and F. L. Chung, "Feature based robust watermarking using image normalization," *Computers & Electrical Engineering*, vol. 36, no. 1, pp. 2–18, 2010.

[18] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," *Signal Processing*, vol. 88, no. 9, pp. 2158–2180, 2008.

[19] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology (Urocrypt'94)*, pp. 1–12, Springer, 1995.

[20] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal processing*, vol. 66, no. 3, pp. 385–403, 1998.

[21] M. Ouhsain and A. B. Hamza, "Image watermarking scheme using nonnegative matrix factorization and wavelet transform," *Expert Systems with Applications*, vol. 36, no. 2, pp. 2123–2129, 2009.

[22] J. C. Patra, J. E. Phua, and C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," *Digital Signal Processing*, vol. 20, no. 6, pp. 1597–1611, 2010.

[23] A. Phadikar, S. P. Maity, and B. Verma, "Region based QIM digital watermarking scheme for image database in DCT domain," *Computers & Electrical Engineering*, vol. 37, no. 3, pp. 339–355, 2011.

[24] J. Portilla and E. P. Simoncelli, "A parametric texture model based on joint statistics of complex wavelet coefficients," *International Journal of Computer Vision*, vol. 40, no. 1, pp. 49–70, 2000.

[25] S. Ranjbar, F. Zargari, and M. Ghanbari, "A highly robust two-stage contourlet-based digital image watermarking method," *Signal Processing: Image Communication*, vol. 28, no. 10, pp. 1526–1536, 2013.

[26] R. S. Run, S. J. Horng, W. H. Lin, T. W. Kao, P. Fan, and M. K. Khan, "An efficient wavelet-tree-based watermarking method," *Expert Systems with Applications*, vol. 38, no. 12, pp. 14357–14366, 2011.

[27] E. Simoncelli, "A rotation invariant pattern signature," in *Proceedings of IEEE International Conference on Image Processing*, vol. 3, pp. 185–188, 1996.

[28] E. P. Simoncelli, W. T. Freeman, E. H. Adelson, and D. J. Heeger, "Shiftable multiscale transforms," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 587–607, 1992.

[29] V. Solachidis and I. Pitas, "Optimal detection for multiplicative watermarks embedded in DFT domain," in *IEEE International Conference on Image Processing (ICIP'03)*, vol. 2, pp. II–723, 2003.

[30] B. Surekha and G. N. Swamy, "Sensitive digital image watermarking for copyright protection," *International Journal of Network Security*, vol. 15, no. 1, pp. 95–103, 2013.

[31] M. J. Tsai, K. Y. Yu, and Y. Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, p. 237, 2000.

[32] C. C. Wang, S. C. Tai, and C. S. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 8, pp. 1589–1598, 2000.

[33] Y. R. Wang, W. H. Lin, and L. Yang, "An intelligent watermarking method based on particle swarm optimization," *Expert Systems with Applications*, vol. 38, no. 7, pp. 8024–8029, 2011.

[34] J. C. K. Yau, L. C. K. Hui, S. M. Yiu, and B. S. N. Cheung, "Towards a secure copyright protection infrastructure for e-education material: Principles learned from experience.," *International Journal of Network Security*, vol. 2, no. 1, pp. 21–28, 2006.

Azz El Arab El Hossaini is a PhD student at the Faculty of Science, Ibn Tofail University. He received a Master's degree in Network and System Administration from the same faculty. He received his Bachelor's degree in administration of Computer Park from Faculty of Sciences Mohamed V-Agdal, Rabat. His research interest includes watermarking technologies, fingerprinting and data authentication.

Mohamed El aroussi has obtained his PHD degree in computer science and telecommunication from the Faculty of Sciences, University Mohamed V-Agdal, Rabat, Morocco, 2009. Since then he has worked in different projects in the field of WSN Biometric embedded systems. He is the author of several articles published in reputed journals.

Khadija Jamali received her Bachelor's degree in java and c++ development, she received a Master's degree in Network and System Administration and she is a Phd student at the Faculty of Science, Ibn Tofail University, Kenitra, Morocco. Her interest is watermarking technologies.

Samir Mbarki received the B.S. degree in applied mathematics from Mohammed V University, Morocco, 1992, and Doctorat of High Graduate Studies degrees in Computer Sciences from Mohammed V University, Morocco, 1997. In 1995 he joined the faculty of science Ibn Tofail University, Morocco where he is currently a Professor in Department of computer science. His research interests include software engineering, model driven architecture, software metrics and software tests. He obtained an HDR in computer Science from Ibn Tofail University in 2010.

Mohamed Wahbi obtained the diploma of engineer and the Ph.D. from ENSEEINT-INP Toulouse in May 1983 and the Docteur Es-Science diploma in December 1986 from the same institution. He is since Professor in the EHTP engineering school. he is the head of its Electrical Engineering and Telecommunications department and the SIR2C2S/LaGeS-EHTP research team. His research interests relate to Physics Electronics & Optoelectronics. He is author of a large number of regular and invited papers in international conferences and journals.