A SECURE AND ROBUST CDMA DIGITAL IMAGE WATERMARKING ALGORITHM BASED ON DWT2, YIQ COLOR SPACE AND ARNOLD TRANSFORM

Mehdi Khalili[1]

[1]Institute for Informatics and Automation Problems, National Academy of Science, Yerevan, Armenia
Khalili.Mehdi@yahoo.com

ABSTRACT

In this paper, a secure and robust cryptographic CDMA watermark algorithm based on DWT2, YIQ color space and Arnold transform is proposed. In the approach, for more security of watermark, the binary watermark image W, after scrambling with Arnold cat map is converted to a sequence and then, to determine the pixel to be used on a given key, a random binary sequence R of size n is adopted to encrypt the watermark using a pseudo-random number generator; where n is the size of the watermark. After that, it is embedded into the selected subbands coefficients of wavelet decomposition of Y channel of YIQ color space. For completely controlling the imperceptibility of watermarked images and the robustness of watermarks an adaptive casting technique is utilized using a gain factor k. The experimental results show that the proposed approach provides extra security and robustness against JPEG compression and different noise attacks compared to the similar proposed methods in earlier. Moreover, to extract watermarks in the proposed scheme, there is no need to original image.

KEYWORDS

CDMA watermarking, DWT2, YIQ color space, Arnold cat map, Pseudo-random number generator

1. INTRODUCTION

Nowadays, watermarking of images is becoming increasingly of interest in tasks such as copyright control, image identification, verification, and data hiding [1]. Advances in computer networking and high speed computer processors have made duplication and distribution of multimedia data easy and virtually costless, and have also made copyright protection of digital media an ever urgent challenge. As an effective way for copyright protection, digital watermarking, a process which embeds (hides) a watermark signal in the host signal to be protected, has attracted more and more research attention [2-3]. One of the earlier watermarking techniques, which used wavelet transform, was based on the adding pseudo random codes to the large coefficients at the high and middle frequency bands of the discrete wavelet transform [4]. This paper is allocated to CDMA digital images watermarking for ownership verification and image authentication applications, which for more security, watermark W, after scrambling by Arnold's cat map, is converted to a sequence and then a random binary sequence R of size n is adopted to encrypt the watermark, where n is the size of the watermark. This adopting process uses a pseudo- random number generator to determine the pixel to be used on a given key. In the other side, wavelet decomposition is applied on Y channel of converted host image to YIQ color space to perform embedding process into the selected subbands coefficients. For completely controlling the imperceptibility of watermarked images and the robustness of watermarks an adaptive casting technique is utilized using a gain factor k. Obtained results of the experiments

DOI : 10.5121/sipij.2011.2211

show the efficiency of proposed technique in acceptable transparency, high security and robustness against jpeg compression and different noise attacks in comparing the earlier works such as [5].

2. CDMA

Code Division Multiple Access or CDMA is a form of spread spectrum where the signal i.e. watermark information, is transmitted on a bandwidth much greater than the frequency content of the original information, in this case, an image. In other words the information bandwidth is much less than the transmitted signal bandwidth. Making spread spectrum is hard to detect because it uses wide-band, noise-like signals. Also, by a pseudo-random code which is independent from the data, the band spread is accomplished [6].

3. YIQ COLOR SPACE

The first NTSC color space was YIQ. This color space is included of one luminance (Y) and two chrominance (I, Q) components. The transform from RGB to YIQ and the backward transform from YIQ to RGB are as follow [7 and 8]:

$$\begin{bmatrix} \mathrm{Y} \\ \mathrm{I} \\ \mathrm{Q} \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} \quad \& \quad \begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} = \begin{bmatrix} 1.000 & 0.956 & 0.621 \\ 1.000 & -0.272 & -0.647 \\ 1.000 & -1.106 & 1.703 \end{bmatrix} \begin{bmatrix} \mathrm{Y} \\ \mathrm{I} \\ \mathrm{Q} \end{bmatrix} \qquad (1)$$

where Y-component stands for luminance or brightness, the I-component seems to mimic mostly shifts from blue, through purple, to red colors (with increasing I), and the Q-component seems to mimic mostly the value of green; the I and Q components jointly represent the chromatic attributes [8]. The decorrelation of R, G, and B component images makes the Y, I and Q component images complementary to each other [8]. For RGB values with a range of 0-255, Y has a range of 0-255, I a range of 0 to ±152, and Q has a range of 0 to ±134. Usually to simplify the implementation in an actual NTSC digital encoder or decoder, Eq. (1) and Eq. (2) are scaled [8].

4. ARNOLD SCRAMBLING TRANSFORM

Usually scrambling transform is used in the pretreatment stage of the watermark as a way of encryption. Generally, a meaningful watermark image becomes meaningless and disorderly (chaotic) after scrambling transform. Without the scrambling algorithm and the key, the attacker will not recover the watermark at all even if it has been extracted from the watermarked image. So the scrambling transform gives a secondary security for the digital products. In addition, after scrambling transform, the spatial relationships of the pixels of an image has been destroyed completely, which makes it evenly distributed in all the space, so the robustness of the algorithm was improved in this way [9]. Arnold transform is a kind of image scrambling methods, called as Arnold's cat mapping. Cause of this name is that, it is proposed by Vladimir Arnold and it is used on the image of a cat in Arnold's work, in the 1960s [10]. The discrete Arnold transformation is defined as follows [11]:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \; mod \;\; \mathrm{N} \qquad (2)$$

Where, a, b, c and d are positive integers, and $|A| = ad - bc.1$, so only three among the four parameters of a, b, c and d are independent. X_{n+1}, Y_{n+1}, X_n and Y_n are integers in {0,1,2,...,N-1}. The discrete Arnold transformation is obtained by extending the cat map. The position of watermark point can be changed to another position in the host image by iterating Eq. (2) n times, and moreover, the watermark point of different positions will get a different embedding position. Eq. (5) can be written as follows [11]:

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A^n \begin{bmatrix} X_1 \\ Y_1 \end{bmatrix} = B \begin{bmatrix} X_1 \\ Y_1 \end{bmatrix} \; mod \;\; \mathrm{N} \qquad (3)$$

where,

$$B = \left(\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} mod \;\; \mathrm{N} \right)^n \right) \; mod \;\; \mathrm{N} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \; mod \;\; \mathrm{N}$$

where, $a', b', c', d' \in (0,1,2,..., N-1)$, (X_1, Y_1) denotes the position of watermark point in the watermark image, and (X, Y) denotes the embedding position of watermark point in the host image. Obviously, the matrix B is constant under this condition a, b, c and d known, so the transformation of Eq. (3) was implemented with more efficiency and speed than Eq. (2) by removing the iterating operation. The constant a, b, c, d and n are kept as the secret key [11]. In this paper the extended Arnold transform in [12] is used to scramble watermarking of copyright protection.

5. PROPOSED WATERMARKING SCHEME

The current study task of digital watermarking is to make watermarks invisible to human eyes as well as robust to various attacks. The proposed watermarking scheme can hide visually recognizable patterns in images and is based on DWT2. In addition, in extraction process, there is no need to original host image. According to characteristic of Human Vision System, RGB color space is highly correlated and is not suitable for watermarking applications [11]. Therefore, in the proposed scheme, the host image is converted into YIQ color space and afterwards the wavelet decomposition is performed on Y channel. For more security of watermark, the watermark *W* after scrambling is converted to a sequence and then a random binary sequence *R* of size *n* is adopted to encrypt the watermark, where *n* is the size of the watermark. This adopting process uses a pseudo-random number generator to determine the pixel to be used on a given key. The selected details subbands coefficients for embedding i.e. HL and LH coefficients are quantized and then their most significant coefficients are embedded by the adopted watermark using the correlation properties of additive pseudo- random noise patterns according to equation shown in below:

$$I_{W_{x,y}} (u, v) = \begin{cases} I_{x,y} + k * W_i & \text{if } \; W = 0 \\ I_{x,y} * W_i & \text{Otherwise} \end{cases} \qquad (4)$$

where I_W denotes the resulting watermarked image and k denotes a gain factor for completely controlling the robustness of watermarks and imperceptibility of watermarked images. This adaptive casting technique is utilized to embed the watermark coefficients for completely controlling the imperceptibility of watermarked images and the robustness of watermarks. To retrieve the scrambled watermark, after converting watermarked image from RGB color space to YIQ channels, the Y channel will be decomposed into the wavelet coefficients. After seeding the same pseudo-random noise generator algorithm with the same key, the correlation will be computed between possible watermarked image in details subbands embedded coefficients and the noise pattern. By computation of the each coefficient correlation whit a certain threshold T, the scrambled watermark is detected; so, because of Arnold transform of periodicity, the original watermark image will be recovered. The block diagram of the proposed watermarking scheme is shown in Figure 1.

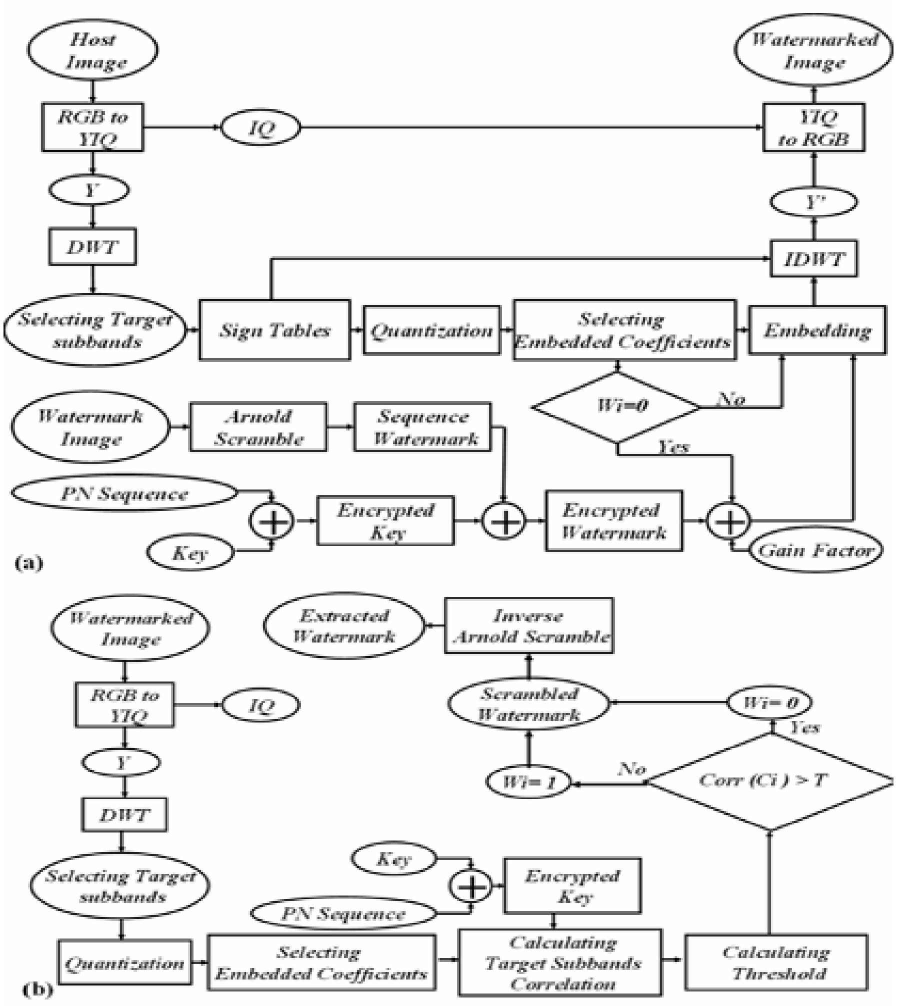


Figure 1. Block diagrams of the proposed watermarking scheme;
(a)Embedding procedure and (b)Extracting procedure

5.1. Watermark Embedding Method

The algorithm for embedding watermark in details subbands coefficients of the Y channel of host image is described as follows:

Step 1: Convert *RGB* channels of the host image *I* into *YIQ* channels using Eq. (1).

Step 2: For security, the watermark image is scrambled with extended Arnold algorithm in [12] for key times and gain the scrambled watermark. Key times can be seeing as secret key.

Step 3: For more security of watermark, the scrambled watermark *W* is converted to a sequence and then a random binary sequence *R* of size *n* is adopted to encrypt the watermark, where *n* is the size of the watermark image. Afterwards, to determine the pixel to be used on a given key, the encrypted watermark sequence $W1$ is generated using a pseudo-random number generator.

Step 4: Decompose the *Y* channel into a one-level wavelet structure with four *DWT* subbands, *F(H)*. For embedding the watermark, the coarsest coefficient of subbands *HL* and *LH* are taken as the target.

Step5: Take absolute values on coefficients of all *LH* and *HL*, and record their signs in sign matrices.

Step 6: Quantize absolute values of selection coefficients.

Step 7: Embed encrypted watermark $W1$ into the coarsest coefficient of subbands *HL* and *LH* by the watermark embedding strategy shown in Eq. (4).

Step 8: Effect sign matrices into the embedded coefficients.

Step 9: Reconvert *YIQ* channels of the changed host image into *RGB* channels.

Step 10: After applying IDWT with all changed and unchanged *DWT* coefficients, a watermarked image I' is generated.

Step 11: Record the pseudo-random noise generator algorithm and the key.

5.2. Watermark Extraction Method

In extraction method of the scrambled watermark, the same pseudo-random noise generator algorithm is used which is seeded with the same key. Afterwards, the correlation between possible watermarked image and the noise pattern is computed. In a result, the original watermark image is gained by the same Arnold transform algorithm with the same key times. The extracting watermark algorithm is described as follows:

Step 1: Converting the watermarked image from *RGB* color space to *YIQ* color space.

Step 2: Decomposing the *Y* channel into four *DWT* subbands.

Step 3: Seeding the recorded key using the recorded pseudo-random noise generator algorithm.

Step 4: Quantizing absolute values of *HL* and *LH* subbands.

Step 5: Computation of threshold *T* as follows:

$$T = \frac{Correlation(HL) + Correlation(LH)}{2} \qquad (5)$$

Step 6: Computation of the threshold T and each embedded coefficient correlation, separately.

Step 7: The sequence scrambled watermark is extracted as follows:

$$\begin{cases} W_i = 0 \quad if \quad C_i \rangle T \\ W_i = 1 \quad Othetwise \end{cases} \qquad (6)$$

Step 8: The Scrambled image watermark is produced by reconverting the extracted sequence watermark.

Step 9: Scramble the extracted watermark with the same Arnold algorithm with the same key times and gain the original watermark image.

6. EXPERIMENTAL RESULTS

The Robustness is the most highly desired feature of a watermarking algorithm especially if the application demands copyright protection, and persistent owner identification.

After achieving the high watermark security, the proposed perceptual watermarking scheme was implemented for evaluating both properties of imperceptibility and robustness against different attacks such as jpeg compression and noise.

Three 512×512 famous images: *Lena*, *Peppers* and *Baboon*, shown in Figure 2(a-c) were taken as the host images to embed a 27×27 binary watermark image, shown in Figure 2(d). For gain factor *k*, different values 0.5, 1.0 and 1.5 were taken entire implementation of the proposed CDMA scheme. For the entire test results in this paper, MATLAB R2007a software is used, too. Also, to initial state of MATLAB random number generator, 9 digit "key" were used. For computation of the wavelet transforms, 9-7 biorthogonal spline (B-spline) wavelet filters are used. Because, B-spline functions, are orthogonal and have better smoothness properties than other wavelet functions, despite the lack of compact support [4].

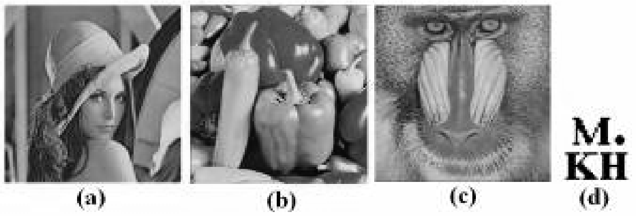


Figure 2. (a-c) The host images (Lena, Peppers, and Baboon)
and (d) The watermark image

After watermark embedding process, the similarity of original host image *x* and watermarked images *x'* was measured by the standard correlation coefficient (Corr) as fallows [1, 13]:

$$Correlation = \frac{\sum (x - x')(y - y')}{\sqrt{(x - x')^2}\sqrt{(y - x')^2}} \qquad (7)$$

where *y* and *y'* are the discrete wavelet transforms of *x* and *x'*, respectively. Moreover, the peak signal-to-noise ratio (*PSNR*) was used to evaluate the quality of the watermarked image. The *PSNR* is defined as [1, 13]:

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

where mean-square error (*MSE*) is defined as [1, 19 and 20]:

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

where $\{h_{i,j}\}$ and $\{h'_{i,j}\}$ are the gray levels of pixels in the host and watermarked images, respectively. The image quality is increased with increasing *PSNR*. In general, if *PSNR* values in watermarked image be greater than 30 dBs, the watermarked image is acceptable by human perception. In other words, the correlation is used for evaluating the robustness of watermarking technique and the *PSNR* is used for evaluating the transparency of watermarking technique [1, 13].

Also the normalized correlation (*NC*) coefficient was used to measure the similarity between original watermarks *W* and the extracted watermarks *W'* that is defined as [1, 13]:

$$NC = \frac{\sum_i \sum_j w_{i,j} * w'_{i,j}}{\sum_i \sum_j {w_{i,j}}^2} \qquad (10)$$

The proposed CDMA watermarking scheme yields satisfactory results in watermark imperceptibility and robustness. The obtained results show that larger gains are reason that CDMA will be remained as more PN sequences are added to the host image but it will be caused to decrease the transparency of the image, because of decreasing correlation between original image and watermarked image. Also, this results show that, the best compression can be made with CDMA, although CDMA is more resistant to different noise attacks such as Gaussian and salt & pepper. The PSNRs of the watermarked images produced by the proposed scheme for different gain factors *k* are all greater than 87 dBs, NCs between original watermark images and extracted watermark images are all equal 1. The results for effecting *k* on PSNRs, correlation between original images and watermarked images and NSs between original watermark images and extracted watermark images are illustrated in and Table 1. As it is seen the PSNR and correlation values indicate that the proposed scheme satisfies imperceptibility as well. After able to achieve the desired fidelity, various attacks were performed to test the robustness of the proposed scheme and it was found, that the proposed scheme performs excellently against JPEG compression and different noise attacks.

Table 1. Obtained results of watermark imperceptibility
with different values and gain factors *k*

Image	k	PSNR (dB)	Corr	NC	Error Bit %
Lena	0.5	78.01	0.9999	1.00	0
	1.0	77.69	0.9990	1.00	0
	1.5	77.13	0.9984	1.00	0
Baboon	0.5	67.42	0.9998	1.00	0
	1.0	67.20	0.9991	1.00	0
	1.5	66.88	0.9977	1.00	0
Peppers	0.5	72.66	0.9999	1.00	0
	1.0	72.29	0.9989	1.00	0
	1.5	71.71	0.9974	1.00	0

6.1. Robustness to Compression Attacks

To evaluate the response of the watermarking scheme to JPEG compression, watermarked images were compressed under different gain factors and different JPEG qualities *Q*s: 10, 15, 25, 50 and 75 with the similar references in [14]. Figure 3 shows the JPEG compression of the watermarked images under quality 10 and gain factor 1. Figure 4 shows the extracted watermarks from watermarked images after JPEG compression under different qualities and different gain factors.

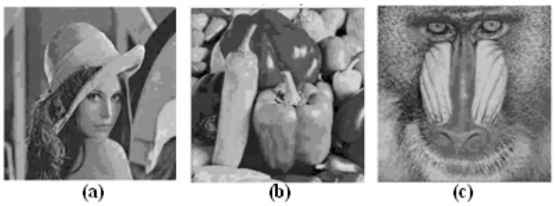


Figure 3. Watermarked images under JPEG compression (Q=10, k=1);
(a) Lena, (b) peppers and (c) Baboon

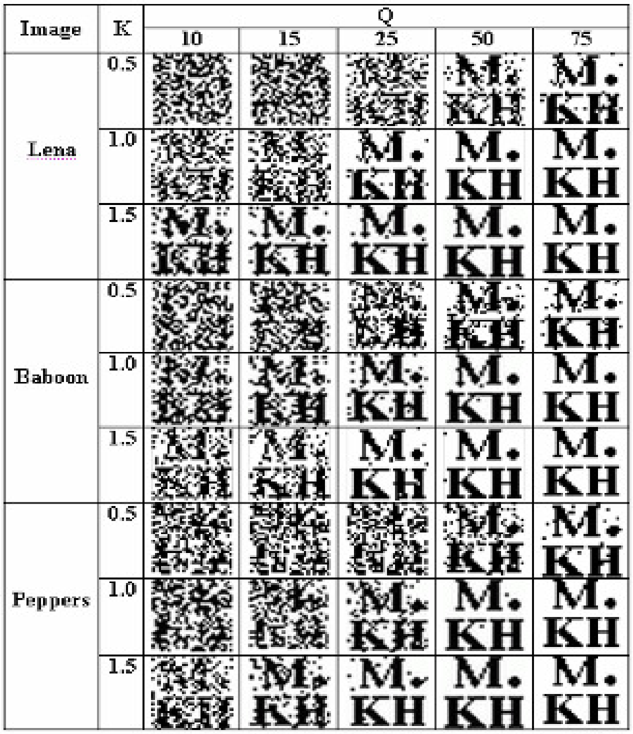


Image
K
Q
10
15
25
50
75
Lena
0.5
1.0
1.5
Baboon
0.5
1.0
1.5
Peppers
0.5
1.0
1.5

Figure 4. Extracted watermarks from watermarked images after JPEG compression

The percentage of the error bit for extracted watermarks under JPEG compression is shown in Figure 5. As it is seen, the percentage of error bit plot shown in this figure indicates that the margin of error is very less for the detection statistic, and CDMA proposed scheme has increased in comparing with the earlier works such as [5]. Table 2, shows the response of the detector to extract the watermark in JPEG compression. From the results it can be said that for JPEG compression with a quality factor of 75 and gain factor 0.5, a quality factor of 50 and gain factor 1 and also a quality factor of 15 and gain factor 1.5 the watermark detection and extraction is near perfect. The recovered watermarks for a quality factor of 25 and gain factor 1 show a number of detection errors and these only become highly noticeable for a quality factor of 15 and gain factor 1. The watermark is still recognizable for a quality factor of 10 and gain factor 1. Therefore, the overall robustness of proposed scheme for JPEG compression is considered high level, according to the robustness requirements table provided by Petitcolas [15] and is higher than earlier works such as [5]. So, it can be seen that the proposed scheme is more robust than earlier works such as [5] against JPEG compression, even for low JPEG quality.

Table 2. Obtained results of extracted watermarks in JPEG compression

***k*=0.5**

Image	**Q**	**10**	**15**	**25**	**50**	**75**
Lena	**NC**	0.2111	0.3416	0.4540	0.7522	0.8966
	PSNR(db)	81.38	84.02	86.81	89.73	92.97
Baboon	**NC**	0.2381	0.3737	0.4872	0.7551	0.8909
	PSNR(db)	79.27	81.25	83.66	87.49	91.86
Peppers	**NC**	0.1256	0.1854	0.3599	0.7464	0.9472
	PSNR(db)	88.00	90.23	92.40	94.94	97.01

***k*=1.0**

Image	Q	10	15	25	50	75
Lena	**NC**	0.4336	0.5910	0.8161	0.9906	1.00
	PSNR(db)	80.94	83.09	85.57	90.83	95.12
Baboon	**NC**	0.4871	0.6722	0.8808	0.9819	1.00
	PSNR(db)	78.56	80.41	82.73	86.51	91.19
Peppers	**NC**	0.2065	0.3849	0.7973	0.9939	1.00
	PSNR(db)	85.91	87.66	89.41	91.74	0.9469

***k*=1.5**

Image	Q	10	15	25	50	75
Lena	**NC**	0.6638	0.8139	0.9551	0.9993	1.00
	PSNR(db)	78.50	85.07	87.66	92.27	95.23
Baboon	**NC**	0.7071	0.8774	0.9586	0.9969	1.00
	PSNR(db)	77.52	79.24	81.48	85.44	90.70
Peppers	**NC**	0.3603	0.7820	0.9643	1.00	1.00
	PSNR(db)	78.20	84.66	86.27	88.92	93.13

6.2. Robustness to Noise Attacks

The CDMA proposed scheme was tested for its robustness against Gaussian and salt & pepper noises. From the results shown below, it is observed that for a Gaussian noise of 1 % with the gain factor 0.5; the watermark recovery is almost recognizable, for a Gaussian noise of 1 % with the gain factor 1, the watermark recovery is moderate and for a Gaussian noise of 1 % with the gain factor 1.5, the watermark recovery is near to perfect with very few detection errors. We must keep in mind that most schemes offer moderate robustness to noise [6]. Figure 6 shows added Gaussian noise of 0.5 % with gain factor 1 to watermarked images. Figure 7 shows the extracted watermarks in Gaussian noise of 1 % with different gain factors.

Figure 8 shows the percentage of error bit in extracted watermarks under different variances of Gaussian noise and gain factors. As it is obvious, the maximum error bit rate is still lower than 32% (variance of 1 % with gain factor 0.5). Figure 9 shows the results of PSNR in Gaussian noise experiment. Figure 10 shows the results of NC in Gaussian noise experiment. It is visible, the NC is acceptable for Gaussian noise of 1% with the gain factor 1.5 and it is moderate in Gaussian noise of 1% with gain factor 1. The obtained results from Gaussian noise experiment show that, the proposed CDMA scheme is more robust than the earlier works such as [5].

When the salt & pepper noise with zero mean and different noise densities of 0.01 to 0.5 with different gain factors introduced in the watermarked images, the extracted watermarks are recognizable in gain factor 0.5 and noise density 0.5, they are recovered in gain factor 1 and noise density 0.5 moderately and they are recovered in gain factor 1.5 and noise density 0.5 with a few detection errors. Figure 11 shows the watermarked images under salt & pepper noise attacks with noise densities of 0.5 and gain factor 1. Figure 12 shows the extracted watermarks from noisy watermarked images under noise density 0.5 with different gain factors and Figure13 shows the percentage of error bit in extracted watermarks under different noise densities of salt & pepper noise with different gain factors. As it is obvious, the maximum error bit rate is still lower than 34.5% (noise density of 1 % with gain factor 0.5). The PSNR results in salt & pepper noise experiment is shown in Figure 14. Figure 15 shows the NC results in salt & pepper noise experiment. The obtained results show that, NC in salt & pepper noise experiment is acceptable for noise density of 0.5 with the gain factor 0.5, it is moderate for the same noise density with the gain factor 1 and it is near to perfect for the same noise density and gain factor 1.5 with a few detection errors. From the obtained results it can be said that the proposed CDMA scheme is very efficient in robustness against salt & pepper attacks.

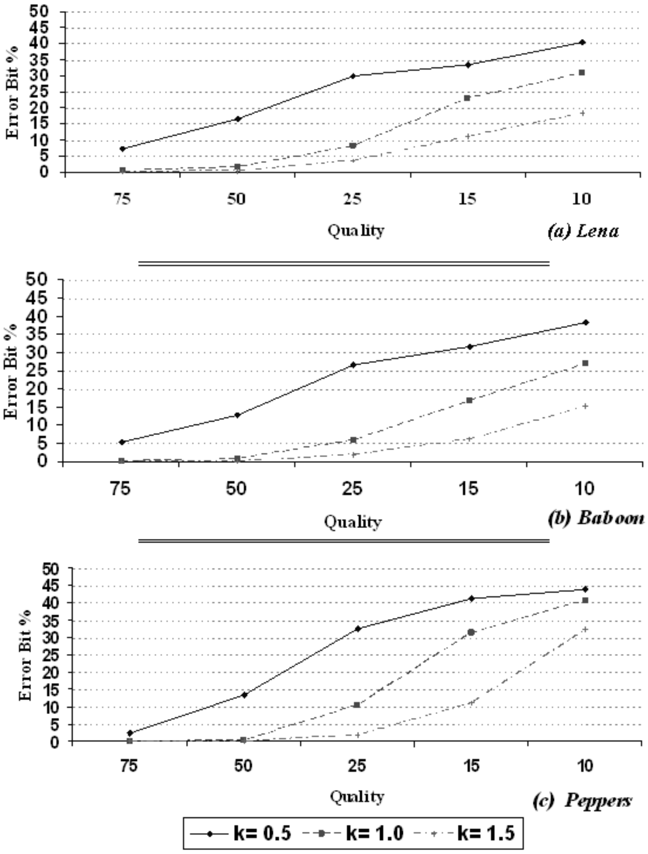


Figure 5. The percentage of error bit in extracted watermarks in JPEG compression under deferent qualities and gain factors

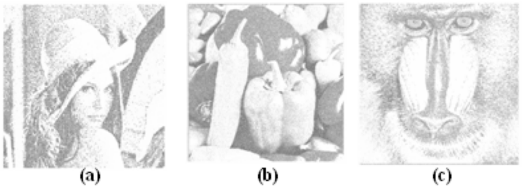


Figure 6. Watermarked images in Gaussian noise under variance 0.5 and k=1; (a) Lena, (b) peppers and (c) Baboon

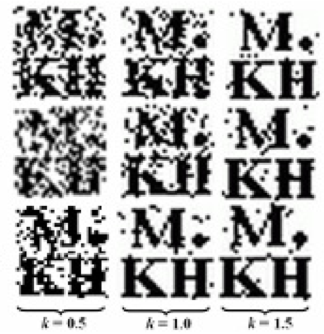
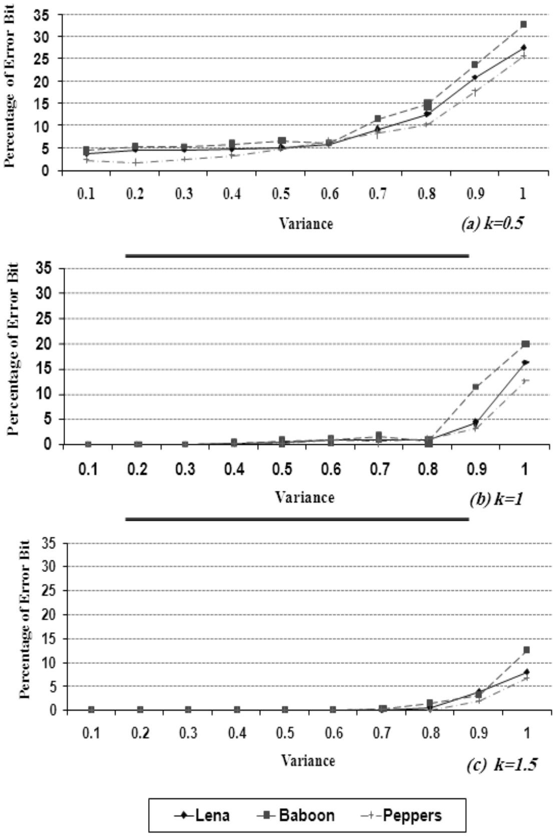


Figure 7. Extracted watermarks from Gaussian noise under variance 1 with different gain factors; (a) Lena, (b) Baboon and (c) Peppers



(a) k=0.5

(b) k=1

(c) k=1.5

Figure 8. Percentage of error bits in extracted watermarks in Gaussian noise experiment

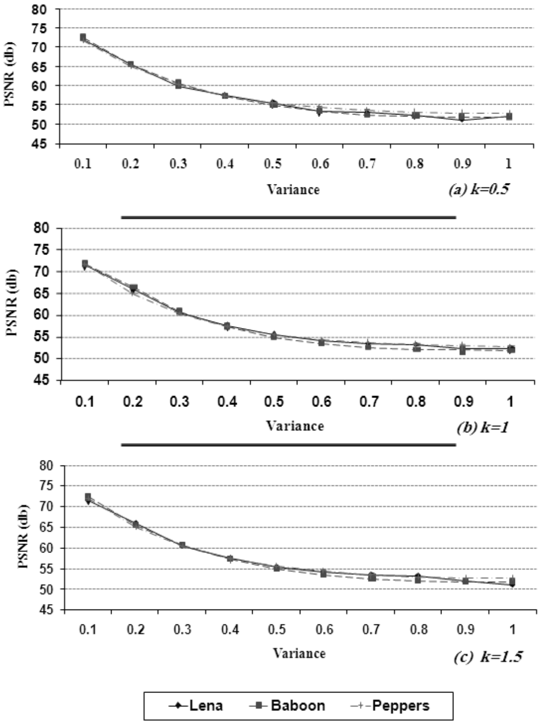


Figure 9. PSNRs under Gaussian noise experiment

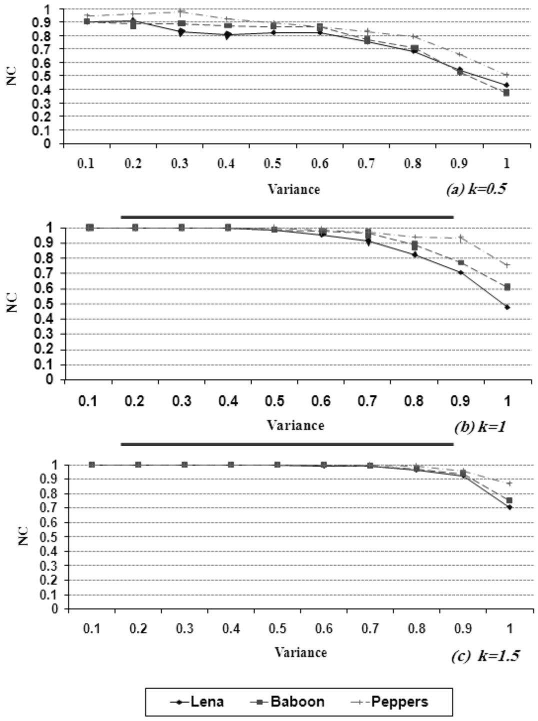


Figure 10. NCs in Gaussian noise experiment

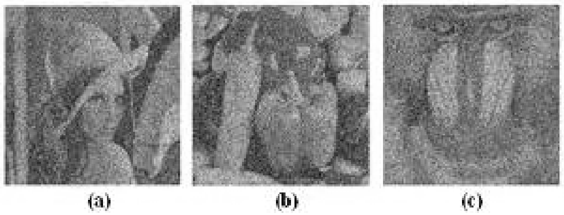


Figure 11. Salt & pepper noise on watermarked images with noise density 0.5 and k=1

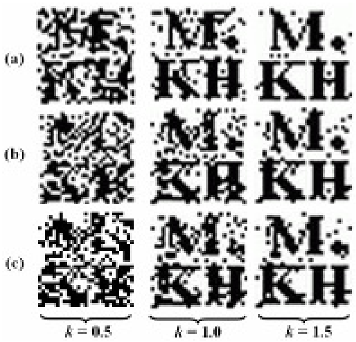


Figure 12. Extracted watermarks from salt & pepper noise under noise density 0.5 with different gain factors; Lena, (b) Baboon and (c) Peppers

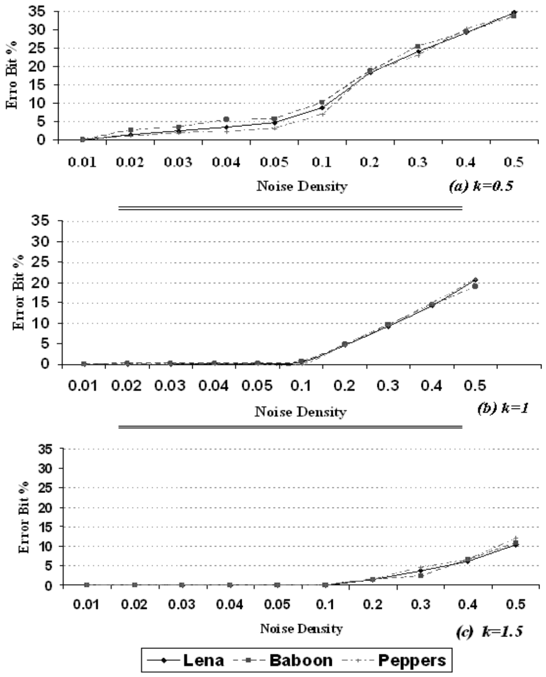


Figure 13. Percentage of error bit under salt & pepper noise experiment

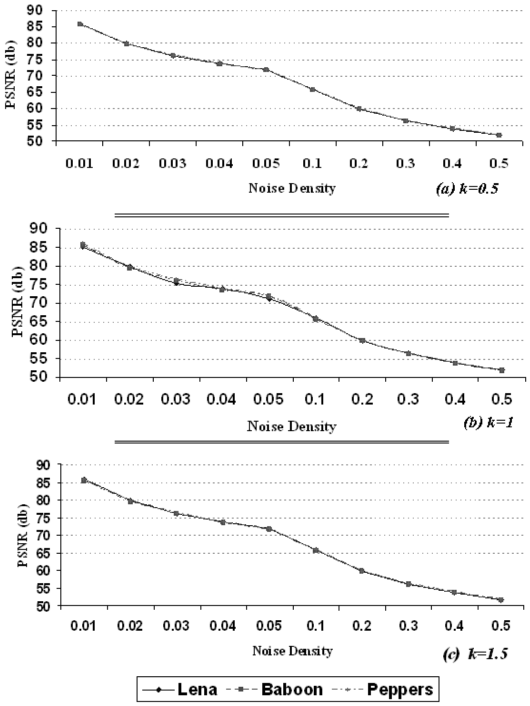


Figure 14. PSNRs in salt & pepper noise experiment

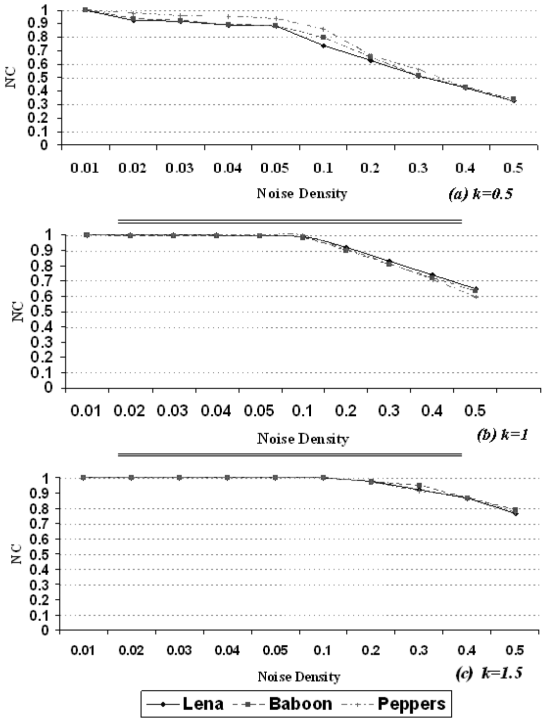


Figure 15. NCs in salt & pepper noise experiment

7. CONCLUSIONS

This paper provides a CDMA watermarking algorithm using DWT2 with satisfactory results in watermark robustness and security that improves upon the earlier work such as [5]. In the scheme, the host image is converted into *YIQ* channels; then, the *Y* channel is decomposed into wavelet coefficients. For more security of watermark, the watermark *W* after scrambling with Arnold transform algorithm is converted to a sequence and then to encrypt the watermark, a random binary sequence *R* of size *n* is adopted to determine the pixel to be used on a given key, using a pseudo-random number generator; where *n* is size of the watermark. The selected details subbands coefficients for embedding are quantized and then their most significant coefficients are replaced by the adopted scrambled watermark using the correlation properties of additive pseudo-random noise patterns. To embed the watermark coefficients for completely controlling the imperceptibility and the robustness of watermarks, an adaptive casting technique is utilized using a gain factor *k*. Also, the CDMA watermark scheme has no need to original Image in extracting process. The observations regarding the proposed watermarking scheme are summarized as follows: (1) Increasing gain factor *k* increases the PSNR and NC. In a result, it decreases the percentage of error bit and increases the robustness of the watermark against JPEG compression and Gaussian and salt & pepper noise attacks. In opposite, increasing gain factor *k*, decreases the transparency property.(2) The robustness of the proposed scheme to JPEG compression is found to be very good at a quality factor of 75 and gain factor 0.5, a quality factor of 50 and gain factor 1 and also a quality factor of 15 and gain factor 1.5. Reasonably, the robustness of the proposed scheme to JPEG compression is found to be good at a quality factor of 25 and gain factor 1 with a number of detection errors and for a quality factor of 15 and gain factor 1, this becomes highly noticeable. (3) The results show that, the watermark is still recognizable for a quality factor of 10 and gain factor 1. This result shows that, the proposed scheme improves the results in earlier works such as [5]. (4) The robustness of the proposed scheme to Gaussian noise with zero mean is found to be very good for a Gaussian noise of 1 % with the gain factor 1.5, and it is good for a Gaussian noise of 1 % with the gain factor 1. Also the extracted watermarks are recognizable for a Gaussian noise of 1 % with the gain factor 0.5; therefore, the results show the improving robustness against Gaussian noise attack in comparing with the earlier works such as [5]. (5) The robustness of the proposed scheme to salt & pepper noise with zero mean with noise density 0.5 is found to be very good for a gain factor 1.5, it is good for a gain factor 1 and also the extracted watermarks are recognizable for a gain factor 0.5.

REFERENCES

[1] Mehdi Khalili & David Asatryan, (2010) "Effective Digital Image Watermarking in YCbCr Color Space Accompanied by Presenting a Novel Technique Using DWT", *Proceedings of the Mathematical Problems of Computer Science Journal*, Vol. 33, pp150-161.

[2] Jian. Ren, (2009) "A Cryptographic Watermarking Technique for Multimedia Signals", *Proceedings of the Springer Science*, Business Media, Vol. 31, No. 1-3, pp267-281.

[3] Wang, S.H & Lin, Y.P, (2004) "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE *Transactions on Image Processing*, Vol. 13, No. 2, pp154–165.

[4] X.G. Xia & C. G. Boncelet & G. R. Arce, (1998) "Wavelet Transform Based Watermark for Digital Iimages", Optics Express, Vol. m, No. 12, pp497-511.

[5] Yanmei Fang & Jiwu Huang & Yun Q. Shi, (2003) "Image Watermarking Algorithm Applying CDMA", *Proceedings of the IEEE International Symposium on Circuits and Systems* , Vol. 2, ppII-948-II-951.

[6] Arvind Kumar Parthasarathy, (2006) "Improved Content Based Watermarking for Images", M.S. Thesis, *Louisiana State University and Agricultural and Mechanical College,* Kanchipuram, India.

[7] Michael Wirth & Denis Nikitenko, (2010) "The Effect of Colour Space on Image Sharpening Algorithms", Canadian *Conference Computer and Robot Vision*, IEEE *Computer Society*, pp79-85.

[8] Zhuqing Jiao & Baoguo Xu, (2009) "An Image Enhancement Approach Using Retinex and YIQ", *International Conference on Information Technology and Computer Science*, IEEE *Computer Society*, Vol. 1, pp476-479.

[9] Wang Hui-qin & Hao Ji-chao, (2010) "Color Image Watermarking Algorithm Based on the Arnold Transform", *International Conference on Communications and Mobile Computing*, IEEE *Computer Society*, Vol 1, pp66-69.

[10] Steven H. Strogatz, (1994) "Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry and Engineering", Pursues Books, *Science Library*, Cambridge.

[11] Qian-Chuan Zhong & Qing-Xing Zhu & Ping-Li Zhang, (2008) "A Spatial Domain Color Watermarking Scheme Based on Chaos", *Proceedings of the International Conference on Apperceiving Computing and Intelligence Analysis* (ICACIA), IEEE, pp137-142.

[12] Yu Wei & Yanling Hao & Yushen Li, (2009) "A Multipurpose Digital Watermarking Algorithm of Color Image", *Proceedings of the* IEEE *International Conference on Mechatronics and Automation*, Changchun, China, pp112-117.

[13] M. Khalili, (2009) "A Comparison between Digital Images Watermarking in Two Different Color Spaces Using DWT2", CSIT, *Proceedings of the 7th International Conference on Computer Science and Information Technologies*, Yerevan, Armenia, pp 158-162.

[14] William A. Irizarry-Cruz, (2006) "FPGA Implementation of a Video Watermarking Algorithm", M.S. Thesis*, University of Puerto Rico Mayaguez Campus.*

[15] F. A. P. Petitcolas, (2000) "Watermarking schemes evaluation", *Proceedings of the* IEEE *Signal Processing*, Vol. 17, No. 5, pp58–64.

Author

Mehdi Khalili: **Ph.D. Student** in Computer engineering in the Institute for Informatics and Automation Problems in National Academy of Science of Armenia, **M.S. Degree** in Electrical-electronic engineering (2006-2008), **Bachelors Degree** in Electrical-electronic engineering (1998-2003). Number of published papers: 5. Number of published books: 2.