On Effective, Secure and Robust CDMA Digital Image Watermarking

Mehdi Khalili and David G. Asatryan

Institute for Informatics and Automation Problems of NAS RA

Russian-Armenian (Slavonic) University

e-mail: Khalili@ioia.sci.sm , dasat@ioia.sci.am

Abstract:

Digital watermarking has been widely used in digital rights management and copyright protection. In this paper, a new cryptographic CDMA watermark scheme is proposed. Compared to the existing watermarking techniques, this proposed watermarking scheme combine transparency, security and robustness that none of the existing schemes can do. In this paper, a wavelet-based watermarking approach for hiding watermark image in color host images is proposed. The experimental results show that the proposed approach provides extra imperceptibility, security and robustness against JPEG compression and different noise attacks such as Gaussian and "Salt & Papper" compared to the similar proposed methods such as [7]. Moreover, the proposed approach has no need of the original image to extract watermarks.

1. Introduction

Nowadays, watermarking of images is becoming increasingly of interest in tasks such as convright control, image identification, verification, and data hiding. 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 [1-3]. A variety of watermarking techniques has been proposed in recent years. 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 Code-Division Multiple Access (CDMA) digital images watermarking for ownership verification and image authentication applications, which for more security, 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. This adopting process uses a pseudo-random number generator to determine the pixel to be used on a given key. This adopted watermark embeds into the selected subbands coefficients of Y channel of YCbCr color space of host image using the correlation properties of additive pseudo-random noise patterns.

Watermarking in YCbCr color space versus image processing attacks is more robust than watermarking in RGB color space, and has higher transparency [4, 7]. Obtained results of the experiments show the efficiency of proposed technique in acceptable transparency, high security and robustness against JPEG compression and different noise attacks such as Gaussian and "Salt & Pepper" in comparing with earlier works such as [7].

2. 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. This scheme is based on the discrete wavelet transform (DWT). Moreover, it has no need of the original host image to extract the embedded watermarks: RGB color space is highly correlated and is not suitable for watermarking applications [8]. So, in the proposed scheme, the host image is converted into YCbCr channels; the Y channel is then decomposed into wavelet coefficients. For more security of watermark, the 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 watermark size. This adopting process uses a pseudo-random number generator to determine the pixel to be used on a given key. The selected 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:

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y} + k^*W_i & \text{if } W = 0 \\ I_{x,y}^*W_i & \text{Otherwise} \end{cases}$$
 (1)

In this equation k denotes a gain factor for completely controlling the imperceptibility of watermarked images and the robustness of watermarks and also $I_{l'l'}$ is the resulting watermarked image. 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 watermark, after converting watermarked image from RGB color space to YCbCr color space the Y channel will be decomposed into the wavelet coefficients. Then the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possible watermarked image in details subbands embedded coefficients will be computed. By computation of the each coefficient correlation with a certain threshold T, the watermark is detected, and a single bit is set.

2.1. Watermark embedding Framework

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 YCbCr channels using the CCIR 601 standard.

Step 2: For more security of watermark, the 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. Then, the encrypted watermark sequence W1 is generated by a pseudo-random number generator to determine the pixel to be used on a given key.

Step 3: Decompose the Y channel into a one-level wavelet structure with four DWT subbands, F(H). The coarsest coefficient of subbands HL and LH are taken as the target for embedding the watermark.

Step 4: Take absolute values on coefficients of all LH and HL, and record their signs in sign matrices.

Step 5: Quantize absolute values of selection coefficients.

Step 6: Embed encrypted watermark W1 into the coarsest coefficient of subbands HL and LH by the watermark embedding strategy shown in equation (1).

Step 7: Effect sign matrices into the embedded coefficients.

Step 8: Reconvert YCbCr channels of the changed host image into RGB channels.

Step 9: A watermarked image I' is then generated by inverse DWT with all changed and unchanged DWT coefficients.

Step 10: Record the pseudo-random noise generator algorithm and the key.

2.2. Watermark extracting Framework

The embedded watermark in details subbands coefficients of the Y channel of host image is extracted using the same pseudo-random noise generator algorithm is seeded with the same key, and computation of the correlation between the noise pattern and possible watermarked image as follows:

Step 1: The RGB channels of the watermarked image are converted into YCbCr channels.

Step 2: Decompose the Y channel into four DWT subbands.

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

Step 4: Quantize absolute values of HL and LH subbands.

Step 5: Computation of threshold T as follows:

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

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

Step 7: The sequence watermark is extracted as follows:

$$\begin{cases} W_i = 0 & \text{if} \quad C_i \rangle T \\ W_i = 1 & \text{Otherwise} \end{cases}$$
 (3)

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

3. Experimental Results

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

The proposed perceptual watermarking scheme was implemented for evaluating both properties of imperceptibility and robustness against different attacks such as JPEG compression and random noise.

Three 512×512 images: Lena, Peppers and Baboon, shown in Fig. 1(a-c) were taken as the host images to embed a 15×64 binary watermark image, shown in Fig 2(d). For gain factor k, different values 0.5, 1.0 and 1.5 were taken for entire implementation of the proposed CDMA scheme. For the entire test results in this paper, MATLAB R2007a software is used, too. 9 digit "key" used as initial state of MATLAB random number generator. Also for computation of the wavelet transforms, 9-7 biorthogonal spline (B-spline) wavelet filters are used. Cause of use of B-spline function wavelet is that, B-spline functions, do not have compact support, but are orthogonal and have better smoothness properties than other wavelet functions [9, 10].



Fig 1. (a-c) The host images (Lena, Peppers, and Baboon).

(d) The watermark image.

After watermark embedding process, the similarity of original host image x and watermarked image x' was measured by the standard correlation coefficient (Corr) as follows [4, 7 and 11]:

$$Correlation = \frac{\sum (x - x')(y - y')}{\sqrt{\sum (x - x')^2 \sum (y - y')^2}}.$$
(4)

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 [4, 7 and 11]:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} (dB),$$
 (5)

where mean-square error (MSE) is defined as [5, 7, 11, 12]:

$$MSE = \frac{1}{mn} \sum_{i=1}^{n} \sum_{j=1}^{n} (h_{i,j} - h'_{i,j})^{2},$$
 (6)

where $\psi_{i,j}$ and $\{\psi_{i,j}\}$ are the gray levels of pixels in the host and watermarked images, respectively. The larger *PSNR* is, the better the image quality is. In general, a watermarked image is acceptable by human perception if its *PSNR* is greater than 30 dB. 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 [4, 7, 11].

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 [4, 7, 1]]:

$$NC = \frac{\sum_{i} w_{i,j} * w'_{i,j}}{\sum_{i} \sum_{i} w_{i,j}^{-1}}$$
 (7)

The proposed CDMA watermarking scheme yields satisfactory results in watermark imperceptibility and robustness. The embedding of large watermarks using CDMA requires the embedding gain k to be lowered to preserve the visual quality of the image. 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 cause decreasing 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 PSNR of the watermarked images produced by the proposed scheme for different gain factors k are all greater than 84 dB, NC between original watermark images and extracted watermark images are all equal 1.

Image	k	PSNR (dB)	Corr	NC	Error Bit %
Lena	0.5	103.541	0.999	1.00	0
	1.0 .	91.720	0.997	1.00	0
	1.5	84.878	0.978	1.00	0
Baboon	0.5	103.541	0.999	1.00	0
	1.0	91.722	0,995	1.00	0
	1.5	84.803	0.982	1.00	0
Peppers	0.5	103.501	0.999	1.00	0
	1.0	91.586	0.993	1.00	0
	1.5	84.594	0.974	1.00	0

Table 1. Obtained results of watermark extracting by different values of the gain factor k

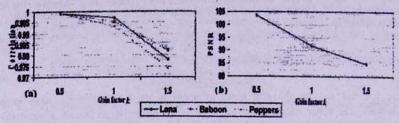


Fig 2. (a) Influence of the gain factor k on correlation.

(b) Influence of the gain factor k on PSNR.

The results for effecting k on PSNR, correlation between original images and watermarked images and NS between original watermark images and extracted watermark images are illustrated in Fig. 2 and Table 1. The correlation plot shown in Fig. 2 indicates that the margin of error is very small for the detection statistic. After being 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.

3.1. Robustness to Compression Attacks

To evaluate the response of the watermarking scheme to JPEG compression, watermarked images were compressed with different JPEG qualities Q. Fig. 3 shows the JPEG compression of the watermarked images under quality 10 and gain factor 1. Fig. 4 shows the extracted watermarks from watermarked images after JPEG compression under different qualities and different gain factors. Comparing with the similar references [12], whether the effect of he extracted watermark or the robustness to the JPEG compression has been improved greatly. To the similar references [7, 12], we compared the experimental results respectively under different JPEG qualities and gain factors.



Fig 3. Watermarked images under JPEG compression (Q=10, k=1).

(a) Lena, (b) peppers and (c) Baboon



Fig 4. Extracted watermarks from watermarked images after JPEG compression at different values for Q and k. (a) Lena, (b) Baboon, and (c) Peppers.

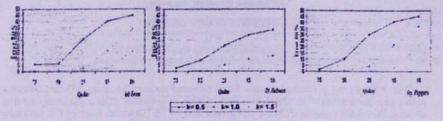


Fig 5. The percentage of error bit in extracted watermarks in JPEG compression under deferent qualities and gain factors.

The percentage of the error bit for extracted watermarks under JPEG compression is shown in Fig. 5. As it is seen, the percentage of error bit plot shown above indicates that the margin of error is very small for the detection statistic, and CDMA proposed scheme has increased in comparing with the earlier works such as [7]. Table (2), shows the response of the detector to extract the watermark in JPEG compression. From the above 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 watermark for a quality factor of 25 and gain factor 1 shows a number of detection errors and this becomes highly noticeable only 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. The overall robustness of proposed scheme for JPEG compression is considered as high level, according to the robustness requirements table provided by Petitcolas [13] and is higher than earlier works such as [7]. It can be seen that the proposed scheme is more robust than earlier works such as [7] against JPEG compression, even for low JPEG quality.

3.2. Robustness to Noise Attacks

The CDMA proposed scheme was tested for its robustness against different types of noise. This is done by first introducing noise into the watermarked images. Gaussian noise with zero mean is introduced to verify as to what extent the proposed scheme can withstand noise. 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 [14].

Fig. 6 shows added Gaussian noise of 0.5 % with gain factor 1 to watermarked images. Fig.

7 shows the extracted watermarks in Gaussian noise of 1 % with different gain factors.



Fig 6. Watermarked images under Gaussian noise of 0.5 % at gain factor 1. (a) Lena, (b) Peppers and (c) Baboon.

Fig 7. Extracted watermarks from Gaussian noise of 1 % with different gain factors. (a) Lena, (b) Baboon and (c) Peppers.

Fig. 8 shows the percentage of error bit in extracted watermarks under different Gaussian noises gain factors. Fig. 9 shows the results of PSNR in Gaussian noise experiment. As it is obvious, the lowest value for PSNR is still greater than 47 dB (Gaussian noise of 1 % with gain factor 0.5). Fig. 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 the 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 [7]. When the "Salt & Pepper" noise with zero mean and different variance of 0.01 to 0.5 with different gain factor introduced in the watermarked images, the extracted watermarks are recognizable in gain factor 0.5 and variance 0.5, they are recovered in gain factor 1 and variance 0.5 moderately and they are recovered in gain factor 1.5 and variance 0.5 with a few detection errors. Fig. 11 shows the watermarked images under "Salt & Pepper" noise attacks with variance of 0.5 and gain factor 1. Fig. 12 shows the extracted watermarks from noisy watermarked images under variance 0.5 with different gain factors, and Fig. 13 shows the percentage of error bit in extracted watermarks under different variance of "Salt & Pepper" noise with different gain factors.

The results in "Salt & Pepper" noise experiment are shown in Fig. 14. As it is obvious, the lowest value for PSNR is still greater than 50 (Gaussian noise of 1 % with gain factor 0.5).

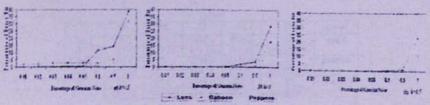


Fig 8. Percentage of error bit under different percentage of Gaussian noise.

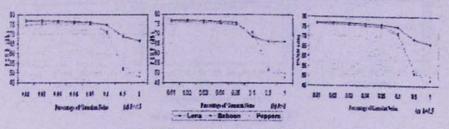


Fig 9. PSNR under Gaussian noise experiment.

Fig. 15 shows the NC results in "Salt & Pepper" noise experiment. The obtained results show that, NC in "Salt & Pepper" noise experiment is acceptable for variance of 0.5 with the gain factor 0.5, it is moderate for the same variance with the gain factor 1 and it is near to perfect for the same variance 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 and it improves the results in the earlier works such as [7].

Table 2. Obtained results of extracted watermarks in JPEG compression under different qualities and gain factors

			k=0.5			
Image	Q	10	15	25	50	75
Lena	NC	0.1105	0.2136	0.5055	0.8735	0.9884
	PSNR(db)	90.173	92,628	95.272	98.319	99.998
Baboon	NC	0.3565	0.4449	0.6173	0.8242	0.9441
	PSNR(db)	79.775	81.351	83.170	85.748	88.519
Peppers	NC	0.0987	0.1959	0.4156	0.800	0.9681
	PSNR(db)	85.741	87,686	89.554	91.769	93.862
			k=1.0		77	
Image	Q	10	15	25	50	75
Lena	NC	0.3286	0.6893	0.9441	1.00	1.00
	PSNR(db)	86.031	0.965	89.439	92,308	97 279
Baboon	NC	0.6085	0.7633	0.8923	0.9907	1.00
	PSNR(db)	78.391	79.828	81.581	84.352	87.846
Peppers	NC	0.2741	0.6027	0.9129	0.9977	1.00
	PSNR(db)	83.002	84.422	85.987	88.296	91.688

k=1.5							
Image	Q	10	15	25	50	75	
Lena	NC	0.6905	0.9481	0.9953	1.00	1.00	
	PSNR(db)	81.946	83.175	84.915	88,737	95.219	
Baboon	NC	0.8071	0.9502	0.9815	1.00	1,00	
	PSNR(db)	76.573	77,935	79.722	83.116	87.369	
Peppers	NC	0.6020	0.9293	1.00	1.00	1.00	
	PSNR(db)	79.792	80.962	82.543	85.682	90.450	

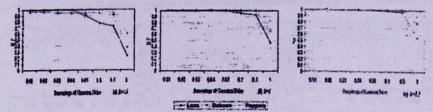


Fig 10. NC in Gaussian noise experiment.

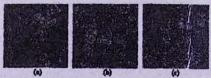


Fig 11. "Salt & Pepper" noise on watermarked images with variance 0.5.

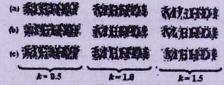


Fig 12. Extracted watermarks from "Salt & Pepper" noise with different gain factors.

(a) Lena, (b) Baboon and (c) Peppers.

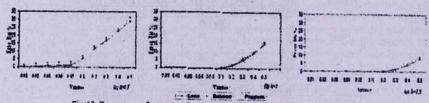


Fig 13. Percentage of error bit under different variances of "Salt & Pepper" noise.

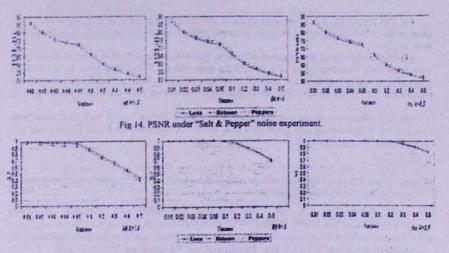


Fig 15. NC under "Salt & Pepper" noise experiment.

4. Conclusions

This paper provides a novel CDMA watermarking scheme using DWT2 with satisfactory results in watermark imperceptibility, robustness and security that improves upon the earlier work such as [7]. In the scheme, the host image is converted into YUV channels; then, the Y channel is decomposed into wavelet coefficients. For more security of watermark, the 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 using a pseudo-random number generator to determine the pixel to be used on a given key. The selected details subbands coefficients for embedding are quantized and then their most significant coefficients are replaced by the adopted 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 different noise attacks such as Gaussian and "Salt & Pepper". 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

(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, and it is recognizable for a Gaussian noise of 1 % with the gain factor 0.5. These results show the improving in comparing with the earlier works such as [7].

(5) The robustness of the proposed scheme to "Salt & Pepper" noise with zero mean with variance 0.5 is found to be very good for a gain factor 1.5, it is good for a gain factor 1 and it is

recognizable for a gain factor 0.5.

References

- [1] Jian. Ren, "A cryptographic watermarking technique for multimedia signals", Springer Science, Business Media, August 2008.
- [2] S.-H. Wang and Y.-P Lin, "Wavelet tree quantization for copyright protection watermarking", IEEE Trans, Image Process , vol.13, no. 2, pp. 154-165, 2004.
- [3] H.S. Malvar, D.A.F Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking", IEEE Trans. Signal Proc., vol. 51, no. 4, pp. 898-905, 2003.
- [4] X.G. Xia, C. G. Boncelet and G. R. Arce, "Wavelet transform based watermark for digital images", Optics Express, vol. m, no. 12, pp.497-511, 1998.
- [5] M. Khalili, "A comparison between digital images watermarking in two different color spaces using DWT2", Proceedings of the 7th International Conference on Computer Science and Information Technologies, pp. 158-162, Yerevan, Armenia, 2009.
- [6] M. Khalili and D. Asatryan, "Effective digital image watermarking in YCbCr color space accompanied by presenting a novel technique using DWT", Mathematical Problems of Computer Science, vol. 33, pp. 150-161, 2010.
- [7] Y. Fang, J. Huang and Yun Q. Shi, "Image watermarking algorithm applying CDMA", IEEE International Symposium on Circuits and Systems(ISCAS03), Bangkok, Thailand, May, pp. 948-951, 2003.
- [8] Oian-Chuan Zhong, Qing-Xin, Ping- Li- Zhang, "A Spatial Domain Color Watermarking Scheme Based on Chaos", IEEE International Conference on Apperceiving Computing and Intelligence Analysis, 2008. ICACIA, pp. 137-142, 2008.
- [9] X.G. Xia, C. G. Boncelet and G. R. Arce, "Wavelet transform based watermark for digital images", Optics Express, vol. m, no. 12, pp.497-511, 1998.
- [10]C. Lin, "Face detection in complicated backgrounds and different illumination conditions by using YCbCr color space and neural network", Elsevier, Pattern Recognition Letters 28 (2007), pp. 2190-2200, 2007.
- [11] M.-S. Hsieh, "Wavelet-based image watermarking and compression", Ph-D Thesis, Institute of Computer Science and Information Engineering National Central University, Taiwan, Dec. 2001.
- [12] A. William and Irizarry-Cruz, "FPGA implementation of a video watermarking algorithm", M.S. Thesis, University of Puerto Rico Mayaguez Campus, 2006.
- [13] F. A. P. Petitcolas, "Watermarking schemes evaluation" IEEE Signal Processing, vol. 17, no. 5, pp. 58-64, 2000.

[14] Arvind Kumar Parthasarathy, "Improved content based watermarking for images", M.S. Thesis, Submitted to the Graduate Faculty of the Louisiana State University and Agricultural and Mechanical College in partial fulfillment of the requirements, 2006.

CDMA պատկերի թվային արդյունավետ, վստահելի և կայուն ջրանշման մասին

Մ. Խալիլի և Դ. Ասատրյան

Ulihnhnul

Թվային ջրանշումը լայնորեն կիրառվում է հեղինակային իրավունքի պաշտպանության րնագավառում։ Հողվածում առաջարկվել է ջրանշման CDMA ծածկագրական նոր սխեմա։ Առաջարկված ջրանշման սխեման համակցում է թափանցիկության, վստահելիության և կայունության այնպիսի հատկություններ, որոնք ի զորու չէ ապահովելու գոյություն ունեցող ջրանշման սխեմաներից ոչ մեկը։ Մույն հոդվածում գունավոր պատկերներում ջրանիշի տեղակայման համար առաջարկվել է վեյվլետների կիրառման վրա հիմնված մոտեցում,: Փորձի տվյալները ցույց են տալիս, որ առաջարկված մոտեցումը նմանատիպ այլ մեթոդների (ինչպես օրինակ՝ [7]) նկատմամբ ապահովում է լրացուցիչ թափանցիկություն, վստահելիություն և կայունություն JPEG սեղմման և տարբեր պատահական աղմուկների, ինչպես օրինակ՝ գառայան, "աղ և պղպեղ" տեսակի, նկատմամբ։ Ավելին, առաջարկված մոտեցումը ջրանիշի արտածման համար չի պահանջում ջրանիշի բնօրինակի առկայությունը։