Chaotic Digital Image Watermarking Scheme Based on DWT and SVD

Gökçen ÇETİNEL¹, LLukman ÇERKEZI²,

^{1, 2} Electrical and Electronics Engineering Dept., Sakarya University, Turkey gcetinel@sakarya.edu.tr, llukmancerkezi@gmail.com

Abstract

In this study chaos based digital watermarking scheme together with Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) is proposed. In the proposed watermarking scheme, the cover image is decomposed to its sub-bands (LL, LH, HL and HH) by a common used frequency domain transform: DWT. Then, the SVD is directly applied to the all sub-bands of the decomposed cover image. The watermark is shuffled with Arnold's Cat Map (ACM) to generate a chaotic watermark. By this way, the robustness and perceptual invisibility of the scheme is improved. In order to evaluate the robustness of the proposed scheme, several image processing and geometric attacks are applied to the scheme. The Normalized correlation (NC) and peak signal-to-noise ratio (PSNR) measures are used to show the performance of the proposed method in terms of robustness and perceptual invisibility. The proposed algorithm gives the promising results and meets the security requirements.

1. Introduction

In recent years digital watermarking has gained great deal of importance with the explosion of the digital media. Several digital watermarking techniques are developed to prevent the unpermitted data transmission and protect the data from the intentional and unintentional attacks. The goal of the digital image watermarking techniques is to embed a secret signal called as watermark to the cover image. The most common applications of the digital watermarking methods are copyright protection, broadcast monitoring, tamper detection, authentication and integrity verification, fingerprinting, content description and secure communication.

Digital watermarking schemes can be classified in different ways. According to the watermark embedding domain, digital watermarking methods can be categorized as spatial domain methods and transform domain methods. In the spatial domain watermarking methods, watermark is directly embedded into the cover image. After embedding process, only the pixel values of the cover image change. On the other hand, in the transform domain watermarking methods, embedding is performed in the transform domain by applying a technique such as Finite Ridgelet Transform (FRIT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Redundant Discrete Wavelet Transform (RDWT) to the cover image. Then the obtained coefficients are modified according to the method. Consequently, the spatial domain methods are easier and less time consuming than the transform domain methods. However, they cannot ensure a good robustness against the common image processing and geometric attacks [1].

The watermarking applications have to meet some specific requirements. There are three main requirements common to most of the applications. They are perceptual invisibility, capacity and robustness. Perceptual invisibility or fidelity can be defined as the perceptual similarity between the original and watermarked data. The number of information bits (watermark) embedded into the original data denotes the capacity of the watermark scheme. Finally, robustness is the ability of detecting watermark that is subject to the common signal processing attacks [1, 2].

SVD is a complementary technique for transform domain techniques and used in the most popular studies about the watermarking. SVD can be applied directly to the image matrix and always shows a good performance. The transform domain techniques utilizing the properties of SVD are referred as the hybrid watermarking techniques in the literature and can be found in [3-5].

In this study, a chaos based hybrid digital image watermarking scheme based on DWT and SVD is proposed. ACM that transforms the original watermark image into the chaotic image pattern is combined to the watermarking scheme to improve the robustness and perceptual invisibility. Digital image watermarking schemes with chaos present in the literature are investigated to evaluate the performance of our method. There are several digital image watermarking schemes in the transform domain that utilizes the properties of the chaos [6-9]. The study is organized as follows. In Section 2, brief information about the ACM is given. To better understand the proposed algorithm, DWT and SVD techniques are introduced in Section 3 and 4, respectively. In Section 5, watermark embedding and extracting algorithms are discussed with all steps. Section 6 illustrates the simulation results to evaluate the performance of the algorithm. Finally, Section 7 concludes the paper.

2. Arnold's Cat Map

Chaotic signals are mainly used in secure communications, signal processing and cryptography because of their inherent properties that can be taken into account as complexity, orthogonality and having broad-band spectrum. As a result, many crucial chaos-based algorithms have been proposed for image processing applications to show whether the performance increase is possible compared to the other applications.

There are several maps appropriate for image processing algorithms. ACM is one of the most famous chaotic maps used for randomizing the pixel locations in the image matrix. This randomizing provides security augmentation for the image watermarking schemes. 2D-ACM for *NxN* square image matrix can be expressed as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod \ N = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod \ N$$
(1)

where (x_n, y_n) and (x_{n+1}, y_{n+1}) are the locations of pixels before and after iterations, respectively. In the above equation *a* and *b* are the positive integers provided that the det(A)=1 [7, 10].

After a few iterations locations of pixels will be scrambled but when the transformation is repeated enough we will attain the original image matrix again. ACM transformation for different iteration numbers are illustrated in Fig. 1. According to the figure, we can say that original watermark is obtained after 40^{th} iterations. Thus, the number of iterations in the watermark extracting process is determined by the number of iterations *X* in the embedding process as, 40-*X*. In this study the size of the binary watermark is 77x77.



Fig. 1.(a) Original watermark and scrambled watermarks after related number of iterations in ACM: (b) 2, (c) 15, (d) 21, (e) 37 and (f) 40.

3. Discrete Wavelet Transform

As we discussed in Section 1, DWT is a common used method in watermarking schemes that transforms the image from the pixel domain to the frequency domain. It is proven that the DWT is superior the widely used DCT in watermarking schemes. DWT is a mathematical tool that splits a one dimensional signal into low-frequency and high-frequency parts. This process is called as decomposition. In DWT, high-pass and low-pass filter are used to analyze the high and low frequencies of the signal. The outputs of the filters are called as DWT coefficients and the original signal can be reconstructed by using them. This reconstruction is referred as inverse DWT (IDWT) [1].

By performing DWT one time, the cover image is divided into four sub-bands i.e.LL₁, LH₁, HL₁, HH₁, LL₁ is the low frequency component and has the maximum power of energy while the other sub-bands are middle and high frequency subbands. These sub-bands represent the edges, outline, texture and other detail information in an image. If we want to decompose the image to narrower frequency sub-bands, we should apply the DWT to the LL₁ sub-band, again. This process can be repeated until we get the desired composition level of wavelet transformation. In Fig. 2., three level DWT decomposition is illustrated.

LL ₃	HL ₃	HL_2	
LH ₃	HH ₃		HL_1
LH	2	HH_2	
	HH_1		

Fig. 2. The 3- level DWT decomposition scheme.

Watermark embedding is performed by changing the DWT coefficients according to the algorithm. We can embed the watermark either in low frequency sub-band or in high frequency sub-band. Embedding watermark to the high frequency sub-band provides high imperceptibility advantage but robustness and stability of the scheme are decreased. Robustness can be improved by embedding watermark to the middle and low frequency sub-bands but this causes the lack of imperceptibility.

4. Singular Value Decomposition

SVD is an efficiently used technique in image and signal processing applications such as image compression, data hiding, noise reduction and image watermarking. Singular value decomposition can be applied directly to the image matrix with any dimensions. Given the data matrix \mathbf{A} which has the W linearly independent column (i.e. rank (\mathbf{A})=W), there are two unitary matrices V and U such that,

$$A = \mathbf{U}\mathbf{S}\mathbf{V}^T \quad (2)$$

where **S**= diag (σ_1 , σ_2 , ..., σ_W) is a diagonal matrix. Singular values (σ 's) are ordered as $\sigma_1 \ge \sigma_2 \ge ... \ge \sigma_W > 0$. This equation is the mathematical statement of the SVD theorem and also referred as Autonne- Eckart- Young theorem [11].

SVD is an optimal decomposition method that can concentrates the maximum signal energy into as few coefficients as possible. From the image processing point of view, SVD has three main advantages important in image processing applications [3, 4]. These advantages can be summarized as follows:

- 1. The image matrix not has to be square matrix. It can be any dimension.
- SVD puts forward the algebraic properties of an image where singular values correspond to the brightness of the image and U and V denotes the geometric properties of the image.
- 3. The slight variations of singular values of an image may not affect the human visual perception. This stability property of SVD is the main reason why it is preferred for watermarking applications.

4. Proposed Method

A general watermarking system consists of two main units: the watermark embedding unit and the watermark detection/ extraction unit. Both units can be considered as a separate

process. In the following subsections, watermark embedding and extracting processes for the proposed method are explained.

5.1. Watermark Embedding Algorithm

The steps of the proposed embedding algorithm are as follows:

Step 1: Apply 21 iteration ACM to the original watermark, W, in order to get chaotic watermark image, W_{ACM} .

Step 2: Perform 3- level DWT to the cover image to decompose it into LL_3 , LH_3 , HL_3 , HH_3 sub-bands.

Step3: Apply SVD to the chaotic watermark image, \mathbf{W}_{ACM} as follows:

$$\boldsymbol{W}_{ACM} = \boldsymbol{U}_{ACM} \boldsymbol{S}_{ACM} \boldsymbol{V}_{ACM}^T \qquad (3)$$

Step 4: Apply SVD to all sub-bands of the cover image (LL3, LH₃, HL₃, HL₃, HH₃), as follows:

$$\boldsymbol{A}^{i} = \boldsymbol{U}^{i} \boldsymbol{S}^{i} \boldsymbol{V}^{i^{T}} \tag{4}$$

where *i* indicates the sub-bands (i.e., LL₃, LH₃, HL₃, HH₃).

Step 5: Modify the singular values S^i with singular values S_{ACM} of chaotic watermark image

$$\boldsymbol{S}^{*i} = \boldsymbol{S}^i + \alpha \boldsymbol{S}_{ACM} \tag{5}$$

where α is scaling factor fixed for all sub-bands and *i* denotes the sub-bands.

Step 6: Apply inverse SVD on the transformed cover image with modified singular values as follows:

$$\boldsymbol{A}^{*i} = \boldsymbol{U}^i \boldsymbol{S}^{*i} \boldsymbol{V}^{i^T} \tag{6}$$

where *i* indicates the sub-bands (i.e., LL_3 , LH_3 , HL_3 , HH_3), again.

Step 7: Finally, perform inverse 3-level DWT using the modified coefficients to construct the watermarked image.

In this study, watermark is embedded to the LL_3 , LH_3 , HL_3 , HH_3 sub-bands, separately. Imperceptibility and robustness evaluated by the computer simulations under the most common attacks are very close for all sub-bands because of inserting ACM, SVD and DWT in the watermarking scheme.

5.2. Watermark Extraction Algorithm

The watermark extraction steps are given below:

Step 1: Perform 3- level DWT to the watermarked image A_{W}^* , obtaining LL3^{*}, LH₃^{*}, HL₃^{*} and HH₃^{*}sub-bands.

Step 2: Apply SVD to all sub-bands, as follows:

$$\boldsymbol{A}^{*i} = \boldsymbol{U}^{*i} \boldsymbol{S}^{*i} \boldsymbol{V}^{*i^{T}}$$
(7)

where *i* indicates the sub-bands (i.e., LL_3^* , LH_3^* , HL_3^* , HH_3^*). *Step 3*: Calculate the singular values S^{W} as follows:

$$\boldsymbol{S}^{W} = (\boldsymbol{S}^{*i} - \boldsymbol{S}^{i})/\alpha \qquad (8)$$

where S^{i} , s are the singular values of the cover image for all subbands, individually.

Step 4: Apply inverse SVD, in order to get extracted chaotic watermark image:

$$\boldsymbol{W}_{ACM}^* = \boldsymbol{U}^i \boldsymbol{S}^w \boldsymbol{V}^{i^T} \tag{9}$$

Step 5: Apply (40 - 21 = 19) iterations to W^*_{ACM} in order to get finally extracted original watermark.

6. Experimental Results

In order to check our proposed algorithm we used gray scale Lena and Cameraman image as cover image of size 512 x 512 and the binary logo 'LL' as watermark image of size 77 x 77. All simulations are implemented by using MATLAB. Fig.(3). demonstrates the cover image, watermark, chaotic binary logo obtained by applying 21 iterations ACM, watermarked image, extracted chaotic watermark and the extracted original watermark, respectively.

After watermark extraction process, PSNR (Peak Signal to Noise Ratio) criterion that can be defined as the similarity between watermarked and cover image is calculated by using the following equation:

$$PSNR = 10 \log_{10} \left[\frac{\max\left((X(i,j))^2 \right)}{MSE} \right]$$
(10)

where MSE (Mean Square Error), which implies the noise energy, is defined as :

$$MSE = \frac{1}{mxn} \sum_{i=1}^{m} \sum_{j=1}^{n} [X(i,j) - Y(i,j)]^2$$
(11)

In Equation (11), m and n are dimensions of the image X and Y. In our simulations, we measure the PSNR between original watermark and extracted watermark. PSNR values are usually given in (dB) and larger values of PSNR such as 30 dB and higher indicate better watermark concealment.

NC (Normalized Correlation) is a parameter used to measure robustness that is another important requirement for any watermarking scheme.NC indicates the similarity between binary logo and logo extracted from the extraction process after attack. Mathematically it can be expressed as:

$$NC = \frac{\sum_{k=1}^{m} \sum_{j=1}^{n} [W(k,j)W'(k,j)]}{\sqrt{\sum_{k=1}^{m} \sum_{j=1}^{n} [W(k,j)]^2} \sqrt{\sum_{k=1}^{m} \sum_{j=1}^{n} [W'(k,j)]^2}}$$
(12)

where **W** and **W**' represent the original and extracted watermark, respectively. The correlation coefficient can take values from the interval [-1, 1]. If it is near 0, the extracted watermark is completely uncorrelated. Generally, the NC is considered acceptable if it is 0.75 or above [5, 12].

In order to investigate the robustness and imperceptibility of our proposed scheme, the watermarked image was attacked by applying salt & pepper noise, Gaussian noise, Poisson noise, histogram equalization, contrast adjustment, wiener filter [3x3],

median filter [3x3], speckle noise, JPEG compression and rotation. DWT based digital image watermarking scheme that uses the features of the logistic map in the embedding and extraction steps is proposed in [8]. To show the advantages of our method, comparative results with [8] are given in Table 1. In Table 1, NC values under different attacks are given to show the robustness of our method for all bands. The higher values are denoted with bold numbers. As can be seen from the Table 1, the proposed chaos based digital watermarking algorithm with SVD and DWT is providing considerably high robustness against the most common attacks.

In Table 2, NC and PSNR values of the proposed method are given in all bands for Lena and Cameraman cover images. The values calculated for Cameraman cover image are denoted with italic numbers in the table. Seventeen attacks are applied to the watermarking scheme in this experiment. The results show that the proposed digital image watermarking scheme is robust against to the most common attacks and meets the perceptual invisibility requirement of the watermarking schemes.

In Fig.4, watermarked image under a few attacks are illustrated. The PSNR values between the cover image and watermarked image is given in parenthesis. Because of the limitations on the number of pages, the watermarked image is given just for some of the attacks.

7. Conclusion

In this study, digital watermarking algorithm based on DWT, SVD and ACM is presented. As discussed in the sections of the paper, SVD is a very convenient tool for watermarking schemes performing in the DWT domain. Therefore, in our hybrid algorithm we used SVD together with DWT. Because of the known specific properties of the chaos especially in signal processing applications, we combined ACM to the proposed scheme to meet the security requirements. PSNR and NC measures are calculated for different cover images in all subbands to evaluate the performance of the proposed method. The proposed method is also compared with a current chaos based digital image watermarking scheme. Experimental results show that the proposed method is robust against the most common attacks and meets the security requirement of the watermarking schemes.



Fig. 3. (a) Cover Image (512×512 Lena), (b) Binary logowatermark (77×77), (c) Chaotic binary logo, (d) watermarked image, (e) extracted chaotic watermark, (f) extracted original watermark.



Fig. 4.Watermarked image under several attacks. (a) Salt & Pepper (var= 0.005), (56.38 (dB)),(b) Gaussian Noise (var= 0.001), (49.36 (dB)), (c) Gaussian Noise (var= 0.05), (35.75 (dB)), (d) histogram equalization (33.8525 (dB)), (e) contrast adjustment (35.12 (dB)), (f) speckle noise (var= 0.01), (42.26 (dB))

 Table 1. Comparison results of NC values between proposed scheme and Khare et al[8].

	L	L	LH		HL		HH	
Attacks	[8]	Ours	[8]	Ours	[8]	Ours	[8]	Ours
Gaussian Noise (0.01)	0.979	0.851	0.974	0.960	0.951	0.913	0.985	0.965
Contrast Enhancement	0.970	0.977	0.981	0.993	0.986	0.994	0.987	0.997
Average Filtering	0.983	0.992	0.955	0.981	0.987	0.997	0.976	0.972
Median Filtering	0.961	0.993	0.953	0.981	0.974	0.997	0.931	0.973
Gamma Correction	0.973	0.999	0.991	0.999	0.991	0.997	0.998	0.999
Histogram Equalization	0.975	0.974	0.978	0.991	0.981	0.994	0.980	0.996
Wiener Filtering	0.979	0.988	0.998	0.993	0.995	0.992	0.962	0.983
JPEG (50)	-	0.977	-	0.993	-	0.854	-	0.975

("-" denotes the value does not exist in corresponding study.)

	LL		HL		LH		HH	
Attacks	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
Salt&Pepper(var	0.9990	74.9372	0.9966	67.2580	0.9982	69.9036	0.9989	72.1557
0.001)	0.9936	65.5565	0.9947	57.8288	0.9979	52.0944	0.9974	58.8756
Salt&Pepper(var	0.9938	66.9966	0.9831	62.0005	0.9955	66.2591	0.9931	63.4295
0.005)	0.9906	65.1130	0.9905	58.0767	0.9912	51.6129	0.9877	55.2503
Salt&Pepper(var	0.9885	64.2959	0.9855	58.9737	0.9893	63.6980	0.9871	59.8822
0.01)	0.9665	59.9923	0.9784	56.3609	0.9718	51.0023	0.9867	55.3219
Salt&Pepper(var	0.8256	53.0939	0.9585	47.9444	0.9602	51.9295	0.9518	47.2206
0.05)	0.7265	49.6725	0.9424	47.8014	0.9052	47.5211	0.9623	46.8338
Gaussian Noise	0.9952	66.2858	0.9934	65.5344	0.9960	68.8256	0.9952	66.2592
(var = 0.001)	0.9914	64.9980	0.9931	57.1841	0.9905	50.9433	0.9937	54.8286
Gaussian Noise	0.9827	56.2390	0.9792	55.6396	0.9854	57.8249	0.9792	54.0747
(var= 0.005)	0.9280	53.5154	0.9663	54.3311	0.9483	49.1942	0.9718	51.0585
Gaussian Noise	0.9510	51.1713	0.9709	50.7160	0.9782	52.5021	0.9700	50.1253
(var= 0.01)	0.8516	48.8959	0.9607	49.7779	0.9137	47.9220	0.9655	49.6661
Gaussian Noise	0.6528	38.5996	0.9644	39.6235	0.9496	42.6086	0.9685	39.5609
(var= 0.05)	0.6806	38.7769	0.9653	41.0077	0.8846	42.1383	0.9674	39.8649
Poisson Noise	0.9909	64.6738	0.9916	63.2975	0.9948	65.8062	0.9912	61.5429
Poisson Noise	0.9974	61.6287	0.9777	56.2685	0.9753	51.2034	0.9777	53.9909
Histogram	0.9745	32.5982	0.9949	42.6029	0.9916	40.2104	0.9967	41.5807
Equalization	0.9762	43.9370	0.9864	43.5188	0.9862	46.8931	0.9862	46.3495
Contrast	0.9771	34.0830	0.9945	44.8962	0.9931	42.6766	0.9979	44.7096
Adjustment	0.9707	31.9373	0.9952	51.0624	0.9915	48.6690	0.9959	52.1178
Wiener Filter [3v3]	0.9888	62.8137	0.9927	52.6239	0.9934	54.7920	0.9831	50.3758
whener Priter [5x5]	0.9906	61.4984	0.9887	50.3623	0.9914	47.8345	0.9810	48.1274
Median Filter [3x3]	0.9937	64.1797	0.9977	52.7629	0.9813	53.6070	0.9735	47.3619
	0.9901	62.4765	0.9860	51.3897	0.9757	47.7819	0.9776	45.9702
Speckle Noise	0.9876	63.3280	0.9871	61.5260	0.9906	62.0874	0.9855	59.2274
(var=0.01)	0.9664	60.0561	0.9731	55.9425	0.9594	50.3564	0.9817	54.0012
IPEG O=25	0.9725	51.3872	0.9963	64.9863	0.9908	59.5707	0.9915	59.1090
JEEU Q-25	0.9202	52.3483	0.9897	54.4521	0.8387	45.2749	0.9744	43.8541
JPEG Q=50	0.9725	51.3875	0.9965	65.0541	0.9932	62.5538	0.9979	63.5272
	0.9771	71.9262	0.9930	54.8623	0.8540	45.4421	0.9757	44.3329
Rotation 2	0.9463	35.4852	0.9480	41.4470	0.9782	41.8661	0.8720	40.7455
	0.8287	33.4206	0.9378	42.9997	0.9493	40.8659	0.9258	41.6365

Table 2. The NC and PSNR values of the proposed algorithm in all sub-bands for Lena and Cameraman cover images.

8. References

[1] N.Terzija, "Robust Digital Image Watermarking Algorithms for Copyright Protection", PhD thesis, Faculty of Engineering, Duisburg Essen University, October 2006.

[2]P. Dong, "Robust Digital Image Watermarking", PhD thesis, Electrical Engineering in the Graduate College of the Illinois Institute of Technology, May 2004.

[3] S. Lagzian, M. Soryani and M.Fathy,"A New Robust Scheme Based on RDWT-SVD", *International Journal of Communications*, vol. 67, pp. 102-112, 2013.

[4] SR. Haque, "Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking", Master's thesis. Department of Interaction and System Design, School of Engineering, Sweden, Blekinge Institute of Technology, 2008.

[5] S. Rastegar, et. al., "Watermarking Algorithm Based on Singular Value Decomposition and Radon Transorm",*International Journal of Communications*, vol. 65, no. 7, pp. 658-663, 2011.

[6] G.S. Kalra, R. Talwar, H.Sadawarti, "Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique",*International Conference on Computational* Intelligence, Communication Systems and Networks, 2011, pp. 225-230.

[7] O. Jane, H.K. Ilk, E. Elbasi, "A Secure and Robust Watermarking Algorithm Based on the Combination of DWT, SVD and LU Decomposition with Arnold's Cat Map Approach", *8th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, 2013, pp. 306-310.

[8] P.Khare, A.K. Verma, V.K. Srivastava, "Digital Image Watermarking in Wavelet Domain Using Chaotic Encryption", *Students Conference on Engineering and Systems*, Allahabad, 2014, pp. 1-4.

[9] L. Kocarev, Z. Galias, and S. Lian (Eds.), A. Mooney, "Intel. Computing Based on Chaos/ Chaos BasedDigitalWatermarking", Springer-Verlag, Berlin, Heidelberg, 2009, pp. 315-332.

[10] S. Ramat, B. Raman, "A Chaotic System Based Fragile Watermarking Scheme for Image Tamper Detection", *International Journal of Communications*, vol. 65, pp. 840-847, October, 2011.

[11] S. Haykin, "AdaptiveFilterTheory", PrenticeHall, New Jersey, 4.th edt., 2002.

[12] A.Al-Haj, "Combined DWT-DCT Digital Image Watermarking", *Journal of Computer Science*, vol.3, vo.9, pp. 740-746, 2007.