A Secure and Robust Watermarking Algorithm Based on the Combination of DWT, SVD, and LU Decomposition with Arnold's Cat Map Approach

Onur Jane[1], Hakkı Gökhan İlk[2], and Ersin Elbaşı[1]

[1]The Scientific and Technological Research Council of Turkey (TÜBİTAK), Ankara, Turkey
onur.jane@tubitak.gov.tr, ersin.elbasi@tubitak.gov.tr
[2]The Department of Electrical and Electronics Engineering, Ankara University, Turkey
ilk@ieee.org

Abstract

Watermarking, in particular, is identified as a major technology to achieve copyright protection and multimedia security. In this study, combination of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) via Lower-and-Upper (LU) Decomposition is proposed as a new watermarking algorithm with a chaotic map approach called Arnold's Cat Map (ACM). Similarity Ratio (SR) and Peak Signal-to-Noise Ratio (PSNR) values in this algorithm, as quality metrics, are greater than that of in the algorithms without chaotic mapping. Apart from robustness, imperceptibility, reliability, and security; the other novel side of this study is to expand the application areas of watermarking with a new algorithm consisting DWT, SVD, and LU with ACM together.

1. Introduction

Digital watermarking is the process that embeds data called watermark into a multimedia object (such as text, audio, image, and video) such that watermark can be detected or extracted later to make an assertion about the object [1]. Digital watermarking has received increasing attention especially in recent years. For the purpose of designing and developing a new watermarking algorithm, the most important properties are robustness, invisibility and security [2] which are the focal point of this study.

There are basically two ways to embed a watermark in: spatial domain and transform domain. While the principle of spatial domain watermarking is to modify the host image pixel values, the principle of transform domain watermarking is to modify transform coefficients with an appropriate algorithm [3, 4]. Spatial domain embedding techniques are very simple and effective, but they are not robust against many attacks [5]. Hence in this study, a new watermarking algorithm in combination of DWT and SVD via LU decomposition will be implemented.

Due to its great frequency component separation properties, the DWT, in contrast to DCT, is very useful to identify the coefficients to be watermarked [6]. Studies in [6-9] show that DWT understands the human visual system more closely in comparison to the DCT. In general, most of the image energy is concentrated at the lower frequency coefficient sets LLs and therefore embedding watermarks in these coefficient sets may degrade the image significantly. However, embedding watermark in the LL bands increase robustness effectively. The fact that makes our study novel is that we will increase robustness of the watermarked image under certain attacks without degrading the image by embedding binary watermark on LL band.

Apart from DWT, SVD in Equation (1) not only decomposes the image, F, into left (U) and right (V) singular vectors which represent horizontal and vertical details respectively, but also obtains luminance (gray scale) values of the image layers produced by U and V [10].

$$F = U \times S \times V^T \tag{1}$$

Studies in [10-13] show that small change in singular values for SVD or SVD-DWT based watermarking algorithms both increase robustness and have small effect on perceptual of the watermark.

1.1. LU Decomposition

Any square matrix F can be written as a product of L and U matrices which are lower and upper triangular matrices respectively.

$$F = L \times U = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & u_{12} & u_{13} \\ 0 & d_2 & u_{23} \\ 0 & 0 & d_3 \end{bmatrix} \tag{2}$$

As seen in Equation (2); the matrix L, is lower triangular, with 1's on the diagonal and the multipliers below the diagonal [14]. U, on the other hand, is upper triangular, with some coefficients on the diagonal and the multipliers above the diagonal. L has always 1's on the diagonal, whereas U does not. Therefore, in this study, we will divide out of U a diagonal matrix D which is made up entirely of the d_n coefficients as shown in Equation (3).

$$F = L \times D \times U$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{bmatrix} \times \begin{bmatrix} 1 & u_{12}/d_1 & u_{13}/d_1 \\ 0 & 1 & u_{23}/d_2 \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

There are almost few studies of LU decomposition in watermarking applications [15, 16]. Therefore, the other novel side of this study is to expand the application areas of watermarking with a new algorithm containing DWT, SVD, and LU together by chaotic map approach.

1.2. Arnold's Cat Map

A chaotic map technique called Arnold's Cat Map (ACM) is generally used for the randomization of the pixel locations in images in order to increase the security of the algorithm, especially in watermark applications. 2-D ACM for any $N \times N$ square images is described in Equation (4), where (x_n, y_n) and (x_{n+1}, y_{n+1}) are the locations of the pixels before and after ACM respectively [17].

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \right] mod N \qquad (4)$$

The pixels of the square image can be scrambled by using Equation (4), but when the transformation is repeated enough times, the original image will appear again. Fig. 1 shows scrambled forms of the watermark in each iteration.

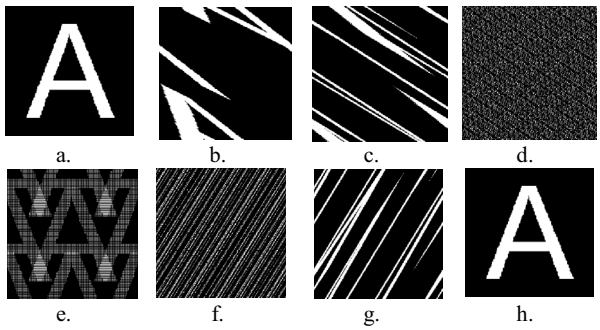


Fig. 1. (a) Original watermark and scrambled watermarks after related number of iterations in ACM: (b) 1, (c) 2, (d) 90, (e) 96, (f) 188, (g) 190, and (h) 192

As seen in Fig. 1, original form of the watermark is retrieved in the 192nd iteration. Therefore, if *X* iterations are applied in the embedding algorithm, *(192-X)* iterations should be implemented in the extracting algorithm in order to obtain the host image again.

As a binary image in size *256x256*, Fig. 1(a) is used as the watermark in this study. In order to increase the security, ACM is frequently used in watermarking algorithms [17-21]. Nevertheless, this study is unique in the sense that DWT, SVD and LU decomposition is secured by that chaotic map.

After explaining transform domain watermarking techniques and chaotic map approach, proposed embedding and extracting algorithm steps related to our previous studies in [22, 23] will be investigated in detail in the following section.

2. Proposed Algorithm

Proposed algorithm consists of watermark embedding and extracting.

2.1. Watermark Embedding Algorithm

Proposed watermark embedding procedure is as follows:

Step 1: The order of the pixel locations of the watermark, *W*, is rearranged in *X* iterations using ACM and chaotic mapped watermark, *WM*, is obtained.

Step 2: The cover work, *F*, is decomposed into four sub bands using DWT: LL, LH, HL, and HH. Even though embedding watermark on LL band degrades the image quality, robustness of the watermarked image under certain attacks can be achieved. In this algorithm LL sub band is chosen to embed the watermark so that the algorithm provides robustness without degrading the image and this can be achieved by using LU factorization in Step 3.

Step 3: By using LU factorization, LL band is decomposed into its lower triangular, diagonal, and upper triangular components as *L*, *D*, and *U* respectively: $LL = L \times D \times U$.
Decomposing LL sub band with LU factorization and using diagonal component, *D*, plays an important role in robustness under attacks.

Step 4: SVD is applied both to the diagonal component *D* (obtained from LU decomposition of LL sub band)
$D = (UDw) \times (SDw) \times (VDw^T)$
and to chaotic mapped watermark, *WM*,
$WM = (Uw) \times (Sw) \times (Vw^T)$.
so as to modify significant-related components by adding *Sw* (the singular values of *WM*) to *SDw* (the singular values of *D*) with the scaling factor α:
$Dw = SDw + \alpha \times Sw$.
The reason why SVD is selected is that it has small effect on perceptual of the watermark.

Step 5: D is reconstructed by updated component, *Dw*:
$Dww = (UDw) \times (Dw) \times (VDw^T)$.

Step 6: Due to the fact that the diagonal matrix (*D*) of LL sub band is updated, it is time to gather *L*, *Dww* and *U* so as to obtain *LLw*: $LLw = L \times Dww \times U$.

Step 7: The inverse DWT for the watermarked cover image, *FW*, is calculated.

Step 8: The number of iteration in ACM and the locations of 1's in *WM* are saved to use them as a key in the watermark extracting algorithm.

2.2. Watermark Extracting Algorithm

Proposed watermark extracting procedure is as follows:

Step 1: Watermarked and possibly attacked image, *FW**, is decomposed into four sub bands by using DWT: LLw*, LHw*, HLw*, and HHw*.

Step 2: By using LU factorization, LLw* band is decomposed into its lower triangular, diagonal, and upper triangular components as *L**, *D** and *U** respectively:
$LLw^* = (L^*) \times (D^*) \times (U^*)$.

Step 3: In order to decompose its orthogonal and diagonal components, SVD is applied to *D**:
$D^* = (UDw^*) \times (SDw^*) \times (VDw^*)$.

Step 4: The singular values of the extracted watermark *Sw** is calculated: $Sw^* = \frac{(SDw^* - SDw)}{\alpha}$.

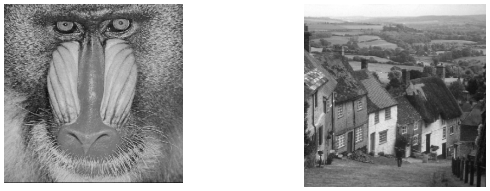
Step 5: The watermark with its SVD components is extracted: $WM^* = (Uw) \times (Sw^*) \times (Vw^T)$.

Step 6: The key which is the location of pixels stored in the embedding algorithm is used. If the mean value of pixels in the key for *WM** is greater than pre-defined threshold value, that pixel value is assigned to binary 0, otherwise to binary 1.

Step 7: Since pixels in the watermark *W* return their initial positions in 192nd iteration and *X* iterations are used in the embedding algorithm, the order of the pixels of extracted watermark, *WM**, is rearranged in *(192-X)* iterations using ACM and extracted and visually desired watermark, *W**, is obtained.

3. Experimental Results

Test images used in this proposed algorithm are shown in Fig. 2. Baboon and Goldhill in Fig. 2(a) and Fig. 2(b) respectively are 8 bit *512x512* gray scale images.



a. b.

Fig. 2. (a) Baboon, and (b) Goldhill as cover works

PSNR is most commonly used as a measure of quality of reconstruction in image watermarking. It is a ratio between the maximum value of a signal and the magnitude of background noise. For an 8-bit gray scale image, it is most easily defined as shown in Equation (5), where $F(i,j)$ is the original image and $FW(i,j)$ is watermarked image that both contain $M \times N$ pixels.

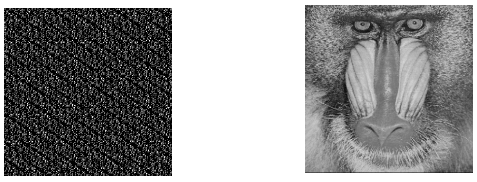
$$PSNR = 20 \times log\left(\frac{255}{\sqrt{\frac{1}{M \times N}\sum_i \sum_j [F(i,j) - FW(i,j)]^2}}\right) \quad (5)$$

While PSNR is a quality metric of embedding, SR in Equation (6) is used as a quality metric of extracting,

$$SR = \frac{S}{S + D} \quad (6)$$

where *S* and *D* represent the number of matching pixel values and the number of different pixel values in compared images respectively.

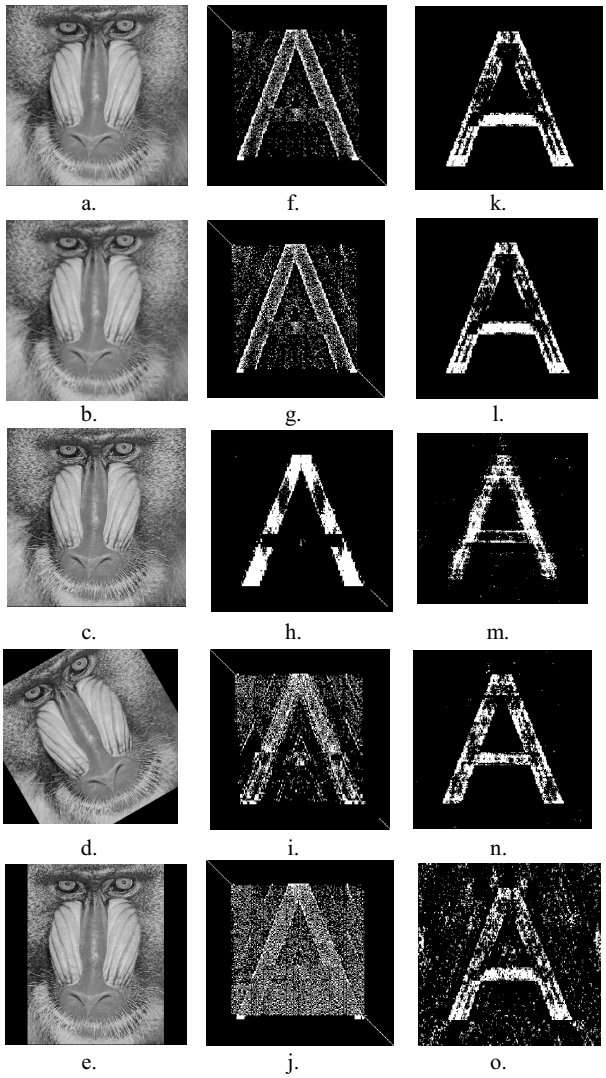
Fig. 3(a) and Fig. 3(b) show binary watermark image obtained from Fig. 1(a) by ACM after 90 iterations (experimentally chosen) and watermarked Baboon image respectively.



a. b.

Fig. 3. (a) Watermark for embedding, and (b) watermarked Baboon

Because of the limitations on number of pages, output images are shown only for Baboon. However, numerical results for Goldhill are also shared with the readers. In this study, "filtering" and "JPEG compression" which represent compression-based attacks and "scaling", "rotation" and "cropping" which stand for geometric attacks are used as attacks. Fig. 4(a)-(e) show watermarked Baboon images after filtering, scaling, JPEG compression, rotation, and cropping. If ACM was not used in the embedding algorithm, extracted watermarks would be obtained as in Fig. 4(f)-(j) relating to the attacks. However, Fig. 3(b) and Fig. 4(k)-(o) show that ACM increase both imperceptibility and robustness of the algorithm against attacks aforementioned.



a. f. k.
b. g. l.
c. h. m.
d. i. n.
e. j. o.

Fig. 4. Watermarked Baboon after attacks: (a) filtering (low-pass), (b) scaling (*512x512→256x256→512x512*), (c) JPEG compression (*Q*=%25), (d) rotation (30°), (e) cropping, (f)-(j) extracted watermarks after attacks in (a)-(e) respectively without ACM, (k)-(o) extracted watermarks after attacks in (a)-(e) respectively with ACM

4. Conclusions

This paper presented a robust and secure approach in watermarking based on the combination of DWT and SVD via LU decomposing by using ACM. After decomposing the cover image into four sub bands (LL, HL, LH, and HH), we decompose LL band again into LU factorization with its *L*, *D*, and *U* matrices and apply SVD to the *D* component. Afterwards, we modify diagonal singular value coefficients of *D* with the diagonal singular value coefficients of chaotic mapped watermark itself, *WM*, by using a scaling factor. Then, LL band coefficients are reconstructed with modified singular values and *D* components and finally inverse DWT is applied to obtain watermarked image.

The order of transform techniques follows DWT, LU, and SVD in this proposed algorithm steps respectively. The reason why DWT is used first is to use the LL frequency components of the cover work (LL is chosen so as to increase robustness of the watermarked image under certain attacks without degrading the image by embedding binary watermark). LU is used between DWT and SVD in order to increase security and robustness of the algorithm since changing *D* components have small effect on degradation of the cover work itself. Finally, modifying singular value coefficients of *D* will cause invisible and negligible distortion in the watermarked image. In addition, this modification allows us to update significant-related components, *SDw* (the singular values of *D* component) and *Sw* (the singular values of chaotic mapped watermark, *WM*), and also guarantees higher SR values. Moreover, because singular values of the watermark are embedded into the singular values of *D* component, the final transform is expected to be SVD.

Table 1 shows PSNR and SR values for Baboon and Goldhill according to proposed algorithm based on the combination of DWT, SVD, and LU with and without ACM. According to Table 1; ACM not only makes the watermark imperceptible by high PSNR but also increases the robustness of the algorithm by high SR in comparison to the algorithm without that chaotic map. Moreover, although attacks are causing low PSNR values, SR values are close to 1, but above all, the algorithm with ACM performs better than the algorithm without ACM in many cases.

Table 1. Comparative study on PSNR and SR values with and without ACM for Baboon and Goldhill in terms of related attacks

	Baboon				**Goldhill**			
	$\alpha = 1.1$, Number of Iteration=90 PSNR without ACM (before attacks) =38.8211 dB PSNR with ACM (before attacks)=39.5347 dB				$\alpha = 1.1$, Number of Iteration=90 PSNR without ACM (before attacks) =23.3735 dB PSNR with ACM (before attacks) =27.4672dB			
	PSNR [dB] without ACM	**PSNR [dB] with ACM**	SR without ACM	**SR with ACM**	PSNR [dB] without ACM	**PSNR [dB] with ACM**	SR without ACM	**SR with ACM**
Filtering (Low-pass)	23.1971	23.2103	0.8865	0.9219	23.1597	25.7410	0.8574	0.9223
Scaling (*512x512→256x256→512x512*)	22.4791	22.4682	0.8747	0.9224	22.8853	25.4137	0.8563	0.9220
JPEG Compression (*Q*=%25)	25.6940	25.7158	0.9275	0.9183	23.3077	26.0714	0.8896	0.8914
Rotation (30°)	10.8560	10.8358	0.8657	0.9214	10.5086	10.6094	0.8726	0.9228
Cropping	11.5758	11.5763	0.8227	0.8678	12.7527	12.9304	0.8107	0.6508

In our study, frequently-preferred transform domain technique DWT and decomposition method SVD is combined via LU decomposition so that watermarked images are much more robust against certain attacks. Thus, on the contrary to traditional DWT and SVD watermarking techniques, this proposed algorithm can be considered as robust against related attacks in Table 1. This is because the change of diagonal coefficients in singular value matrix in SVD and diagonal decomposition matrix in LU for LL sub band obtained by DWT, have small effect on perceptual of the watermark. Therefore, this study is novel in the sense that it expands the application areas of watermarking with a new algorithm consisting DWT, SVD, and LU with ACM.

Future works will be focused on more successful values of SR on cropping and be focused on robustness against various attacks.

5. References

[1] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI implementation of invisible digital watermarking algorithms towards the development of a secure JPEG encoder", *Proceedings of the IEEE Workshop on Signal Processing System (SIPS)*, Florida, USA, 2003, pp. 183-188.

[2] C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, and H. Perez-Meana, "A blind video watermarking scheme robust to frame attacks combined with MPEG2 compression", *Journal of Applied Research and Technology*, Vol. 8, pp. 323-369, 2010.

[3] O. Duman and O. Akay, "A new method of wavelet domain watermark embedding and extraction using fractional Fourier transform", *7th International Conference on Electrical and Electronics Engineering (ELECO 2011)*, Bursa, Turkey, 2011, pp. 187-191.

[4] M. Furat and M. Oral, "Digital image watermarking based on a relation between spatial and frequency domains", *5th International Conference on Electrical and Electornics Engineering (ELECO 2007)*, Bursa, Turkey, 2007.

[5] R. G. Schyndel, "A digital watermark", *In Proceedings of IEEE International Conference on Image Processing (ICIP94)*, Austin, Texas, USA, 1994, Vol. 2, pp. 86-90.

[6] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images", *Proceedings of 1998 International Conference on Image Processing (ICIP 1998)*, Urbana, USA, 1998, Vol. 2, pp. 419-423.

[7] M. S. Hsieh and D. C. Tseng, "Hiding digital watermarks using multiresolution wavelet transform", *IEEE Transactions on Industrial Electronics*, Vol. 48, pp. 875-882, 2001.

[8] E. Elbasi and A. M. Eskicioglu, "A DWT-based robust semi-blind ımage watermarking algorithm using two bands", *IS&T/SPIE's 18th Annual Symposium on Electronic Image Security, Steganography, and Watermarking of Multimedia Contents VIII Conference*, San Jose, CA, 2006, Vol. 6072, pp. 1-11.

[9] E. Elbasi, "Robust multimedia watermarking: hidden markov model approach for video sequences", *Turkish Journal of Electrical Engineering and Computer Sciences*, Vol. 18, pp. 159-170, 2010.

[10] E. Yavuz and Z. Telatar, "Improved SVD-DWT based digital image watermarking against watermark ambiguity", *Proceedings of the 2007 ACM Symposium on Applied Computing*, Seoul, Korea, 2007, pp. 1051-1055.

[11] V. I. Gorodetski, L. J. Popyack, V. Samoilov, and V. A. Skormin, "SVD-based approach to transparent embedding data into digital images", *In Proceedings of International Workshop on MMM-ACNS01)*, St. Petersburg, Russia, 2011, Vol. 2052, pp. 263–274.

[12] 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.

[13] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 15, No. 1, pp. 96-102, 2005.

[14] G. Strang, "Linear algebra and its applications", Thomson Learning, Inc., 2005.

[15] N. Shao-zhang, N. Xin-xin, and Y. Yi-xian, "Digital watermarking algorithm based on LU decomposition", *Journal of Electronics & Information Technology*, Vol. 26, pp. 1620-1625, 2004.

[16] S. Wang, W. Zhao, and Z. Wang, "A gray scale watermarking algorithm based on LU factorization", *International Symposiums on Information Processing*, Moscow, Russia, 2008, pp. 598-602.

[17] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection", *International Journal of Electronics and Communications*, Vol. 65, pp. 840-847, 2011.

[18] X. Wu and Z. Guan, "A novel digital watermark algorithm based on chaotic maps", *Physics Letters A*, Vol. 365, Issues 5-6, pp. 403-406, 2007.

[19] M. R. Keyvanpour and F. Merrikh-Bayat, "A New Encryption Method for Secure Embedding in Image Watermarking", *2010 3rd International Conference on Advanced Computer Theory and Engineering (1CACTE)*, Tehran, Iran, 2010, Vol. 2, pp. 403-407.

[20] L. Gang and Y. Ke-xin, "A novel chaos and HVS based image watermarking algorithm", *2010 3rd International Conference on Advanced Computer Theory and Engineering (1CACTE)*, China, 2010, Vol. 1, pp. 31-34.

[21] X. Wu, Z. Guan, and Z. Wu, "A chaos based robust spatial domain watermarking algorithm", *Advances in Neural Networks*, Vol. 4492, pp. 113-119, 2007.

[22] O. Jane and E. Elbasi, "A new approach in non-blind watermarking method based on DWT and SVD via LU Decomposition", *Turkish Journal of Electrical Engineering and Computer Sciences*, 2013, doi: 10.3906/elk-1212-75.

[23] O. Jane, H. G. Ilk and E. Elbasi, "A robust transform domain watermarking technique by triangular and diagonal factorization", *36th International Conference on Telecommunications and Signal Processing (TSP 2013)*, Rome, Italy, 2013 (accepted).