

Digital Watermarking Scheme Based on Arnold and Anti-Arnold Transforms

M. Abdallah Elayan^(✉) and M. Omair Ahmad

Department of Electrical and Computer Engineering,
Concordia University, Montreal, Canada
{a.alayan,omair}@ece.concordia.ca

Abstract. The goal of an image watermarking scheme is to embed a watermark that is robust against various types of attacks while preserving the perceptual quality of the cover image. In this paper, a discrete cosine transform and singular value decomposition based digital image watermarking scheme that makes use of Arnold transform is proposed. The basic idea behind the proposed Arnold transform based watermarking scheme is to improve the robustness of the watermarked image, while providing complete security to the embedded watermark. The new scheme is shown to retain the perceptibility of the cover image in the watermarked image due to the discrete cosine transform and singular value decomposition based watermark embedding. Extensive experiments are performed to demonstrate the performance of the proposed scheme in providing security to the watermark content, preserving the perceptibility of the cover image and in being robust against various types of attacks on the watermarked image.

Keywords: Digital watermarking · Discrete Cosine Transform (DCT) · Singular Value Decomposition (SVD) · Arnold transform

1 Introduction

With the rapid development of multimedia, it has become easy to obtain the intellectual properties. Consequently, the multimedia owners need more than ever before to protect their data and to prevent the unauthorized use of their data. Digital watermarking has attracted considerable attention and has several applications including copyright protection and fingerprinting of the multimedia for tracing and data authentication [1, 2].

According to the embedding domain, watermarking schemes can be categorized into two groups, spatial domain schemes and transform domain schemes. The schemes in the first category have the advantages of low complexity and easy implementation. However, these schemes generally lack the robustness against

This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada and in part by the Regroupement Stratégique en Microélectronique du Québec (ReSMiQ).

lossy image compression. On the other hand, a more robust watermarking can be achieved by the schemes in the second category by embedding the watermark into the transform coefficients of the host multimedia. In an effort to further improve the robustness of these transform domain schemes, in recent years, a number of watermarking schemes have been developed using singular value decomposition in the transform domain [3–7]. A feature of the singular value decomposition pertinent to digital watermarking is that the singular values of an image do not change significantly when common image processing attacks are performed on an image, and thus yields a more robust watermarking.

In [3], the authors have proposed a watermarking scheme based on DCT and SVD, where the watermark image is embedded into the singular value decomposition matrix of the DC values of the transformed cover image. This scheme provides a good robustness against general processing attacks while providing good imperceptibility, but the scheme lacks robustness against other attacks such as, contrast adjustment, rotation and cropping. In 2010, Lai and Tsai [4] proposed a watermarking scheme based on DWT and SVD. The watermark image is divided into two parts and embedded by modifying the singular values of the middle sub-bands of the one-level decomposed cover image. The proposed scheme has a good robustness against some kinds of attacks such as JPEG compression, rescaling and histogram equalization, but not so against other types of attacks such as, noise corruption or rotation. In [6], a DCT-SVD based watermarking scheme has been proposed, where the watermark image is embedded by modifying the singular values of each sub-band of the DCT coefficients by making use of the singular values of the watermark image. The proposed algorithm has a good resistant against general image processing attacks such as, noise corruption, contrast adjustment, and brightening adjustment, but lack the robustness against attacks such as, rotation, histogram equalization and translation. In [7], the authors have proposed a watermarking scheme based on DWT-SVD using Arnold transform. In this scheme, a watermark image is embedded into the low sub-band of the one-level decomposed cover image. The proposed scheme provides a good robustness against rotation, rescaling and contrast adjustment attacks, but not so against other types of attacks such as, gamma correction, histogram equalization and cropping. In general, the main limitation of the watermarking schemes described in [3–7] is that they, in general, are not robust against the different types of attacks.

In this paper, a DCT-SVD based digital image watermarking scheme that makes use of Arnold transform is developed with a view to providing improved robustness against different types of attacks while preserving the perceptual quality of the cover image. The paper is organized as follows. In Sect. 2, image scrambling are briefly reviewed. In Sect. 3, a new DCT-SVD based digital image watermarking scheme that makes use of the Arnold transform is proposed. In Sect. 4, experimental results demonstrating the performance of the proposed algorithm are presented. The performance of the proposed algorithm is also compared with those of other existing algorithms in this section. Finally, Sect. 5 concludes this paper by summarizing and highlighting the salient contributions of this work.

2 Background

2.1 Image Scrambling

Image scrambling process is an important image encryption technique that has been used in digital image watermarking. The objective of digital image scrambling is to transform a meaningful image into unintelligible image that prevents unauthorized users from understanding its true content. Without the knowledge of the image scrambling algorithm and the secret key, an unauthorized user (attacker) would not be able to recover the original watermark, even if it has been extracted from the watermarked data. Thus, scrambling provides an additional security for the digital data. Furthermore, since scrambling of an image, eliminates the spatial correlation of its pixels, the robustness of a watermarking scheme can be further improved.

Arnold Transform. The Arnold transform was introduced by Arnold [8]. For an image C with $N \times N$ pixels, the Arnold transform operation on the position (x, y) pixel is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod} N \quad (1)$$

The Arnold transform, which changes the positions of the pixels, can be repeated many times in order to obtain a scrambled image. However, due to the periodicity of the Arnold transformation, the original image can be restored after a certain number of iterations. Dyson and Falk [9] have studied the properties of the Arnold transform and pointed out that the transform given by (1) has a period $T_N \leq N^2/2$, for $N > 2$.

Anti-Arnold Transform. Use of the Arnold transform periodicity on a scrambled image to recover the original image could be achieved at the expense of possibly a large computational complexity depending on how many iterations have already been used to obtain the scrambled image. For this reason the authors in [10] have obtained the anti-Arnold transform. The anti-Arnold transform is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{mod} N \quad (2)$$

If a scrambled image is obtained by using n iterations of the operation of the Arnold transform, it needs the same number of iterations to recover the original image using the anti-Arnold transform. Therefore, the use of anti-Arnold transform to recover the original image can provide significant savings in computation, if $n \ll T_N$, as depicted in Fig. 1.

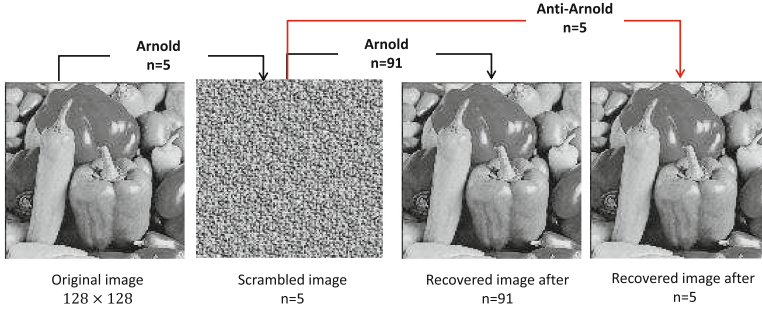


Fig. 1. Arnold and Anti-Arnold transforms.

3 Proposed Watermarking Scheme

3.1 Watermark Embedding Scheme

The discrete cosine transform is first applied to an $M \times M$ cover image, c . Next, the entire array of the DCT coefficients are zig-zag scanned, then the scanned coefficients are mapped in a zig-zag manner into the subbands B_1, B_2, B_3 and B_4 starting from the subband B_1 , and ending with the subband B_4 , as depicted in Fig. 2. Then, each subband is individually made to undergo an SVD operation. Next, an $N \times N$ ($2N \leq M$) watermark image is scrambled by applying r iterations of the Arnold transform. The number of iterations r is saved as a secret key, to be used during the extraction process to recover the original watermark image. The singular value matrix of each subband is then modified by adding to this matrix the scrambled watermark image. The resulting subband image $S_k + \alpha W'$ ($k = 1, 2, \dots, 4$) is singular value decomposed to obtain the singular value matrix S_{wk}^* of the watermarked subband. The subband watermarked DCT coefficients are obtained by augmenting S_{wk}^* with U_k and V_k as $B_k^* = U_k S_{wk}^* V_k^T$. Finally, the modified DCT coefficients are mapped back to their original positions, followed by an inverse discrete cosine transform operation to obtain the watermarked image. The proposed watermark embedding scheme is presented as Algorithm 1.

Algorithm 1. Watermark embedding algorithm

-
- Step 1 Apply the discrete cosine transform to the cover image, c .
 - Step 2 Rearrange the 2-D DCT coefficients into four subbands: B_1, B_2, B_3 and B_4 , through a zig-zag scanning of the DCT coefficients.
 - Step 3 Perform SVD operation to each subband: $B_k = U_k S_k V_k^T$ ($k = 1, 2, \dots, 4$).
 - Step 4 Apply r iterations of the Arnold transform on the watermark image W to obtain scrambled watermark image W' .
 - Step 5 Modify the singular value matrices S_k corresponding to each subband through a watermark embedding as $S_k + \alpha W'$, where α is a scaling factor.

- Step 6 Perform the SVD operation on the embedded subband singular value matrices $S_k + \alpha W'$ as $S_k + \alpha W' = U_{wk} S_{wk}^* V_{wk}^T$.
- Step 7 Augment the singular value matrix S_{wk}^* with U_k and V_k to obtain the watermarked DCT coefficients as $B_k^* = U_k S_{wk}^* V_k^T$.
- Step 8 Map the watermarked DCT coefficients of the subbands back to their original positions.
- Step 9 Apply the inverse discrete cosine transform to obtain the watermarked image, c_w .

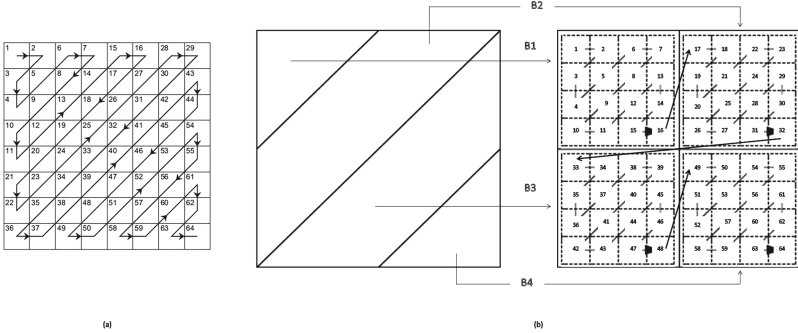


Fig. 2. (a) Zig-zag scanning of the 2-D discrete cosine transform coefficients. (b) Mapping of the scanned DCT coefficients into four subbands.

3.2 Watermark Extraction Scheme

The discrete cosine transform operation is applied to the watermarked image c_w , possibly after attack, followed by a re-arranging of the DCT coefficients into four subbands B_{w1}, B_{w2}, B_{w3} and B_{w4} through a zig-zag scanning of the coefficients. Then, each subband is individually made to undergo an SVD operation. Next, the singular value matrix of each subband S'_{wk} is augmented with U_{wk} and V_{wk}^T to obtain $D'_k = U_{wk} S'_{wk} V_{wk}^T$ ($k = 1, 2, \dots, 4$). A scrambled watermark image is extracted from each subband as $W'^*_k = (D'_k - S_k)/\alpha$, followed by an application of r iterations of the anti-Arnold transform to obtain the original watermark image. It should be noted that the number of iterations r of the anti-Arnold transform is used as a secret key during the extraction process. The proposed watermark extraction scheme is summarized as Algorithm 2.

Algorithm 2. Watermark extraction algorithm

-
- Step 1 Apply the discrete cosine transform to the watermarked image, c_w .
 - Step 2 Rearrange the 2-D DCT coefficients into four subbands: B_{w1}, B_{w2}, B_{w3} and B_{w4} , through a zig-zag scanning of the DCT coefficients.
 - Step 3 Perform SVD operation to each subband: $B_{wk} = U'_{wk} S'_{wk} V'^T_{wk}$ ($k = 1, 2, \dots, 4$).

- Step 4 Augment S'_{wk} with U_{wk} and V_{wk}^T to obtain $D'_k = U_{wk}S'_{wk}V_{wk}^T$, where U_{wk} and V_{wk} , are as obtained in Step 6 of Algorithm 1.
- Step 5 Extract the scrambled watermark image from each subband as $W'_k = (D'_k - S_k)/\alpha$.
- Step 6 Apply r iterations of the anti-Arnold transform on the scrambled watermark image W'_k to obtain the watermark image W_k^* .

4 Experimental Results and Discussion

The proposed watermarking scheme is implemented using MATLAB (R2012a) on a PC with a 1.6-GHz AMD E-350 processor, 3-GB RAM, and Microsoft Windows 7 operating system. Extensive experiments are conducted to demonstrate the performance of the proposed scheme. Three gray-scale cover images, *Lena*, *Pirate*, and *Couple*, and three watermark images, *Boat*, *Peppers*, and *Camera-man*, as depicted in Fig. 3, are used in these experiments. The size of each cover image is 256×256 and that of each watermark image is 128×128 .



Fig. 3. Cover images: (a) *Lena*, (b) *Pirate*, and (c) *Couple*. Watermark images: (d) *Boat*, (e) *Peppers*, and (f) *Cameraman*.

Figure 4 shows an example of a watermarked image and the extracted watermark image obtained by applying the proposed watermarking scheme. It is seen from this figure that the embedded watermark dose not degrade the perceptual quality of the cover image, and the proposed scheme is able to extract the watermark images successfully from the un-attacked watermarked image.

For objective evaluation of the perceptual quality of watermarked image, the peak signal-to-noise ratio (*PSNR*) is used [11]. The *PSNR* is given by

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \quad (3)$$

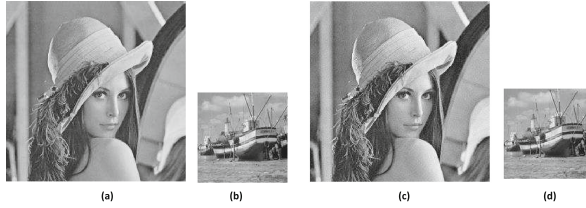


Fig. 4. (a) Cover image, *Lena*. (b) Watermark image, *Boat*. (c) Watermarked image. (d) The watermark image extracted from the watermarked image.

In general, a *PSNR* value is higher than 30dB is considered to be an indication of good perceptual quality of the watermarked image [11]. Table 1 gives the *PSNR* values of the various watermarked images obtained by using the proposed scheme. This table clearly indicates that the embedded watermark does not degrade the perceptual quality of the cover image, and thus the proposed embedding scheme guarantees the imperceptibility of the watermark.

Table 1. *PSNR* values (in *dB*) of various watermarked images

Cover image	Watermark image		
	Boat	Peppers	Cameraman
Lena	32	32.53	32.79
Couple	31.18	32.13	32.55
Pirate	31.67	32.38	32.83

To investigate the robustness of the proposed watermarking scheme, each watermarked image obtained by using the proposed watermark embedding scheme is subjected to different types of attacks. After each of these attacks, we extract four watermarks using the proposed watermark extraction scheme and then select the one having the largest normalized correlation coefficient between the extracted and the original watermark images. The normalized correlation (*NC*) between the original $N \times N$ watermark image W and the extracted watermark image W^* is given by

$$NC = \frac{\sum_{i=1}^N \sum_{j=1}^N (W_{ij})(W_{ij}^*)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (W_{ij}^2)} \sqrt{\sum_{i=1}^N \sum_{j=1}^N (W_{ij}^{*2})}} \quad (4)$$

Figure 5 shows the watermarked *Lena* images, each subjected to one type of attack, and the watermark images extracted from the attacked images. It is seen from this figure that the proposed effectively resists different types of attacks and is able to extract the watermark images with high perceptual quality.

In order to provide an objective analysis of the robustness of the proposed scheme, the normalized correlation coefficient between the extracted and the



Fig. 5. Watermarked *Lena* image attacked by different types of attacks and the extracted watermark images.

original watermark images is computed. Table 2 gives the values of the correlation coefficient using the cover images, *Lena*, *Couple*, and *Pirate*, and the same watermark image, *Boat*. It is seen from this table that the values of the correlation coefficient are almost invariably larger than 0.9 for the various attacks regardless of the images used in the experiments.

We also implement the SVD based watermarking scheme of [5], the DCT-SVD based watermarking algorithm of [6], and the DWT-SVD based watermarking scheme of [7], in order to compare the performance of the proposed scheme with theirs in terms of the PSNR of the watermarked image measuring the imperceptibility of the watermark and the correlation coefficient measuring the robustness of the watermarking schemes. The performance comparison is given in Table 3. It is seen from this table that the proposed watermarking scheme preserves the perceptual quality of the cover image, and provides an improved robustness against various types of attacks. Thus, the proposed scheme outperforms the other three algorithms used for comparison.

Table 2. Values of the correlation coefficient between the extracted and original watermark images

Attack	Cover image		
	Pirate	Couple	Lena
Rotation 2	0.9643	0.9489	0.9381
JPEG compression (Q = 10)	0.9974	0.9992	0.9993
Histogram Equalization	0.9665	0.9359	0.9371
Gaussian Noise ($\sigma^2 = 0.3$)	0.9870	0.9892	0.9875
Re-scaling (256-128-256)	0.9862	0.9831	0.9955
Contrast adjustment (-20 %)	0.9886	0.9956	0.9841
Sharpening (80 %)	0.8137	0.9078	0.8315
Gamma correction ($\gamma = 0.6$)	0.9937	0.9997	0.9998
Cropping (left and right sides by 25 columns)	0.9947	0.9970	0.9998
Blurring (using Gaussian filter)	0.9207	0.9284	0.9530
Median filter (3 × 3)	0.9805	0.9754	0.9909
Brightening (70 %)	0.9991	0.9994	0.9990
Darkening (70 %)	0.9800	0.9960	0.9979
Contrast adjustment (+20 %)	0.9705	0.9939	0.9871

Table 3. Performance, in terms of PSNR and normalized correlation coefficient, of the proposed and three other watermarking schemes against various types of attacks (Cover Image: *Lena*, Watermark Image: *Boat*)

Scheme	Proposed scheme	[5]	[6]	[7]
PSNR	32	28.31	24	24.26
	NC			
Rotation 2	0.9381	0.8864	0.8157	0.9292
JPEG compression (Q = 10)	0.9993	0.9881	0.9998	0.9981
Histogram Equalization	0.9371	0.9316	0.7492	0.5983
Gaussian Noise ($\sigma^2 = 0.3$)	0.9875	0.9441	0.9853	0.9767
Re-scaling (256-128-256)	0.9955	0.9785	0.9964	0.9928
Contrast adjustment (-20 %)	0.9841	0.9626	0.9504	0.9006
Sharpening (80 %)	0.8315	0.7449	0.7898	0.8105
Gamma correction ($\gamma = 0.6$)	0.9998	0.5960	0.9460	-0.7115
Cropping (left and right sides by 25 columns)	0.9998	0.8256	0.9969	0.0155
Blurring (using Gaussian filter)	0.9530	0.9501	0.9521	0.9350
Translation (20,20)	0.9955	0.9024	0.7101	0.8693
Brightening (70 %)	0.9990	0.3524	0.9678	0.9408
Darkening (70 %)	0.9979	0.3351	0.9927	-0.9287
Contrast adjustment (+20 %)	0.9871	0.9742	0.9816	0.9550

Table 4. Execution times of running the proposed and two other watermarking schemes

Watermark embedding/extraction	Execution time in seconds		
	Proposed Scheme	[6]	[7]
Embedding	2.145	2.061	2.848
Extraction	0.339	0.327	0.585

Table 4 gives the execution times of running the proposed watermarking algorithms and that of running the schemes developed in [6, 7]. A comparison of the proposed scheme with the scheme of [6] indicates that the use of the Arnold and anti-Arnold transforms for the embedding and extraction of the watermark in the proposed scheme does not add to its computation time. However, the data scrambling using the Arnold transform in the proposed scheme significantly improves its robustness. It is also seen from this table that the proposed scheme provides savings of 24.7% and 42% in the execution times of its embedding and extraction parts, respectively, over those of the scheme of [7] that also uses the Arnold transform.

5 Conclusion

In this paper, a DCT-SVD based watermarking scheme, in which the watermark image is embedded using the approach of Arnold transform has been proposed. The DCT coefficients of the cover image are zig-zag scanned and mapped in a zig-zag manner into four subbands. The watermark image is scrambled using the operation of the Arnold transform, and then embedded into the singular value matrices of the four subbands of the array of the re-arranged DCT coefficients.

Extensive experiments have been conducted to evaluate the performance of the proposed scheme. The results of the experiments have demonstrated that the proposed embedding scheme ensures the imperceptibility of the watermark and that the embedded watermark does not degrade the perceptual quality of the cover image. The performance of the proposed scheme has also been compared with three other watermarking schemes. The results of comparison have demonstrated that the proposed watermarking scheme yields a performance superior to that of the other three schemes in preserving the perceptual quality of the cover image, and in providing an improved robustness against various types of attacks.

References

1. Zebbiche, K., Khelifi, F.: Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking. *IET Image Proc.* **8**(1), 23–32 (2014)
2. Li, Z., Ping-ping, Z., Gong-bin, Q., Zhen, J.: Image watermarking with optimum capacity. In: 5th International Conference on Visual Information Engineering, pp. 117–123 (2008)

3. Liu, F., Liu, Y.: A watermarking algorithm for digital image based on DCT and SVD. In: Proceedings of Conference on Image and Signal Processing, vol. 1, pp. 380–383 (2008)
4. Lai, C.C., Tsai, C.C.: Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **59**(11), 3060–3063 (2010)
5. Liu, R., Tan, T.: A SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multi.* **4**(1), 121–128 (2002)
6. Gupta, P.K., Shrivastava, S.K.: Improved RST-Attacks resilient image watermarking based on joint SVD-DCT. In: Proceedings of International Conference on Computer and Communication Technology, Allahabad, India, pp. 46–51 (2010)
7. Sushila, K., Maheshkar, V., Agarwal, S., Srivastava, K.: DWT-SVD based robust image watermarking using Arnold map. *Int. J. Inf. Technol.* **5**(1), 101–105 (2012)
8. Arnold, V., Avez, A.: *Ergodic Problems in Classical Mechanics*. Benjamin, New York (1968)
9. Dyson, F.J., Falk, H.: Period of a discrete cat mapping. *Amer. Math. Mon.* **99**, 603–624 (1992)
10. Wu, L., Zhang, J., Deng, W., He, D.: Arnold transformation algorithm and anti-arnold transformation algorithm. In: Proceedings of the Information Science and Engineering International Conference, Nanjing, China, pp. 1164–1167 (2009)
11. Chang, C.C., Lin, C.C., Hu, Y.S.: An SVD oriented watermark embedding scheme with high qualities for the resorted images. *Int. J. Innovative Comput. Inf. Control* **3**, 609–620 (2007)