International Journal of Computer Networks and Communications Security

VOL. 3, NO. 3, MARCH 2015, 110–116
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

EFFECTIVE SVD-YCBCR COLOR IMAGE WATERMARKING

FARZANEH SARKARDEH[1] and MEHDI KHALILI[2]

[1] M.S. Student, Dept. Computer and Informatics Engineering ,PayameNoor University, Tehran, Iran

[2] Assistant Professor, Dept. Computer and Informatics Engineering ,PayameNoor University, Tehran, Iran

E-mail: [1]f.sarkardeh@yahoo.com, [2]m.khalili@pnu.ac.ir

ABSTRACT

In this paper, a blocked-SVD based color image watermarking scheme is proposed in which, to embed the color watermark, two levels SVD are applied on Y channel of the converted host image. Moreover, to more security, imperceptibility and robustness, the watermark insertion is done using zigzag method on non-overlapping blocks. The experimental results reveal that the proposed algorithm not only satisfies the imperceptibility and watermarking robustness against different signal processing attacks such as JPEG compression, scaling, blurring, rotation, noising, filtering and etc., as well, rather, has better values compared to the existing works.

Keywords: *Color Image Watermarking, SVD, Zigzag Method, Ycbcr Color Space.*

1 INTRODUCTION

Nowadays, digital watermarking has become an important issue. Because, it can be used as an effective tool for copyright protection of digital documents. Digital watermarking hide the information in to different documents such as audio, image, video, and text, so that the hidden information can be extracted without any errors, using the unique way, to make an assertion by the owner of the object [1], [2].

According to domains, watermark insertion is divided into two broad groups: spatial-domain and frequency-domain methods. Embedding the watermark into the spatial-domain component of the host image is the direct method. This has the advantages of low complexity and easy implementation. However, the spatial domain watermarking algorithms are fragile to image processing operations or the other attacks. On the other hand, the frequency-domain techniques embed the watermark using modulating the magnitude of coefficients in a transform domain, such as discrete cosine transform (DCT), discrete wavelet transform (DWT) and Singular value decomposition (SVD). Generally, frequency watermarking algorithms are more robust, more complex and more widely applied than spatial based schemes [2]–[5].

Normally watermarking methods have different requirements such as robustness, invisibility, capacity and security. There is always a deal between the requirements. For example, increasing the capacity of embedding the image may increase the robustness while decreasing invisibility features and vice versa. Therefore, a compromise should be made between conflicting parameters [6]–[8].

In image processing applications, due to the resistance of singular values of SVD, it has become an attractive domain for watermarking applications. In [9], the authors have proposed an algorithm for color images resistant to geometrical distortions such as rotation and scaling, in which, the singular value decomposition is used for watermark embedding and extraction. In this scheme, the log-polar mapping (LPM) method is used to improve its resistance to geometrical attacks. In [10], the authors have presented a block-SVD based image watermarking scheme, using modifying the middle SVs of the cover image. In this work, the watermark image is just based on two colors. In [11], a based SVD color image watermarking

algorithm is proposed, in which the watermarks are embedded into the color host image. So that, after applying SVD, the watermark bits are embedded into 4×4 block using modifying the second and third rows of the first column form U component. similarly, in [12], a watermarking scheme has proposed which is based on singular value decomposition and analyzing the orthogonal matrix U. The watermark image in the proposed shame is based on two colors. This work, to embed the watermark modifies the values of the second and the third rows of the first column from U matrix. Also, to extract the watermark, the modified relation is used.

In the aforesaid works, the strength of the watermark against various image processing attacks is acceptable, but in higher severe attacks, the watermark may be destroyed seriously. In this paper, we propose a block-SVD based watermarking scheme in which the embedding process is perfumed on Y channel of converted host image in the second level of the SVD. Using SVD blocking in the proposed scheme leads to faster speed than global SVD. Plus, for more security of the watermark, we use zigzag process to rearrange the blocks of cover image. The experimental results show that the proposed algorithm not only achieves to a satisfactory results in balancing between quality and robustness against common image processing operations, rather has higher values, compared to earlier works.

2 EXPLAIN THE BASIC CONCEPTS

2.1 Singular Value Decomposition (SVD)

The singular value decomposition (SVD) is a mathematical analysis technique that was discovered for extracting the algebraic properties of the image. The digital image can be defined as a real non-negative matrix. Assume 'A' is an image of size N×N, we can show the case of singular values decomposition of the image as follows [7], [13]:

$$A = USV^{T} = \begin{bmatrix} u_{1,1} & \cdots & u_{1,N} \\ \vdots & \ddots & \vdots \\ u_{N,1} & \cdots & u_{N,N} \end{bmatrix} \begin{bmatrix} \partial_{1,1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \partial_{N,N} \end{bmatrix} \begin{bmatrix} v_{1,1} & \cdots & v_{1,N} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \cdots & v_{N,N} \end{bmatrix}$$

The U and V are N × N orthogonal matrices, whiles the S is N×N diagonal matrix containing the singular values Si in a decreasing order.

The widespread usage of SVD in image processing applications is due to its important characteristics such as [7], [13], [14]:

Good stability of the singular values of each image, since no significant changes to the SVs of images will occur upon the addition of small perturbations.

The singular values of an image explain its algebraic properties, representing an image's brightness, whereas the singular vectors (U and V) reflect the geometry characteristics of an image.

Singular values are sorted in descending, and many of them have small values compared to the first singular value. Ignoring these small SVs in the reconstruction stage, leads to a minimal effect on an image's quality.

SVD can be performed on square or rectangle matrices.

2.2 Ycbcr Color Space

YCbCr is similarity of color spaces commonly used as a part of color image pipeline in video and digital photography systems. In this color space, the Y component shows the luminance or brightness, while Cb and Cr respectively explain blue-difference and red-difference. The conversion relationships between RGB and YCbCr color spaces are defined as follows [15]:

$$\begin{bmatrix} Y & Cb & cr \end{bmatrix} = \begin{bmatrix} R & G & B \end{bmatrix} \begin{bmatrix} 0.299 & -0.16875 & 0.500 \\ 0.587 & -0.33126 & -0.41869 \\ 0.114 & 0.500 & -0.08131 \end{bmatrix}$$

$$\begin{bmatrix} R & B & B \end{bmatrix} = \begin{bmatrix} Y & Cb & Cr \end{bmatrix} \begin{bmatrix} 1.0 & 1.0 & 1.0 \\ 0.0 & -0.34413 & 1.772 \\ 1.402 & -0.71414 & 0.0 \end{bmatrix}$$

3 THE PROPOSED WATERMARKING SCHEME

3.1 Embedding Watermark Procedure

Flowchart of the proposed color image watermarking algorithm is shown in Fig. 1.

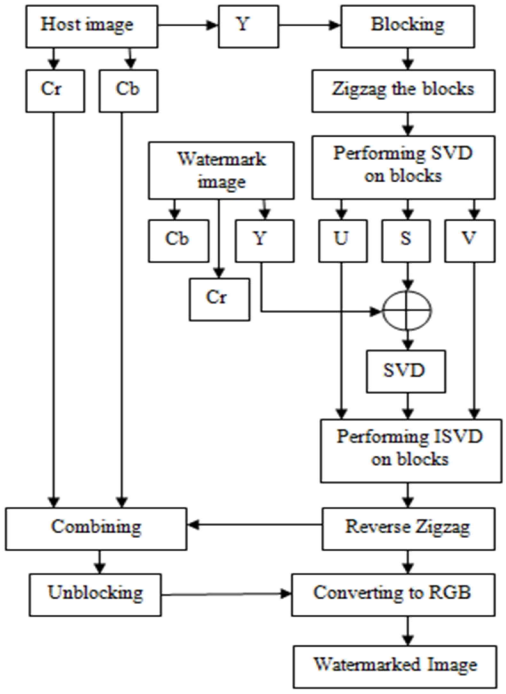


Fig. 1. Embedding Watermark Flowchart

The watermark embedding procedure contains the following steps:

Step1: Convert RGB color space of the host image (H) into YCbCr color space using the Eq. 2, and select Y component (YH) for insertion the color watermark.

Step 2: Divide the Y component into non-overlapping blocks 8×8.

Step 3: Rearrange the blocks using applying zigzag scanning process to obtain rearranged blocks. The zigzag scanning for rearranging pixel of image is displayed in Fig. 2 [16]:

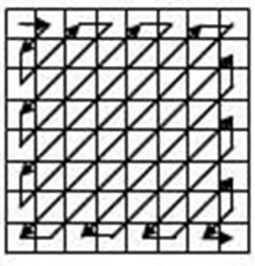


Fig. 2. Zigzag Scanning

Step 4: Convert the color watermark image (W) from RGB color space into YCbCr color space using the Eq. 2, and select Y component (YW).

Step 5: Perform SVD on each block of YH as follows:

$$Y_H = USV^T \quad (4)$$

Step 6: multiply each pixel of YW in scaling factor (α). Then insert it in the latest singular value of each block of S. Thus, a modified matrix SS is obtained as follows:

$$S(8,8) = \alpha Y_w ; SS = S \quad (5)$$

Step 7: Perform SVD on SS matrix again.

$$SS = U_w S_w V_w^T \quad (6)$$

Step 8: Apply inverse SVD by multiplying matrices S_W, U and V together to achieve modified blocks.

$$Y'_H = US_w V^T \quad (7)$$

Step 9: Perform reverse zigzag on each block.

Step 10: Unblock and combine Y'_H, Cb and Cr of the host image.

Step 11: Convert the changed YCbCr image to RGB image using the Eq. 3, to achieve RGB watermarked image.

Step 12: Save the factors: V_W, U_W, α, Cb and Cr as the keys, to extract the color watermark.

A. Extracting Watermark Procedure

Flowchart for extracting watermark proposed algorithm is shown by Fig. 3.

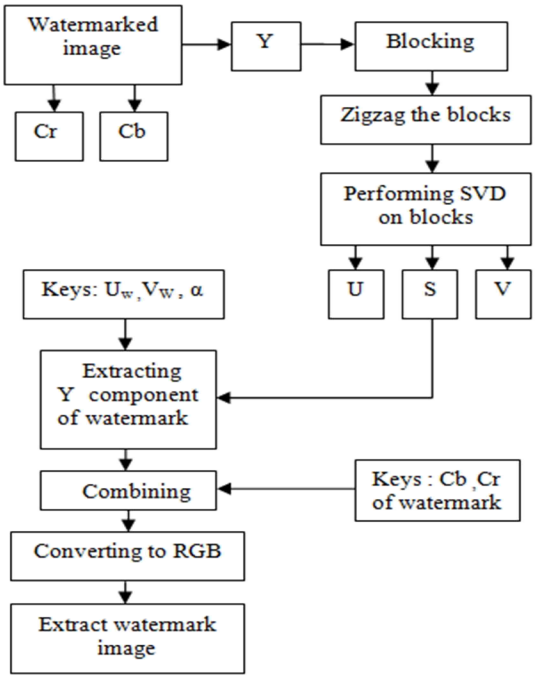


Fig.3. Extracting Watermark Flowchart

The color watermark can be extracted if V_W, U_W, α, Cb and Cr be presented by owner. The watermark extracting procedure contains the following steps:

Step 1: Convert RGB color space of the watermarked image (H^*) into YCbCr color space using the Eq. 2, and select Y component for extracting the color watermark.

Step 2: Divide the Y component into non-overlapping blocks 8×8.

Step 3: Rearrange the blocks using applying zigzag scanning process to obtain rearranged blocks.

Step 4: Perform SVD on each block as follows:

$$Y_H^* = U^* S_w^* V^{*T} \quad (8)$$

Step 5: Select the latest singular value of each block as follows:

$$SS^* = U_w S_w^* V_w^T \quad (9)$$

$$Y_w^* = \frac{1}{\alpha} SS^* \quad (10)$$

Thus, one pixel of Y component from color watermark image is extracted.

Step 6: Combined the extracted Y_w^* with keys Cb and Cr.

Step 7: Convert the combined image to RGB color space using the Eq. 3, to extract the color watermark image.

4 SIMULATION AND EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed algorithm, we used three 24 bit 512×512 color images as host images which are shown in Fig. 4 (a-c). Moreover, one 32×32 color image shown in Fig. 4 (d) was used as watermark image.

Fig. 4. (a-c) Host Images And (d) Color Watermark Image

To evaluate the invisibility of the watermark, between the host image (F) and the watermarked image (G), the peak signal to noise ratio (PSNR) was used. It is defined as follows [17], [18]:

$$PSNR = 10 \log_{10} \frac{(MaxPixelValue)^2}{MSE} \quad (11)$$

Where MSE is represents the mean squared error of image and is defined as follows [17], [18]:

$$MSE = \frac{1}{M * N} \sum_{y=1}^{M} \sum_{x=1}^{N} (F_{xy} - G_{xy}) \quad (12)$$

where M and N represents width and height of image, F_{xy} denotes the pixel value in the original image and G_{xy} denotes the pixel value in reconstructed image.

Generally, the larger PSNR value leads to more imperceptibility of the watermarked image. It means, the watermarked image is very similar to the original one [17], [18].

Moreover, we used the normalized correlation (NC) between the original watermark image (W)

and the extracted watermark image (W') to measure the robustness of the watermark. It is defined as follows [18]:

$$NC = \frac{\sum_{I=1}^{N} w_i w_i'}{\sqrt{\sum_{i=1}^{N}\sum_{i=1}^{N} w_i'}} \qquad (13)$$

where N represents total of pixels, w_i denotes the pixel value in the original watermark image and w'_i denotes the pixel value in the extract watermark image.

The NC can take any value between 0 and 1. If the NC value is closer to 1, the extracted watermark image is more similar to the embedded one [18].

Fig. 5 (a-c) shows the watermarked images. Also, the extracted color watermark is shown in Fig. 5 (d).

Fig. 5. (a-c) Watermarked Image, And (d) Extract Color Watermark Image

The PSNR and NC of the proposed watermarking scheme for different images are listed in table 1. It can be seen from the PSNR values that the watermarked images have a good quality and our proposed scheme is able to obtain the extracted color watermark with the best NC value.

Table 1: PSNR And NC From Proposed Scheme

	Lena	Baboon	F16
PSNR	49.6189	49.3153	48.4662
NC	1.0000	1.0000	1.0000

After satisfying the PSNR and NC, we compare our proposed color watermarking scheme to the other algorithms which are provided in [9]–[12]. Simulation results shown in table 2 reveal that our proposed scheme has better quality and more robustness compared to the other schemes.

An important property of the watermarking schemes is that they must be robust against different signal processing attacks. Therefore, different attacks are conducted on the proposed algorithm.

Table 3 lists the obtained results of the extracted color watermark image form different common attacks. As it can be seen, all of the extracted watermarks are recognizable as well.

Table 2: Compare Between Proposed Scheme And Another Schemes

	Proposed scheme	[9]	[10]	[11]	[12]
PSNR	49.6189	33.4874	35.0987	33.8823	38.3985
NC	1.0000	1.0000	0.9983	1.0000	0.9998

Table 3: NC Value From Image Watermarking Scheme After Different Attacks

Attack Type	Parameter	Extracted Watermark
Blurring	1	
Gaussian filter	3×3	
Rotation	0.1	
Salt & pepper noise	0.002	
Average filter	3×3	
Median filter	3×3	
Cropping	0.5	

JPEG compression is one of the most common signal processing attacks. So, we test our algorithm to this attack. In this experiment, the watermarked images are compressed with different compression factors from 10 to 100. The obtained results of JPEG experiment are shown in table 4.

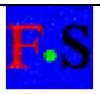
As it can be found, the proposed method is so robust against JPEG compression attack. So that,

the NC values are acceptable and the extracted color watermarks are recognizable as well.

After satisfying JPEG experiment, we compare our proposed scheme to the earlier works in [9]–[12]. Fig. 6 illustrates the comparative results. It is visible that the proposed algorithm achieves to higher robustness against JPEG compression, compared to the others.

The other experiment to show the robustness of the proposed scheme was scaling attack.

Table 4: NC Value Of Proposed Scheme After JPEG Compression Attack

Compression Factor	NC Proposed Scheme	Extract Watermark
10	0.9555	
20	0.9756	
30	0.9830	
40	0.9854	
50	0.9893	
60	0.9878	
70	0.9917	
80	0.9909	
90	0.9920	
100	1.0000	

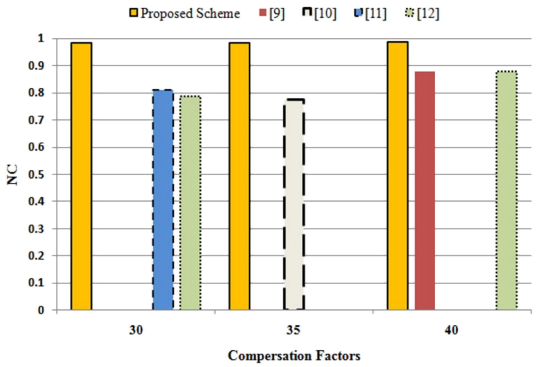


Fig. 6. Compare NC Values Of Different Image Watermarking Scheme After JPEG Compression Attack

Table 5 shows the obtained results of this experiment in the proposed method. Also the comparative results to the earlier works in [10]–[12] are listed in this table. As it can be seen the proposed method leads to satisfactory NC and has higher robustness than the other works.

Table 5:NC Value From Different Watermarking Scheme After Scaling Attack

	parameter	Proposed scheme	[10]	[11]	[12]
NC	0.5	0.9868	0.5917	0.71741	0.90372

5 CONCLUSION

In this paper, an effective color image watermarking scheme has proposed in which to embed the color watermark image, the host image, after converting to YCbCr channels, is decomposed to two levels SVD. Moreover, to archive more security, imperceptibility and robustness of the watermark, non-overlapping blocks are selected to insertion the watermark using zigzag scanning method. The experimental results show that the proposed scheme not only satisfies the imperceptibility and watermarking robustness against different signal processing attacks such as JPEG compression, scaling, blurring, rotation, noising, filtering and etc., as well, rather, leads to better results compared to the earlier works in [9]–[12].

7 REFERENCES

[1] A. Basu, A. Saha, J. Das, S. Roy, S. Mitra, I. Mal, and S. K. Sarkar, “On the Implementation of a Digital Watermarking Based on Phase Congruency,” in Proceedings of the 3rd International Conference on Frontiers of

Intelligent Computing: Theory and Applications (FICTA) 2014, 2015, vol. 328, pp. 113–120.

[2] S. Jia, "A novel blind color images watermarking based on SVD," Optik - International Journal for Light and Electron Optics, vol. 125, no. 12, 2014, pp. 2868–2874.

[3] N. Harish, B. Kumar, and D. Kusagur, "Hybrid Robust Watermarking Technique Based on DWT, DCT and SVD," international Journal of Advanced Electrical and Electronics Engineering, vol. 2, no. 5, 2013, pp. 137–143.

[4] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," Digital Signal Processing, vol. 21, no. 4, Jul. 2011, pp. 522–527.

[5] K. Loukhaoukha, M. Nabti, and K. Zebbiche, "A robust SVD-based image watermarking using a multi-objective particle swarm optimization," Opto-Electronics Review,vol. 22, no. 1, 2014, pp. 45–54.

[6] A. Bajaj and Shagun, "Review on Watermarking Techniques: A Unique Approach for Digital Image Protection," International Journal of Advanced Research in Computer Science and Software Engineering, 2014,vol. 4, no. 5, pp. 763–773.

[7] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Digital Signal Processing, vol. 1, Jul. 2014,pp. 1–14.

[8] C. Fung, A. Gortan, and W. G. Junior, "A Review Study on Image Digital Watermarking," in ICN 2011 : The Tenth International Conference on Networks, 2011, pp. 24–28.

[9] Y. Xing and J. Tan, "A color image watermarking scheme resistant against geometrical attacks," Radio Engineering, vol. 19,no. 1, 2010, pp. 62–67.

[10] N. Goléa, R. Seghir, and R. Benzid, "A bind RGB color image watermarking based on singular value decomposition," in omputer Systems and Applications (AICCSA)IEEE/ACS International Conference on, 2010, pp. 1–5.

[11] Q. Su, Y. Niu, Y. Zhao, S. Pang, and X. Liu, "A dual color images watermarking scheme based on the optimized compensation of singular value decomposition," AEU - International Journal of Electronics and Communications, vol. 67, no. 8, Aug. 2013, pp. 652–664.

[12] Q. Su, Y. Niu, H. Zou, and X. Liu, "A blind dual color images watermarking based on singular value decomposition," Applied Mathematics and Computation, vol. 219, no. 16, Apr. 2013, pp. 8455–8466.

[13] A. a. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," Signal Processing, vol. 88, no. 9, Sep. 2008, pp. 2158–2180.

[14] M. Manjunath and S. Siddappaji, "A new robust semi blind watermarking using block DCT and SVD," IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), no. 978,2012, pp. 193–197.

[15] F. Douak, R. Benzid, and N. Benoudjit, "Color image compression algorithm based on the DCT transform combined to an adaptive block scanning," AEU - International Journal of Electronics and Communications, vol. 65, no. 1, Jan. 2011, pp. 16–26.

[16] M. Rahman, "A dwt, dct and svd based watermarking technique to protect the image piracy," International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT), vol. 4, no. 2, 2013.

[17] W. Wang, W. Li, Y. Liu, and B. Žalik, "A SVD Feature based Watermarking Algorithm for Gray-level Image Watermark," Journal of Computers, vol. 9, no. 6, Jun. 2014, pp. 1497–1502.

[18] R. Islam and J. Kim, "Reliable RGB color image watermarking using DWT and SVD," Informatics, Electronics & Vision (ICIEV), no. 1, 2014, pp. 1–4.