Open Access

SCHOLARENA

Journal of Mathematical and Statistical Analysis

REVIEW ARTICLE

ISSN: 2642-018X

Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection

Fita A* and Endebu B

Adama Science and Technology University, Adama, Ethiopia

***Corresponding author:** Fita A, Adama Science and Technology University, Adama, Ethiopia, Tel: +251911840839, E-mail: fitaadu@yahoo.com

Citation: Fita A, Endebu B (2019) Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection. J Math Stat Anal 2: 104

Article history: Received: 26 December 2018, **Accepted:** 25 January 2019, **Published:** 28 January 2019

Abstract

Digital watermarking is the process of embedding information into a digital signal such as image, video, audio data to easily identify the ownership of the original data. Such information is embedded for many different purposes, such as copyright protection, source tracking, piracy deterrence, tamperproof etc. Therefore, it shall be embedded in a way that makes it difficult to be visualize with human eye and difficult to be removed. As computers are more and more integrated via the network, the distribution of digital data is becoming faster, easier, and requiring less effort to make exact copies. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. In this paper, we propose an algorithm for colored digital image watermarking technique based on singular value decomposition. This paper covers embedding, watermark extraction algorithm and some robustness tests while both host and watermark images are colored. The quality of the watermarked image is tested through experiment against most common attacks such as image compression, filtering, cropping, injection of noise, blurring, and sharpening. Standard benchmark was used to test the robustness of the proposed watermarking algorithm. Experimental result shows that the algorithm is robust against geometric attacks.

Keywords: Colored Image; Embedding: Singular Value; Watermark; Watermarking attacks

Introduction and Background

Nowadays digital multimedia is undergoing dramatic changes in information communication technologies. Images, texts, audio, video files contain information normally stored on conventional media and easily shared through internet. However, all of these advancements lead to a serious problems of security, misuse and copyright problems. Over the past few years, digital watermarking has emerged as a leading candidate that could solve the fundamental problems of legal ownership [1].

In order to keep the intellectual property, digital watermarking technique has been proposed as a method to embed an invisible or visible signal into multimedia data so as to check the owner identification and to discourage the misuses of digital data. The domain in which watermark is embedded are categories into spatial domain and transform domain [2]. On one hand the spatial domain methods modify pixels directly to hide the watermark bits and have low computational complexity [3]. On the other hand, the transform domain methods do not alter the pixel values directly but rather modify the transform coefficients to hide the watermark bits such as Discrete Cosine Transform, Discrete Wavelet Transform and Singular Value Decomposition (SVD) [3,4].

In hybrid watermarking, Discrete Wavelet Transform and Singular Value Decomposition have been used where the watermark is embedded on the singular values of the cover images in Discrete Wavelet Transform sub bands [3]. A novel dual watermarking mechanism has been studied for digital media that embeds a visible pattern into the spatial domain and an invisible logo into the frequency domain [4,5]. Some authors developed a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements [6]. In order to achieve the objectives they have used singular values of wavelet transformation's HL and LH sub bands to embed watermark. The hybrid of Discrete Wavelet and Singular Value Decomposition watermarking schemes had been studied and there comparative study was done using the different peak signal to noise ratio (PSNR) values taken over different values of scale factor in gray scale images [7,8]. In all transfer domains watermarking such as Discrete Cosine Transforms, Discrete Wavelet Transform and Discrete Fourier Transform (DFT), use linear transform of image intensity to frequency domain [9]. The image is passed through high-pass filters and low-pass filters to analyze frequencies which eliminated the sample according to the Nyquist theory which cases blurring and noise near edge [10-13].

In this paper we focused on the invisible watermarking techniques based on singular value decomposition. Singular value decomposition (SVD) is a mathematical based on linear algebra and used by factorization of a real matrix or complex matrix, with many useful applications in image processing. The use of SVD decomposition in the image hashing problem was proposed by Kozat, *et al.* where SVD decomposition is used twice and has been shown to be robust to some small variations in rotation and scaling [14].

The main advantages of using SVD from the viewpoint of image processing and properties of SVD to employ in digital watermarking schemes are [13].

Small perturbation in singular values does not change the image significantly which have very good stability and each singular value specifies the brightness of an image layer while the corresponding pair of singular vectors specifies the geometry of the image. To solve the false positive problem in various SVD-based watermark schemes, transform domain encryption is utilized and the embedding component of watermark instead of the whole watermark is embedded into the host image [14,15].

In this study, the performances of proposed methods will be evaluated in terms of imperceptibility and robustness. Different types of attacks were first performed in MATLAB and measurement will be done with standard benchmark tools called Stir Mark.

The singular value decomposition (SVD) is very powerful and useful matrix decomposition, particularly in the context of data analysis, dimension reducing, image hiding, image compression, noise reduction and camera calibration for satellite data and is the method of solving most linear least squares problems.

Singular Value Decomposition

The singular value decomposition (SVD) is very powerful methods for matrix decomposition, particularly in the context of data analysis, dimensional reduction and satellite data and image processing. Singular Value Decomposition (SVD) of a real matrix A is factorization of A in to three matrices, two orthogonal matrices U, V and a diagonal matrix D such that

$$A = UDV^T \tag{1}$$

where

- *U*: mxm a rotation orthogonal matrix called left singular vectors.
- *V*: nxn a rotation orthogonal matrix and right singular vectors
- *D*: mxn a stretching diagonal matrix known as the singular values.

$$A = \begin{pmatrix} u_{1,1} & \cdot\cdot & u_{1,m} \\ \vdots & \ddots & \vdots \\ u_{m,1} & \cdot\cdot & u_{m,m} \end{pmatrix} \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} v_{1,1} & \cdot\cdot & v_{1,n} \\ \vdots & & \vdots \\ v_{n,1} & \cdot\cdot & v_{n,n} \end{pmatrix}^T \tag{2}$$

$$D = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad and \quad D = \begin{pmatrix} \sigma_1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_m & 0 & \cdots & 0 \end{pmatrix} \quad if \quad m < n \tag{3}$$

$$when \ m > n$$

The entries of (3) are ordered in descending order according to $\sigma_1 \geq \sigma_2 \geq ....\sigma_r \geq 0$, where $r = \min\{m,n\}$

The columns of *U* are called the left singular vectors, the columns of *V* the right singular vectors, and the diagonal elements of D the singular values of the matrix *A*.

To establish the decomposition, first multiply Equation (1) from the right by *V* to obtain

$$AV = DU \tag{4}$$

Componentwise, the i[th] column of equation (4) is given as

$$Av_i = \sigma_i u_i \text{ for, } i = 1, 2, \ldots, n \tag{5}$$

Note that Equation (5) shows that u_i may be calculated directly from knowledge of A, v_i *and* σ_i.

We get another relation again by taking the transpose of Equation (1)

$$A^T = VD^T U^T \tag{6}$$

and then multiply from the right by U to obtain

$$A^T U = VD^T \tag{7}$$

Columnwise, equation (7) is given as

$$A^T u_i = \sigma_i v_i \text{ for } i = 1, 2, \ldots, n \tag{8}$$

Note that Equation (8) shows that v_i may be calculated directly from knowledge of A, v_i *and* σ_i.

Eigenvalues problems associated with SVD

There are two eigenvalues problems that can be obtained from the SVD. For the first eigenvalues problem we start with Equation (2) and multiply from the left by A^T

$$\begin{aligned} A^T AV = A^T UD &= \left(UDV^T\right)^T UD \\ &= VD^T \\ &= VD^2 \end{aligned} \tag{9}$$

$$D^2 = \begin{pmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_n^2 \end{pmatrix}$$

Let $R_1 = A^T A$ and $\Lambda_1 = D^2$, then we can write Equation (9) as the eigenvalues problem

$$R_1 V = V\Lambda_1 \tag{10}$$

For the second eigenvalues problem we start with Equation (7) and multiply from the left by A

$$\begin{aligned} AA^T U = \left(UDV^T\right) VD^T &= UDD^T \\ &= UD^T \end{aligned} \tag{11}$$

Let $R_2 = ?AA?^T$ and $\wedge_2 = DD^T$, then we can write Equation (11) as the eigenvalues problem

$$R_2 V = V\Lambda_2 \tag{12}$$

Where Λ_2 is given by (13)

$$\Lambda_2 = DD^T = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} \sigma_1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_n & 0 & \cdots & 0 \end{pmatrix} \tag{13}$$

which generates a square mxm matrix with diagonal elements

$$\Lambda_2 = \begin{pmatrix} \sigma_1^2 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_n^2 & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & & \cdots & 0 \end{pmatrix}$$

Because the diagonal elements $\Lambda_{kk} = 0$ for $k = n+1$, the eigenvectors (singular vectors) u_{n+1}, $u_{n+2}, \ldots, u_m$ are of no importance. As a result we define a new mxn matrix *U* (it is *U* with the last $m - n$ columns deleted) and a new nxn diagonal matrix *D* (whose diagonal elements are $\sigma_1, \sigma_2, \ldots \sigma_n$) and written as equation (14).

$$A = \tilde{U}\tilde{D}V^T \tag{14}$$

it can be expressed as rank one matrix as:

$A = \sigma_1 u_1 v_1^{\ T} + \sigma_2 u_2 v_2^{\ T} + \ldots + \sigma_r u_r v_r^{\ T}$ Which is very crucial in data compression

We consider that a host mxn image matrix ***'I'*** and apply SVD on host image to get matrix *U*, *D* and *V* and modifying singular value S using watermark image ***W*** of size mxn as *D'*. Apply SVD on *D'* to obtain its corresponding singular values as *D''*

Embedding process

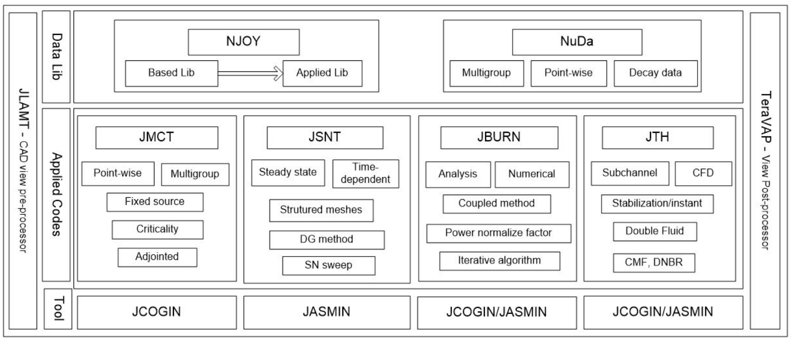


Figure 1: Image pixels at given position

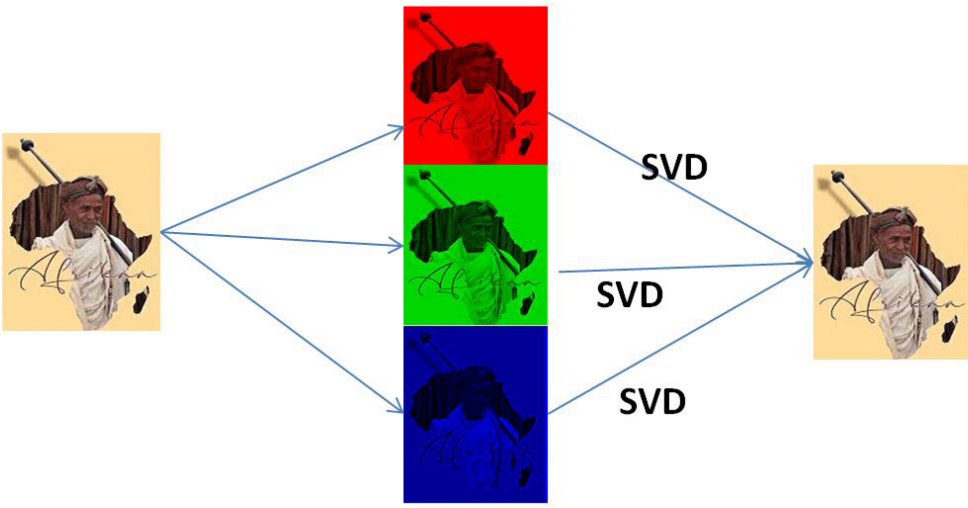


Figure 2: Images show RGB components

Consider a mxn matrix *'I'* representing host image or watermark image, to apply singular value decomposition (SVD) a colored image have to be separated into three band monochrome images, where each band corresponds to a different color, typically red, blue and green or RGB each takes values from (0-255) as shown in (Figures 1 and 2)

A colored image is vector valued function and mathematically expressed as:

$I(x,y) \rightarrow [r(x,y), b(x,y), g(x,y)]$, Representing RBG,

Then singular value decomposition applied to three matrices bands and obtained matrices *U*, *D* and *V* for these three matrixes separately and recombined to get: $I = U\,D\,V^T$

Modifying singular value *D* using watermark image *W* of size *mxn*

$$D' = D + \alpha W \tag{15}$$

Where:

D: Singular values of original image
W: Watermark image
α: Positive real adjusted for watermark strength

Apply SVD on D' of equation (15) to obtain its corresponding singular values D'' in (16)

$$D' = U'D''V'^T \tag{16}$$

Combining, we obtain a colored watermarked image in equation (17)

$$I^w = UD''V^T \tag{17}$$

Extraction process

First apply singular value decomposes to watermarked image I^w which is possibly distorted, and obtain

$$I^w = U^w D^w V^{wT} \tag{18}$$

Calculate matrix E according to equation (19)

$$E = U'D^w V'^T \tag{19}$$

Get the watermark image extracted from I^w as

$$W^e = \frac{E - D}{\alpha}$$

$$= \frac{U'D^w V'^T - D}{\alpha}$$

The singular values of an image have very good stability, that is, when a same perturbation is added to an image, its Singular values do not change significantly. Each singular value specifies the brightness of an image layer while the corresponding pair of singular vectors specifies the geometry or rotation of the image. The quality of watermarking algorithm will be evaluated through JPEG compression, Rotation, cropping, scaling, Median filtering, Gaussian noise injection, and blurring, sharpening attacks [16].

The performance can be measured by imperceptibility and robust capabilities. Stir Mark (standard benchmark) will be used to test the robustness of the proposed watermarking algorithm. The peak signal to noise ratio (PSNR) between original image I and watermarked image I^w and mean square error (MSE) between original watermark *W* and corresponding extracted watermark W^e will be measured for the quality and robustness capability.

The performance of the watermarking methods can be measured by imperceptibility and robust capabilities. Imperceptibility means that the superficial quality of the original image should not be distorted by the presence of watermark image. On the other hand, the robustness is a measure of the intentionally attacks and unintenally attacks. It was found that the image quality measured by peak signal to noise ratio (PSNR) among the watermarked images was larger than 42 db (B. Kim, J. G. Choi and D. Min 2003, pp.139-149) [17]. This peak signal to noise ratio is defined as [18,19].

$$PSNR = 10\log 10\left(\frac{Max_i}{MSE}\right)^2 \tag{20}$$

Where

Max_i: (19) is the largest value of pixel or picture element ranging from 0 - 255.

The PSNR is employed to measure the difference between an original image I and watermarked image I^w. For the robust capability, mean absolute error (MSE) measures the difference between an original watermark W and corresponding extracted watermark W^e [16].

$$MSE = \frac{1}{nm}\sum_{i=1}^{m}\sum_{j=1}^{n}(W_{ij} - W_{ij}^e)^2 \tag{21}$$

Where

W_{ij}: is watermark image and $i = 1,2,\dots,m$; $j = 1,2,\dots,n$
W_{ij}^e : is extracted watermark image and $i = 1,2,\dots,m$; $j = 1,2,\dots,n$

Generally, if PSNR value is larger than 40 db the watermarked image is within acceptable degradation levels, i.e. the watermarked are almost invisible to human visual system. A lower mean absolute error reveals that the extracted watermark W^e resembles the W more closely. The strength of digital watermarking method is accessed from the watermarked image I^w, which is further degraded by attacks and the digital watermarking performance of proposed method is compared with MSE and If a method has a lower MSE, it is more robust.

Results of lab Experiments

The experimental results are simulated with the software MATLAB R2017b version. All problems and solutions in Matlab are expressed in notation used in linear algebra and essentially involve operations using matrices and vectors. We are using a 256 × 256 pixel *"Lena"*, *"Abba Geda"*, and *"Logo"* colored original host images with JPEG format, and a 256 × 256 pixel colored images which is also in JPEG format for watermark images. These images are shown in (Table1).

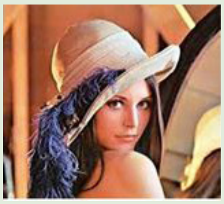
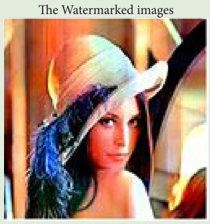
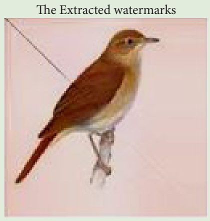
Host Images		
		
1. Lena	2. Abba Geda	3. Logo
		
4. Bird	5. Abba Geda	6. missile

Table 1: The first row contains Host images while second row contains corresponding watermark images

Host Images	Watermark Images	Watermarked images	Extracted watermarks	PSNR (DB)
		The Watermarked images 	The Extracted watermarks 	34.856

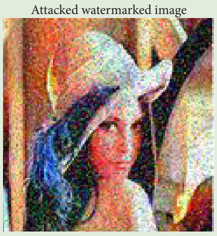
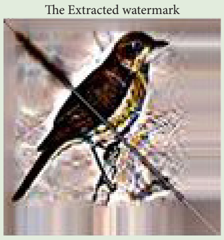
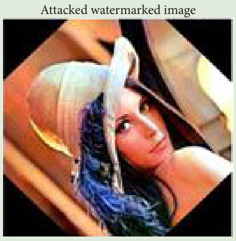
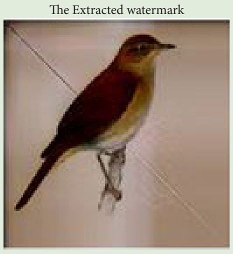
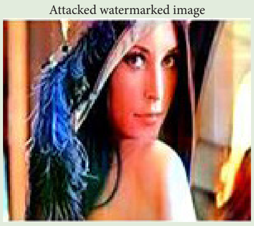
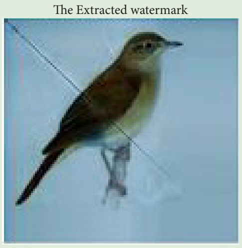
Host Images	Watermark Images	Watermarked images	Extracted watermarks	PSNR (DB)
		The Watermarked images 	The Extracted watermarks 	35.390
		The Watermarked images 	The Extracted watermarks 	37.091

Table 2: Shows the Host, watermark, watermarked and extracted watermark at (α = 0.2)

We claimed the embedding algorithm and extracting algorithm to identify the ownership of the original colored watermarked image as shown in Tables 2. The watermarked colored image is as pretty good as original host image.

For the following simulation alpha (α = 0.2) is used and the error ratio of the embedded watermark with attacks is measured by PSNR (DB). Simulation results suggest that this digital color watermarking algorithm is robust against many different common attacks such as cropping; rotation, noise, sharing, blurring and JPEG compression attacks see Table 3, 4 and 5. However, cropping is a geometrical manipulation and rotation is a geometrical distortion in practical application but due to singular vectors are rotation matrices the image is unaffected by rotation attack and less affected by cropping and JPEG compression attacks.

Generally, when we see the results of the experiment singular value based algorithm isles affected with geometric attacks and mostly affected with frequencies and noise attacks. If alpha's value is more than 0.2 then quality of original image and watermarked image is not good. So we are using the dumpy value in these techniques.

Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Logo	Noise Attacks ('salt & pepper',0.2)	Attacked watermarked image 	The Extracted watermark 	29.16 0
	Rotation Attacks (45 counter clockwise)	Attacked watermarked image 	The Extracted watermark 	28.860
	Cropping Attacks	Attacked watermarked image 	The Extracted watermark 	28.871

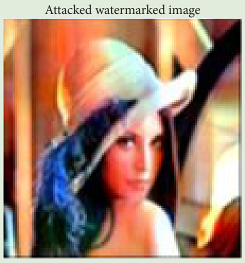
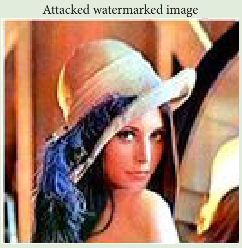
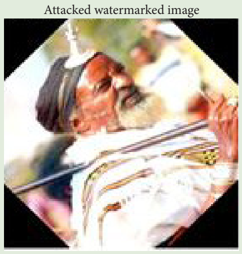
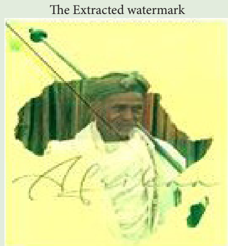
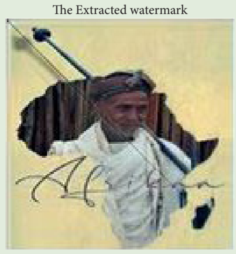
Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Logo	Sharping Attacks High pass filter	Attacked watermarked image 	The Extracted watermark 	28.846
	Blurring Attacks Low pass filter	Attacked watermarked image 	The Extracted watermark 	29.143
	JPEG compression (Taking 64 eigenvalues)	Attacked watermarked image 	The Extracted watermark 	29.252

Table 3: Extracted watermarks after different attacks

Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Abaa Geda	Noise Attacks ('salt & pepper',0.2)	Attacked watermarked image 	The Extracted watermark 	30.510
	Rotation Attacks (45 counter clockwise)	Attacked watermarked image 	The Extracted watermark 	48.799
	Cropping Attacks	Attacked watermarked image 	The Extracted watermark 	30.004

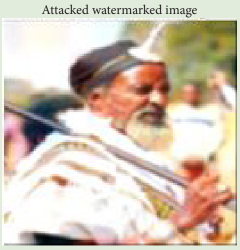
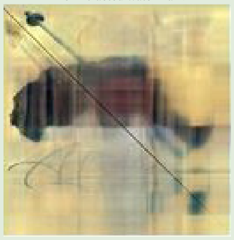
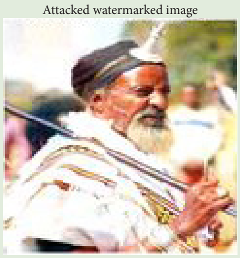
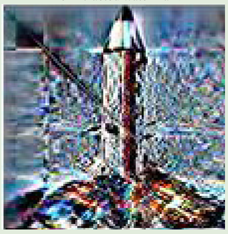
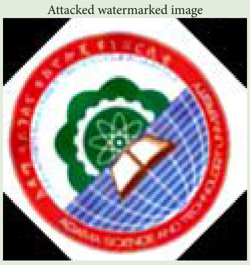
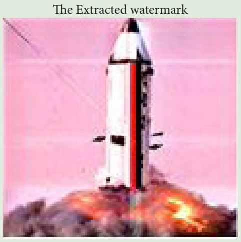
Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Abaa Geda	Sharping Attacks High pass filter			28.990
	Blurring Attacks Low pass filter			30.507
	JPEG compression (Taking 64 eigenvalues)			30.351

Table 4: Extracted watermarks after different attacks

Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Logo	Noise Attacks ('salt & pepper',0.2)			29.955
	Rotation Attacks (45 counter clockwise)			39.750
	Cropping Attacks			30.657

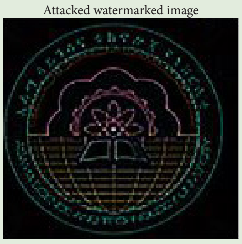
Host	Types of Attacks after watermark	Attacked watermarked image	Extracted watermark	PSNR (DB) values
Logo	Sharping Attacks High pass filter	Attacked watermarked image 	The Extracted watermark 	28.909
	Blurring Attacks Low pass filter	Attacked watermarked image 	The Extracted watermark 	29.205
	JPEG compression (Taking 64 eigenvalues)	Attacked watermarked image 	The Extracted watermark 	32.970

Table 5: Extracted watermarks after different attacks

Conclusions

A color image watermarking scheme based on singular value decomposition for copyrights protection was studied in this paper. The main advantages of this method are both the host and embedded images are colored. Experiments show that watermarked colored image is perceptually invisible and also robust against different attacks; especially geometric attacks such as rotation and cropping. Therefore, we conclude that this method is suitable for using color image information to protect data of colored images that will be sent through digital Medias. For future work, metaheuristic algorithm will be used to improve the efficiencies of watermarking. The quality of watermarked and extracted image is the tradeoff values of alpha. If the value of alpha is less than 0.3 then quality of the original image and watermarked image is good and also seen in [17]. The experimental results also show that the proposed methods are effective and robust against geometrical attacks and JPEG compression attacks.

Acknowledgment

First of all, we would like to express our deepest and special thanks to Adama Science and Technology University, Department of Applied Mathematics for their all rounded support. We would like to extend our thanks to collogue for their valuable comments.

References

1. Podilchuk CI, Delp EJ (2001), Digital Watermarking: Algorithms and Applications. IEEE Signal Process Mag 18: 33-46.

2. Santhi V, Thangavelu A (2009), DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1: 424-9.

3. Lai CC, Tsai CC, (2010), Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Trans Instrum Meas 59: 3060-3.

4. Lin PY, Lee JS, Chang CC (2009), Dual Digital Watermarking for Internet Media Based on Hybrid Strategies. IEEE Trans Circuits Syst Video Technol 19: 1169-77.

5. Hemdan EED, El-Fishaw N, Attiya G, El-Samii FA (2013) Hybrid Digital Image Watermarking Technique for Data Hiding. IEEE 30th National Radio Sci Conf.

6. Ramakrishnan S, Gopalakrishnan T, Balasamy K (2015) SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform. Comput Sci Inf Technol 155-67.

7. Bisla N, Chaudhary P (2013) Comparative Study of DWT and DWT-SVD Image Watermarking Techniques. Int J Adv Res Comput Sci Eng 3: 821-5.

8. Malakooti MV, Panah ZF, Hashemi SM (2013) Image Recognition Method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

9. Ram B (2013) Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform. Int J Adv Res Technol 2.

10. Singh P, Agarwal S (2013) A Hybrid DCT-SVD Based Robust Watermarking Scheme for Copyright Protection. Int Confon Emerging Trends Eng Technol.

11. Santhi V, Thangavelu A (2009) DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1: 424-9.

12. Lai CC (2011), A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Process 21: 522-7.

13. Santhi V, Thangavelu A (2009 DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1.

14. Kozat SS, Venkatesan R, Mihcak MK (2004) Robust perceptual image hashing via matrix invariants. Int Conf Image Process 5: 3443-6.

15. Nan Run Zhou, An Luo, Wei Ping Zou (2018) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimedia Tools Appl 1-17.

16. Nan Run Zhou, Wei Ming Xia, Ru Hong Wen (2018) imperceptible digital watermarking scheme in multiple transform domains. Multimedia Tools Appl 77: 30251-67.

17. Jia Sl (2014) A novel blind color images watermarking based on SVD. Int J Light Electron Opt.

18. Kim B, Choi JG, Min D (2003) Robust Digital Watermarking Method Against Geometric Attacks. Real Time Imaging 9: 139-49.

19. Manjit Thapa, Sandeep Kumar Sood (2011) On Secure Digital Image Watermarking Techniques. J Inf Secur 2: 169-84.