A robust and secure watermarking scheme based on singular values replacement

AKSHYA KUMAR GUPTA* and MEHUL S RAVAL

Dhirubhai Ambani Institute of Information and Communication Technology,
Gandhinagar 382 007, India
e-mail: akshya_12@yahoo.com; mehul_raval@daiict.ac.in

Abstract. Digital watermarking is an application associated with copyright protection. Any digital object can be used as a carrier to carry information. If the information is related to object then it is known as a watermark which can be visible or invisible. In the era of digital information, there are multiple danger zones like copyright and integrity violations, of digital object. In case of any dispute during rights violation, content creator can prove ownership by recovering the watermark. Two most important prerequisites for an efficient watermarking scheme are robustness and security. Watermark must be robust and recoverable even if a part of content is altered by one or more attacks like compression, filtering, geometric distortions, resizing, etc. In this work, we propose a blind watermarking scheme based on the discrete wavelet transform (DWT) and singular value decomposition (SVD). Singular values (SV's) of high frequency (HH) band are used to optimize perceptual transparency and robustness constraints. Although most of the SVD-based schemes prove to be robust, little attention has been paid to their security aspect. Therefore, we introduce a signature-based authentication mechanism at the decoder to improve security. Resulting blind watermarking scheme is secure and robust.

Keywords. Authentication; security; watermarking.

1. Introduction

Fast development of digital technologies has improved the ways to access information. These new technologies enable us to store, transfer and process digital content with less time, lower complexities and better efficiency. However, digitization also brings in disadvantages like illegal reproduction and distribution of digital content. Internet plays a very crucial role in circulation of illegal and unauthorized digital content. This increases the risk of violating owner right and hampering authenticity of a digital content. One way to protect digital content against illegal reproduction and distribution is to embed some extra information called watermark into it. The

---

*For correspondence

information should be embedded in secure and robust manner such that it remains resistive to malicious attempts of removal (Katzenbeisser & Petitcolas 2000). Usually the watermark is the information about the digital content it intends to protect.

A watermark should be embedded in such a way that it remains detectable as long as the perceptual quality of the digital content stays at an acceptable level (Lee & Jung 2001).

In general, any watermarking system consists of following parts: Watermark, Carrier, Encoder, Decoder.

The conceptual model of the watermarking system is explained in figure 1 (Podilchuk & Delp 2001). Original image depicts the carrier which needs protection. The watermark encoder embeds the watermark in to the cover image. The watermark can be a pseudo-random number or binary sequence. The optional key is used to enhance the security of the system. Decoder estimates the watermark from the received image with the help of key and original image if required. Watermarked image is subjected to various forms of manipulations on communication channel.

Watermarking schemes can be classified based on the presence or absence of original content at the time of watermark detection.

 (i) Non-blind scheme: It requires presence of original content during watermark detection.
(ii) Blind scheme: It does not require the presence of original content while decoding the watermark.

In the early days non-blind watermarking schemes were popular as they were more robust than blind schemes. It is due to the fact that in watermarking model, original content is treated as a noise source to watermark, which is the signal of interest. Presence of original content at the receiver nullifies the effect of this noise. However, non-blind schemes suffer from two distinct disadvantages.

 (i) Security compromise: Non-blind detection does not guarantee unequivocal claims of ownership by the content creator. Attacker can easily fool the system and even worst, may claim the ownership by inserting another watermark in the content.
(ii) Practical application constraints: It is not possible to ensure presence of original content during detection for every watermarking application. For e.g., copy protection in DVD.

With the development in watermarking research, blind schemes are matching the performance criteria of non-blind schemes. Hence state-of-art watermarking system offers blind detection, which is the case with this work as well.
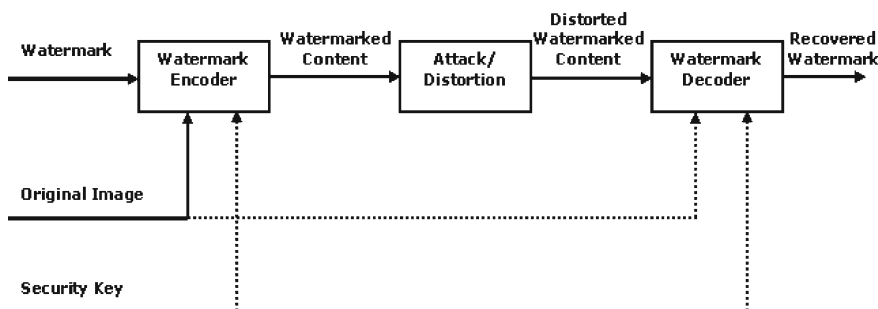

Figure 1. A typical watermarking system.

In this paper, we propose a blind, secure and robust watermarking scheme based on SVD and DWT. The paper is organized in different sections; section 2 presents the prior art on watermarking, describes SVD with its application and importance to watermarking. In section 3, we propose a DWT–SVD based watermarking scheme. Section 4 highlights the authentication problem with prior SVD based watermarking approaches and also suggests an authentication mechanism to improve security of SVD based watermarking schemes. Section 5 provides the details of experiments performed with their results; finally conclusions are drawn in section 6.

2. Prior art

So far many watermarking schemes have been proposed with the intentions of improving robustness vis-a-vis perceptual quality. Compression is most common form of attacks in watermarking. Two widely used image compression standards are JPEG and JPEG2000. The former is based on the discrete cosine transform (DCT), and the latter is based on discrete wavelet transform (DWT). Many watermarking schemes which are robust against compression have been developed using these transforms. Raval & Rege (2003) proposed a DWT based multiple watermarking schemes. Image was decomposed in two levels and watermarks were inserted in LL (low frequency) and HH (high frequency) bands. The scheme showed good results against wide range of attacks like compression, noise addition, histogram equalization but could not resist rotation, scaling and print-scan attacks.

Kasmani & Naghsh-Nilchi (2008) proposed a combination of DWT and DCT to embed the binary watermark. They performed 3-level DWT decomposition and then applied DCT to embed the watermark. Results showed a good watermark recovery against many attacks but this scheme suffers from high time complexity. Moreover, it had a non-blind detection.

Recently singular value decomposition became very popular in watermarking schemes due to its attractive mathematical features. In the next part, we briefly discuss SVD and its role in the watermarking.

2.1 *Singular value decomposition (SVD)*

SVD is one of the most useful tools in linear algebra with several applications in image compression, watermarking, and other signal processing areas. If A is an nxn matrix, then SVD of matrix A can be defined as

$$A = U * S * V^{T}, \tag{1}$$

where U and V are the orthogonal matrices and S is a diagonal matrix. Diagonal elements of S are the singular values and they satisfy the following property

$$s\,(1,1) > s\,(2,2) > s\,(3,3) > \dots\dots\dots\dots\dots\dots > s\,(n,n)\,. \tag{2}$$

SVD is popular for the watermarking (Andrews & Patterson 1976; Zhou & Chen 2004) because (i) few singular values can represent large portion of signal energy, (ii) SVD can be applied to square and rectangular images, (iii) the SV's (singular values) of an image have very good noise immunity, i.e., SV's do not change significantly when a small perturbation is added to an image intensity values, (iv) SV's represent intrinsic algebraic properties.

An experiment was conducted using 512×512 8 bit gray scale Lena image to check the noise immunity of SVD. Four most significant singular values of original image were compared

with singular values obtained after application of various attacks. Table 1 shows outcome of this experimentation.

From table 1 we conclude that singular values are fairly robust against perturbation. Due to its robustness against noise, SVD became a popular tool in watermarking domain.

2.2 *Watermarking schemes based on SVD*

In recent years several watermarking algorithms have been proposed based on SVD. The main idea in these approaches is to compute the SVD of a cover image and then modify singular values to embed the watermark. Some algorithms used only SV's to embed the watermark. Recently hybrid watermarking algorithms have been proposed where different transforms domain are used with SVD. In the following subsection, some of the popular SVD based schemes are discussed.

2.2a *Pure SVD based schemes*: Many of the earlier algorithms, based on SVD, embeds watermark directly into singular values. For example, Liu & Tan (2002) proposed an algorithm in which watermark was embedded into the SVD domain and the detection was blind in nature. Results showed that scheme proved resilient against compression, filtering, cropping but could not resist rotation, scaling and print-scan attacks.

Ghazy *et al* (2007) divided the image into non-overlapping blocks and then applied SVD to these blocks. Singular values of these blocks were used to embed the watermark. This scheme gave good results against compression, filtering, noise addition but failed against cropping and geometric attacks.

With an aim to increase the robustness of watermarking scheme Bhandari *et al* (2005) used spread spectrum (SS) along with SVD. They used two watermarks during embedding; one was inserted using spread spectrum technique and other by pure SVD. SS techniques provided robustness against compression, rotation, filtering, scaling, print and scan attack, while, SVD offered good robustness against noise addition and histogram equalization. Hence, these two complementary techniques covered wide range of attacks however, scheme was non-blind in nature.

2.2b *Hybrid SVD based schemes*: The SVD schemes which are using transform domain coefficients for decomposition are called hybrid SVD schemes. DCT, DWT, FFT are among popular frequency transforms. A hybrid method based on DCT and SVD has been proposed by Quan

Table 1. Variation in singular values after applying attacks.

Image	S1	S2	S3	S4
Lena image (original values)	151.5234	42.2745	36.1516	27.9067
JPEG Compression (Q = 20)	151.6007	42.2129	36.0787	27.6894
Rotation (15°)	144.1636	48.0665	39.9409	28.7351
Scaling (512->256->512)	152.1418	42.1731	36.0141	27.7552
Scaling (512->1024->512)	152.7299	42.2633	36.1170	27.8758
Gaussian noise (M = 0, Var = 0.01)	158.5279	40.7767	35.4015	27.3755
Salt and pepper noise (M = 0, Var = 0.01)	152.3987	41.9533	35.8831	27.7077
Median filter [3×3]	151.2235	42.3403	36.1912	27.9125
Histogram equalization	151.5234	42.2745	36.1516	27.9067

& Qingsong (2004). They applied DCT to the cover image and coefficients are mapped to frequency bands using zig-zag scanning. SVD was then applied to each band. Singular values of the DCT-transformed visual watermark are then used to modify the singular values of each band of the cover image. Results displays robustness against compression, filtering and cropping but watermark cannot survive against geometrical attacks and print-scan attack. The scheme was computationally expensive and non-blind in nature.

A SVD based algorithm using DWT has been presented by Ganic & Ahmet Eskicioglu (2004) which is very similar to the algorithm by Quan & Qingsong (2004). The cover image is decomposed using DWT into four sub bands. SVD is applied to each sub band and also to the watermark. Singular values of the cover image are modified using the singular values of the watermark during embedding process. This scheme gives comparatively good results vis-a-vis all the schemes discussed so far.

Study in this section shows that robustness of SVD-based watermarking schemes is reasonably good but it can be improved using suitable combination of the transform domain and SVD.

3. Proposed watermarking scheme

We propose a basic watermarking which is based on cascading DWT with SVD. DWT decomposes the image into four frequency bands: LL, HL, LH, and HH band. LL band represents low frequency, HL and LH represent middle frequency and HH represents high frequency band, respectively. LL band represents approximate details, HL band gives horizontal details, LH provides vertical details and HH band highlights diagonal details of the image. In this proposal, we select HH band to embed the watermark because it contains the finer details and contributes insignificantly to the image energy. Hence watermark embedding will not affect the perceptual fidelity of cover image. Moreover, high energy LL band coefficient cannot be tweaked beyond certain point as it will severely impact perceptual quality. Also, Raval & Rege (2003) observed that watermark inserted in HH band survives certain image processing operations like noise addition, intensity manipulation and limitation of the human visual system can be exploited by inserting watermark into HH band. HVS fails to differentiate changes made to HH band.

The proposed scheme is based on the idea of replacing singular values of the HH band with the singular values of the watermark. In table 2, singular values of the HH band of different test images are given. It is observed that singular values lie between 84 and 173. If a watermark is selected such that its singular values lies within the given range, then the energy of the singular values of watermark will be approximately equal to the energy of the singular values of the HH band. Hence the replacement of the singular values will not affect perceptual quality of image and the energy content of HH band.

Table 2. Singular values of HH frequency band of different test images.

Image	Singular values	
	Max	Min
Lena	142.6490	0
Bubble	84.7352	0
Building	173.2125	0
Cameraman	109.2292	0

Watermark used for experimentation in this scheme is preprocessed to have singular values within the range of 0–150 and it closely matches the singular values of the given test images. Watermark size is made equal to the size of the HH band.

3.1 *Watermark embedding algorithm*

(i) Watermark W is decomposed using SVD

$$W = U_w * S_w * V_w^T. \tag{3}$$

(ii) Apply Haar wavelet and decompose cover image into four sub-bands: LL, HL, LH, and HH.
(iii) Apply SVD to HH band.

$$H = U_H * S_H * V_H^T. \tag{4}$$

(iv) Replace the singular values of the HH band with the singular values of the watermark.
(v) Apply inverse SVD to obtain the modified HH band.

$$H' = U_H * S_w * V_H^T. \tag{5}$$

(vi) Apply inverse DWT to produce the watermarked cover image.

3.2 *Watermark extraction algorithm*

(i) Using Haar wavelet, decompose the noisy watermarked image into four sub-bands: LL, HL, LH, and HH.
(ii) Apply SVD to HH band.

$$H = U_H * S_H * V_H^T. \tag{6}$$

(iii) Extract the singular values from HH band.
(iv) Construct the watermark using singular values and orthogonal matrices U_w and V_w obtained using SVD of original watermark.

$$W_E = U_w * S_H * V_w^T. \tag{7}$$

This constitutes a blind decoding as watermark extraction process does not require original cover image for extracting the watermark at the receiver.

4. Authentication mechanism in the proposed scheme

Zhang & Li (2005) observed an authentication problem in the basic SVD based approaches proposed by Zhou & Chen (2004) and Ganic & Ahmet Eskicioglu (2004). This section describes the common problem with majority of SVD-based schemes appearing in the state-of-art literature. The solution is proposed in the later half of the section. To demonstrate the problem, Zhang & Li (2005) set-up an experiment using two Lena images. Two different watermarks were embedded in them as shown in figure 2 using basic SVD scheme. The watermarks were embedded by modifying the singular values of Lena image with the singular values of the watermarks.

Decoder estimates the watermark by combining SV's extracted from one watermarked image and using orthogonal matrices of other watermark. Figure 3 shows that the decoder extracted SV's from watermarked image-2 and combine them with orthogonal matrices (U_1 and V_1) for watermark reconstruction. As a result, watermark-1 is recovered instead of watermark-2.
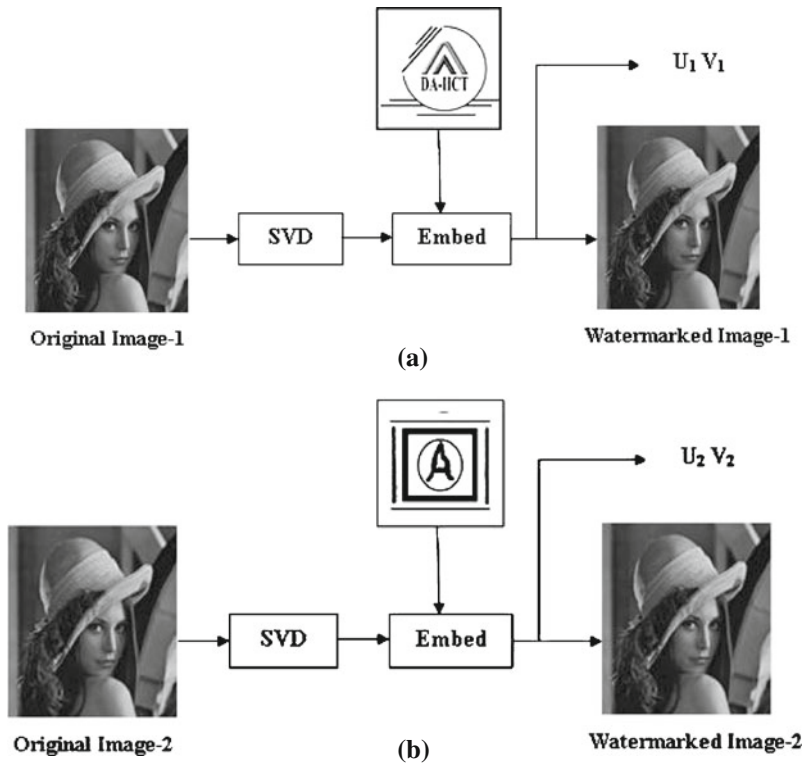
Figure 2. Embedding of watermark.

Zhang & Li (2005) explained that the orthogonal matrices U and V preserve major information as they represent eigen vectors of the respective singular values. When inverse SVD is applied, eigen vectors plays an important role in reconstruction. Hence if any singular matrix is used along with eigen vectors it will generate the correlated output instead of the actual output. The correlation will be high if the unmatched singular values will be approximately equal to the original singular values. So it gives rise to large number of false-positives during watermark detection and also presents a security threat. This threat can be seen as problem of unauthorized embedding where in an attacker may use his/her own set of eigen vectors during watermark extraction and claims false ownership. To overcome these drawbacks, we propose a signature-based
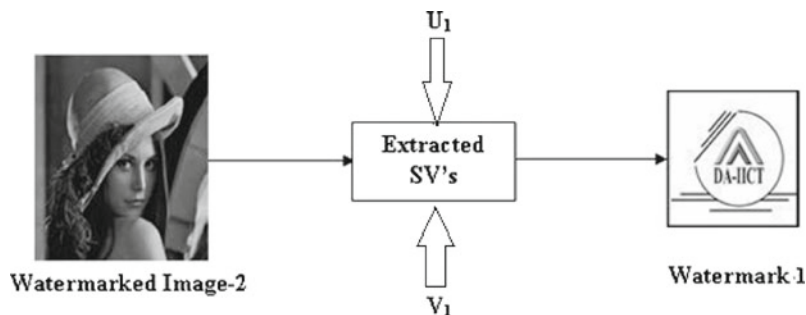
Figure 3. Extraction of watermark.

authentication mechanism for U and V matrices. Orthogonal matrices (U and V) are authenticated before combining them with singular values to generate watermark. A unique signatures corresponding to the orthogonal matrices are generated and embedded into the cover image along with the watermark. Decoder extracts these signatures, authenticates orthogonal matrices and then proceeds with the extraction of watermark. This will ensure a correct mapping between the singular values and orthogonal matrices.

4.1 *Generation of signature*

Digital signature of the orthogonal matrices is a unique binary string generated through a hashing function. In addition, the digital signature must be random, so that an attacker cannot predict them. Digital signature for the orthogonal matrices is generated as follows.

4.1a *Proposed algorithm*:

  (i) Sum the column of orthogonal matrices and create 1-D array.
 (ii) Based on the threshold, map the array values into corresponding binary digits.
(iii) By XORing the binary digits generate the signature for the given orthogonal matrices.

Threshold value plays an important role while mapping and it is used to randomize the mapping, improving the security.

4.2 *Proposed authentication scheme*

Embedded signature should remain robust against processing manipulation. Change in signature bits at decoder causes authentication to fail. Thus, signature bits should be embedded into high energy region for improved robustness. The length of the signature is kept small to minimize changes in the high energy coefficients. Signature should remain robust against wide range of attacks hence one set of signature bits are embedded into LL4 and another set is embedded into HH4 band to ensure recovery from at least one of the band. The algorithm for embedding and extracting the signature is as follows.

4.2a *Signature embedding*:

  (i) Generate the signature of N bits for the U and V matrices of watermark.
 (ii) Using Haar wavelet, decompose the cover image into 4 sub-bands: LL, HL, LH, and HH. Further decompose LL band to the 4th level.
(iii) Select N random coefficient from LL4 and HH4 band with the help of secret key. Convert the integer part into the binary code of L bits.
(iv) Replace the n th bit of the coefficient with signature bit and then convert the binary code to its decimal representation.
 (v) Apply the inverse DWT with modified LL4 and HH4 band coefficients.

4.2b *Signature extraction*:

  (i) Using DWT, decompose the watermarked image into 4 sub-bands: LL, HL, LH, and HH with help of Haar wavelet and further decompose LL band to the 4th level.

 (ii) Select N random coefficient from LL4 and HH4 band with the help of shared secret key. Convert the integer part of selected coefficient into the binary code of L bits.
(iii) Extract the n th bit from the coefficient to extract the signature.
(iv) Generate signature using U and V matrices of the original watermark at the receiver and compare it with extracted signature. If they match, authenticate U and V matrices and use them in watermark estimation.

8 bit signature is generated for the authentication. Selected coefficients from LL4 and HH4 were converted to 16 bit binary number and 10th most significant bit position is replaced with signature bits.
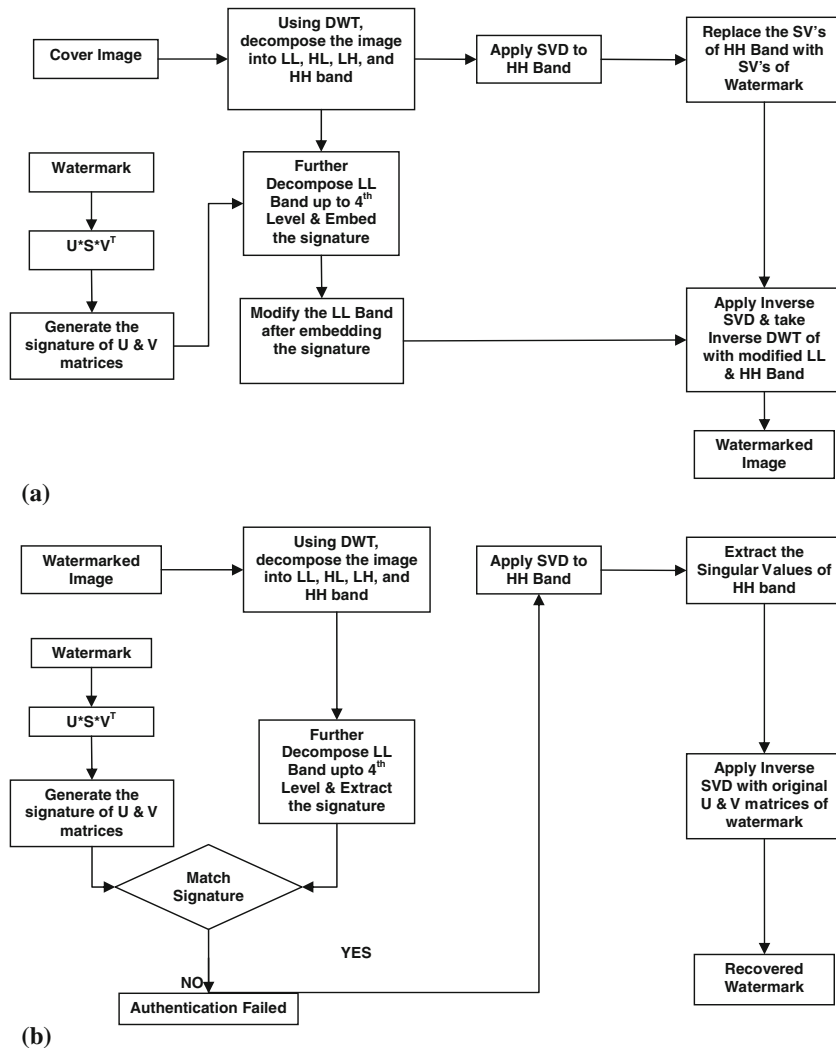
Figure 4. (**a**)–(**b**) Block diagram of proposed scheme at encoder and decoder side.

This authentication mechanism is implemented in parallel with the watermarking scheme. Figures 4a and b show the block diagram of the proposed scheme. The encoder will embed the watermark and signature bits according to the proposed scheme.

Decoder extracts the signature and matches it with the regenerated signature for authentication of U & V matrices. If matching criteria is satisfied, then decoder will continue estimating watermark.

5. Experimentation and results

It is important to test an image watermarking scheme on different types of images for fair comparison. In our experiments 512×512 8 bit gray scale test images namely 'Lena', 'Bubble', 'Cameraman' and 'Building' were used as shown in figures 5a–d. All the images have different intensity variations and background. 256×256 gray scale DA-IICT sample logo is used as a watermark. The watermarked images were subjected to various attacks to check the robustness of the scheme. The method's performance is compared with the scheme proposed by Ganic & Ahmet Eskicioglu (2004).

Correlation coefficient between recovered and original watermark, is used as a metric for performance evaluation. The value of correlation coefficient lies between -1 and $+1$. If two watermarks are identical, then its value will be $+1$, if they are completely opposite (i.e., one is negative of other) then its value will be -1 and it will be 0 if watermarks are completely uncorrelated. The correlation coefficient value from 0.4 to 0.9 indicates significant similarity between two watermarks.

All the experimentation and testing is performed on Windows-XP platform (2002 edition). MATLAB version 7.7 is used for the implementation of the proposed algorithm.
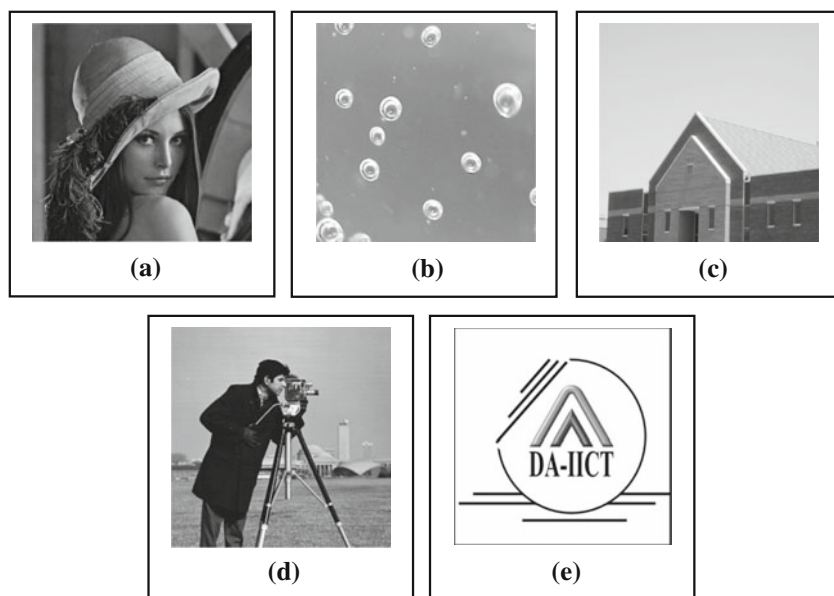
Figure 5. (**a**)–(**d**) Grayscale test images (512×512), (**e**) Grayscale watermark (256×256).

Table 3. PSNR of watermarked test images.

Image	Lena	Bubble	Building	Cameraman
PSNR (in dB)	43.3374	50.6747	45.7734	47.4209
Correlation coefficient	0.9994	0.9977	0.9988	0.9993

5.1 *Experiments*

Multiple experiments were executed to validate perceptual quality, robustness and security of the proposed water marking scheme. Their results and analysis are as follows.

5.1a *Perceptual quality*: Peak-signal-to-noise ratio (PSNR) and correlation coefficient are used as a metric to check perceptual similarity between original and watermarked image. The PSNR (in dB) of the watermarked images are shown in table 3. According to Chen *et al* (1998), PSNR above 40 dB indicates a good perceptual fidelity. It can be observed that PSNR for the different test images is above 40 dB which indicates the effectiveness of the proposed scheme. Correlation coefficient between original and watermarked image is also very close to 1, indicating excellent perceptual fidelity.

5.1b *Robustness*: After embedding the watermark, a given set of attacks were applied on the watermarked image to test the robustness of the scheme. The various attacks are compression, filtering, rotation, noise addition, scaling, cropping and print-scan. Figures 6 and 7 shows the watermarked image after various attacks.

Correlation coefficient is used as a metric to quantify resistivity of scheme against various attacks. Recovered watermarks for the respective set of attacks are shown in figures 8a–k.

These results show that the proposed watermarking scheme is robust against large set of attacks especially against geometrical and print-scan attacks. Decoder does not require any information about the original image.

5.1c *Authenticity*:

 (i) At the receiver decoder regenerates the signature for U_w and V_w matrices of original watermark using steps in-lined in Section 4.2 .
 (ii) Extract the signature of U_w and V_w matrices from the received image.
(iii) If extracted signature matches with the computed signature, U_w and V_w matrices are used during watermark extraction.

Figure 6. (**a**) Original cameraman image, (**b**) watermarked cameraman image.
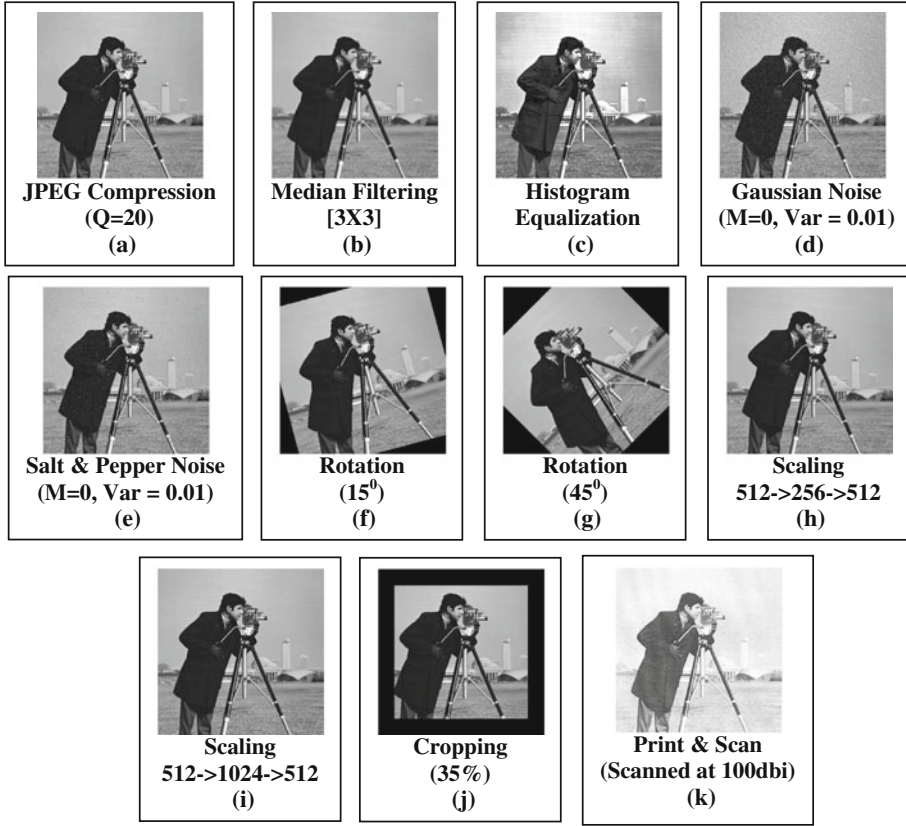
Figure 7. Watermarked cameraman image after applying various attacks.

Signature bits from LL4 band were recovered for compression, filtering and geometric attacks. Whereas for attacks like histogram equalization, Gaussian noise addition and print-scan, signature bits from HH4 band was recovered. Cameraman image was used in testing and table 4 shows the results of signature bit recovery with respect to given attacks.

Table 4 shows that all the 8 signature bits were recovered from either LL4 or HH4 band but for attacks like gaussian noise addition, histogram equalization and print-scan fewer bits were recovered. If the anticipated severity of attacks is high, signature bit matching criteria can be relaxed for attacks like print-scan and recovery of few correct bits can be interpreted as case of correct authentication.

5.2 *Comparison between proposed and existing DWT–SVD based approach*

Table 5 shows the comparison between the proposed and scheme presented by Ganic & Ahmet Eskicioglu (2004). They proposed a non-blind watermarking scheme with four watermarks embedded into all frequency bands of the cover image using DWT. The author's motivation for multiple watermarks was to ensure survival of at least one against attacks. Correlation coefficient is used as metric to quantify the robustness of the recovered watermark. We compared the performance based on LL band watermark recovery with correlation coefficient as a metric.
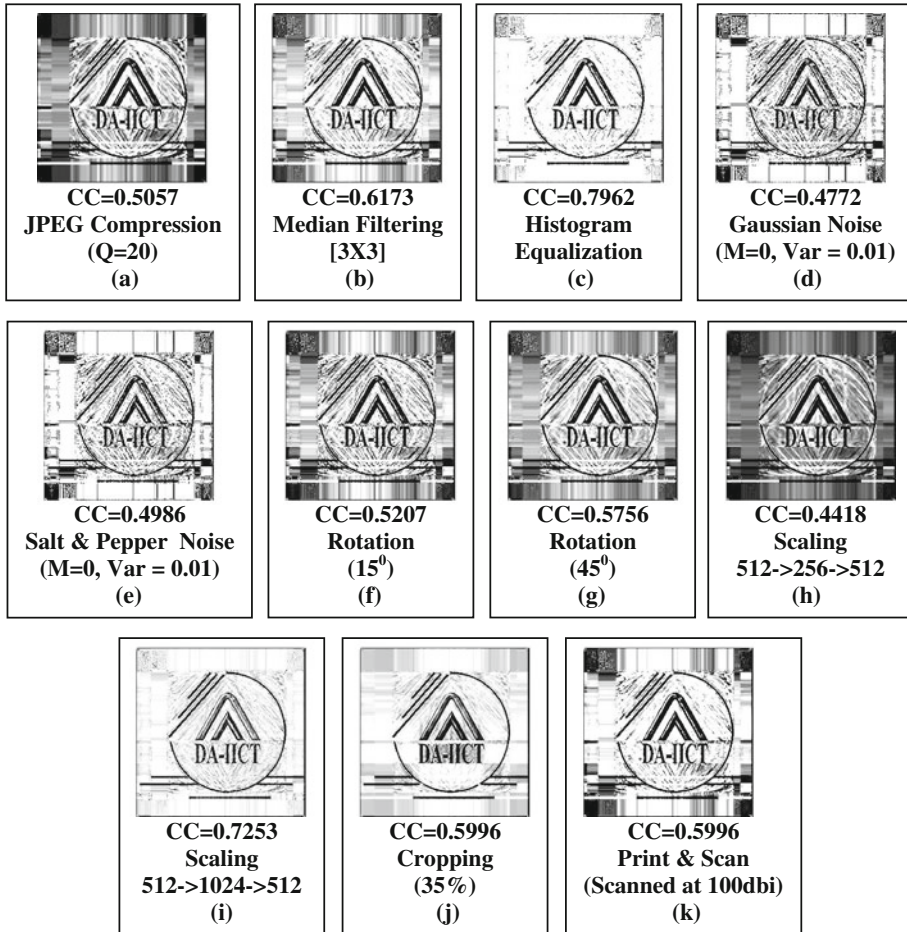
Figure 8. Extracted watermark by the proposed algorithm after applying various attacks.

Table 4. Recovered signature bits.

Attack	From LL4 Band	From HH4 Band
JPEG Compression(QF = 20)	8	8
Rotation (15°)	8	8
Rotation (45°)	8	8
Median filtering	8	7
Salt and pepper noise(M = 0, Var = 0.01)	8	8
Scaling (512->256->512)	8	7
Scaling (512->1024->512)	8	6
Cropping (35%)	8	8
Gaussian noise	3	6
Histogram equalization	4	6
Print-scan	5	7

Table 5. Comparison between the proposed and existing scheme.
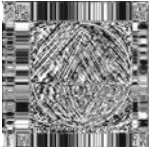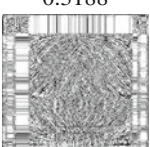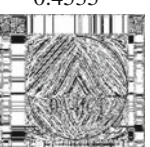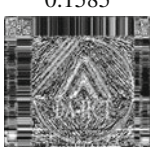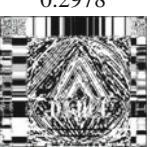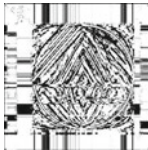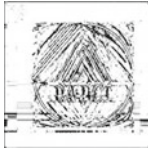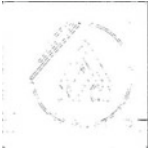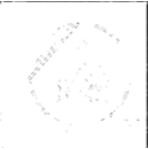
Attacks	Proposed scheme	Ganic & Ahmet Eskicioglu (2004)			
	LL Band	LL Band	LH Band	HL Band	HH Band
		Correlation coefficient of the recovered watermark			
JPEG compression (QF = 20)					
	0.5057	0.9014	−0.0635	−0.3440	−05106
Median filtering					
	0.6173	0.2422	−0.6471	−0.5230	0.0110
Histogram equalization					
	0.7962	0.9003	0.8323	0.8048	0.7006
Gaussian noise (M = 0, V = 0.01)					
	0.4772	0.2078	0.3188	0.2978	0.4535
Salt and pepper noise (M = 0, V = 0.01)					
	0.4986	0.1585	0.2997	0.2978	0.4773
Rotation (15°)					
	0.5207	0.0959	−0.0157	0.3259	−0.1543
Rotation (45°)					
	0.5756	0.0778	−0.0715	−0.2327	−0.6567

Table 5. *contd.*

Attacks	Proposed scheme	Ganic & Ahmet Eskicioglu (2004)			
	LL Band	LL Band	LH Band	HL Band	HH Band
		Correlation coefficient of the recovered watermark			
Scaling (512->256->512)	0.4418	0.0244	−0.6580	−0.5930	−0.6030
Scaling (512->1024->512)	0.7253	0.2733	−0.6404	−0.5663	−0.6776
Cropping (35%)	05231	−0.3030	0.2637	0.2994	0.1695
Print and scan	0.5231				

Results in table 5 show that the proposed scheme performs better than the scheme proposed by Ganic & Ahmet Eskicioglu (2004) in spite of blind detection. The performance is improved in terms of robustness and additionally proposed scheme is resilient to the print and scan attack which is not the case with most of the existing SVD-based schemes. Closeness between original and extracted watermark has improved as reflected in terms of correlation coefficient.

6. Conclusion

Our proposed scheme has high degree of robustness which is validated by recovering the watermark against print and scan attack which is among the strongest attacks. Even though scheme is blind in nature it gives result better than non-blind ones. Many of the existing DWT and SVD based approaches do not handle the issue of authentication and security. The proposed method covers this flaw by incorporating signature-based authentication mechanism. Thus the resultant method is both robust and secure.

References

Andrews H C and Patterson C L 1976 Singular value decomposition (SVD) image coding. *IEEE Trans. Commun.* 24(4): 425–432

Bhandari Kunal, Mitra Suman K and Jadhav Ashish 2005 *A hybrid approach to digital image watermarking using singular value decomposition and spread spectrum*. S K Pal *et al* (eds): PreMI, LNCS 3776: 272–275

Chen T S, Chang C C and Hwang M S 1998 A virtual image cryptosystem based upon vector quantization. *IEEE Trans. Image Process.* 7(10): 1485–1488

Ganic Emir and Ahmet Eskicioglu M 2004 Robust DWT-SVD domain image watermarking: Embedding data in all frequencies. *Proceedings of the workshop on Multimedia and Security* 166–174

Ghazy R A, El-Fishawy N A, Hadhoud M M, Dessouky M I and El-Samie F E A 2007 An efficient block-by-block SVD-based image watermarking scheme. *Radio Science Conference*, NRSC 1–9

Kasmani S A and Naghsh-Nilchi A 2008 A new robust digital image watermarking technique based on joint DWT-DCT transformation. *Convergence and Hybrid Information Technology ICCIT '08 Third International Conference* 2(1): 539–544

Katzenbeisser Stefan and Petitcolas Fabien A 2000 Information hiding techniques for steganography and digital watermarking. Norwood, MA, USA: Artech House, Inc.

Lee Sin-Joo and Jung Sung-Hwan 2001 A survey of watermarking techniques applied to multimedia. industrial electronics. *Proceedings. ISIE 2001. IEEE International Symposium* pp.272–277

Liu R and Tan T 2002 A SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimed.* 4(1): 121–128

Podilchuk C I and Delp E J 2001 Digital watermarking: Algorithms and applications. *Signal Process. Mag. IEEE.* 18(4): 33–46

Quan Liu and Qingsong Ai 2004 Combination of DCT-based and SVD-based watermarking scheme. *Signal Processing Proceedings, ICSP '04, 7th International Conference* pp. 873–876

Raval M S and Rege P P 2003 Discrete wavelet transform based multiple watermarking scheme. *TENCON, Conference on Convergent Technologies for Asia-Pacific Region* 3(1): 935–938

Zhang Xiao-Ping and Li Kan 2005 Comments on-An SVD-based watermarking scheme for protecting rightful ownership. *Multimed., IEEE Trans.* 7(3): 593–594

Zhou B and Chen J 2004 A geometric distortion resilient image watermarking algorithm based on SVD. *Chin. J. Image Graphics.* 9(1): 506–512