Block Based Blind & Secure Gray Image Watermarking Technique Based on Discrete Wavelet Transform and Singular Value Decomposition

Muhammad Imran and Bruce A. Harvey
Department of Electrical & Computer Engineering
College of Engineering, Florida State University
Tallahassee, FL 32310 - USA
[e-mail : iimran@fsu.edu]
*Corresponding author : Muhammad Imran

Received June 1, 2016; revised October 20, 2016; accepted December 8, 2016; published February 28, 2017

Abstract

In this paper block based blind secure gray image watermarking scheme based on discrete wavelet transform and singular value decomposition is proposed. In devising the proposed scheme, security is given high importance along with other two requirements: robustness and imperceptibility. The use of discrete wavelet transform not only improves robustness but the selection of bands with high tolerance towards noise caused an improvement in terms of imperceptibility. The robustness further improved due to the involvement of singular vectors along with singular values in watermark embedding and extraction process. Finally, to achieve security, the selected DWT band is decomposed into smaller blocks and random blocks are chosen for modification. Furthermore, the elements of left and right singular vectors of selected blocks are chosen based on their dependence upon each other for watermark embedding. Various experiments using different images as host and watermark were conducted to examine and validate the proposed technique. Additionally, the proposed technique is tested against various attacks like compression, affine transformation, cropping, translation, X shearing, scaling, Y shearing, filtering, blurring, different kinds of noises, histogram equalization, rotation, etc. Lastly, the proposed technique is compared with state-of-the-art watermarking techniques and their comparison shows significant improvement of proposed scheme over existing techniques.

Keywords: Digital Watermarking, security, copyright protection, data protection, singular value decomposition,

https://doi.org/10.3837/tiis.2017.02.014 **ISSN : 1976-7277**

1. Introduction

The innovation and accessibility of Internet across the globe has made life easy. For instance, enormous information in the form of digital data (images, audios, videos, pdfs, etc.) available on Internet, can easily be accessed and used from anywhere. Likewise, people acrross the world can share information (that may be senstive or confidential in some cases) via email or through clouding services like Dropbox™ or Google drive. However, this convenience of Internet has a major drawback. The data available online, once accessed and downloaded, can be redistributed after making its pirated copies. For end user both original and copied data look alike. This results in the form of copyright violation and causes enormous economic loss to various distributing industries each year [1]. To deal with copyright violation and claiming ownership, digital watermarking is proposed as prominent solution [1-8].

The process of embedding one type of data into another data is called watermarking. In case of images, it is known as image watermarking. Some sort of data (image, strings, etc.) called watermark is embedded into the image which is to be protected referred as host image, and the resulting image is called watermarked image. The embedded information can later be retrieved to use as ownership poof. A watermarking information is considered good if it meets at least three requirements: robustness, security and imperceptibility [1, 2, 9-13]. The performance of proposed scheme in terms of all mentioned requirements are examined and results are discussed in detail in Section 3.

Watermarking can be classified based on information required at the time of watermark extraction as non-blind (original image is required at watermark extraction stage) and blind (no need of original image to extract the hidden information) [8, 12, 14]. Blind watermarking is considered convenient and preferred over its counterpart [14]. Keeping this in view, the proposed scheme is designed to be blind in nature. Watermark can either be embedded directly into host image or into other domains after transforming host image into frequency domain using Discrete Cosine Transform (DCT) [5, 8, 15-16], Discrete Wavelet Transform (DWT) [3, 10, 17-19], or Discrete Fourier Transform (DFT) [7, 10, 12, 20]. The former type of watermarking is called spatial domain watermark – less complex, less robust and less secure, the latter type is known as transform domain watermarking – complex, robust and secure [17]. In transform domain watermarking, the host image is transformed into another domain, and then watermark is embedded. Afterwards, the watermarked image is obtained by applying inverse transformation. The transform domain watermarking is considered robust because during inverse transformation the concealed information is distributed in entire image; hence applying geometric attacks does not remove or destroy the hidden information and can later be extracted. Among other transforms, DWT is given importance due to its multi-resolution decomposition property. The proposed scheme has utilized DWT to transform the image from spatial to frequency domain.

Singular Value Decomposition (SVD) based watermarking schemes [3, 10, 17-18] are famous for robustness, especially against geometric attacks. This is due to i) changes in image do not cause noticeable alteration in singular values and vice versa and ii) luminance and geometric information of images is contained in singular values and vectors, respectfully [10], [17]. An SVD based watermarking technique presented in [21], where, singular values of host images are modified, and singular vectors remained undisturbed. The singular vectors of modified matrix (singular values of host image added with watermark) are utilized as keys and required at the time of watermark extraction. Later on, it is found that with fake keys (singular

vectors of another image), an entire different watermark can be extracted [22-23]. This flaw completely violates the purpose of watermarking that is to protect ownership. Anyone can extract watermark of their own choice and hence can claim ownership. In [24] an SVD based watermarking scheme was proposed, where, tiny genetic algorithm was exploited to find adaptive scaling factor for watermark embedding. However, [24] and [25] identified similar kind of flaws in [26] that were present in [21]. In [17], both DWT and SVD were utilized for watermark embedding and extraction. In [18], an attempt is made to meet the security lacks that were present in previous watermarking schemes. In [18], the watermark embedding process is same as of [17], except that all four bands LL, LH, HL, and HH are used, whereas, in [17] only LH and HL bands are utilized for watermark embedding. Moreover, an additional step is introduced in [18] for authentication of watermarking keys. The eight values for singular vectors (secret key) are modified and are checked at the time of watermark extraction to validate the security key.

The use of SVD in the field of image watermarking gives significantly good results in terms of robustness and imperceptibility but lacks in terms of security. Therefore, in the proposed watermarking technique it is investigated that how SVDs can be used without compromising security of watermarking scheme. The contribution in this paper is to achieve robustness, security and imperceptibility at the same time. For comparison, two state-of-the-art techniques [18] and [26] are chosen. The scheme [26] gives good results in terms of robustness and imperceptibility but unable to provide security, whereas, in [18] the lacks presents in [26] are tried to be improved. The experimental results shows that proposed scheme not only provides better robustness and imperceptivity than existing schemes [18, 26] but also proposes a more secure watermarking scheme. The proposed scheme is discussed in detail in following section.

2. Proposed Scheme

In the proposed watermarking technique, host image is decomposed into four bands (Approximation (LL), Horizontal (LH), Vertical (HL), and Diagonal (HH)) using DWT decomposition. The edge information remains unchanged in the process of watermark embedding by keeping the three bands (LH, HL and HH) intact as they contain edge information of original image [10-17]. The SVD is utilized to decompose the blocks of chosen band (LL). Both singular values and vectors of chosen band's blocks are involved in watermark embedding process to obtain good results in terms of robustness and capacity. Additionally, a special technique is opted to select the elements from the SVD matrices U, S and V based on correlation matrix of blocks of LL band. The method to find elements suitable for watermark embedding not only increases the security but also causes improvement in imperceptibility as suggested by results in Section 3.

The use of SVD in this paper has an important role in terms of achieving all the requirements: robustness, security and imperceptibility. Therefore, a few observations made regarding SVD are discussed in following sub-section.

2.1 Mathematical Background

Remark 1: Modifications made in left singular vectors of A causes less visible effects on modified A_w that was reconstructed using modified left singular vector of A.

In order to elaborate Remark 1, consider a matrix A of size 4×4, where $\{a_{ij} \in A | i \leq i \leq 4, 1 \leq j \leq 4\}$, is decomposed into U, V and S using SVD

$$A = USV^T$$

where

$$\left.\begin{matrix} U = [u_{ij}] \\ V = [v_{ij}] \\ S = [\lambda_{ij}] \end{matrix}\right\} \begin{matrix} i \le i \le 4, \ \ 1 \le j \le 4 \\ \lambda_{ij} = 0 \quad if \quad i \ne j. \end{matrix}$$

The columns of U and V are called left and right singular vectors of A respectively [27], whereas, S contains the singular values of A. Likewise, A can be recovered by combining the elements of U, V and S as shown below.

$$a_{ij} = \sum_{p=1}^{4}\sum_{q=1}^{4} u_{ip}\lambda_{pq}v_{jq} \qquad i \le i \le 4, 1 \le j \le 4 \tag{1}$$

Replacing first column of U with zero i.e. $\{u_{i1} = 0 | 1 \le i \le 4\}$, reduces (1) into (2), which is shown below.

$$a_{ij} = \sum_{p=2}^{4}\sum_{q=1}^{4} u_{ip}\lambda_{pq}v_{jq} \qquad i \le i \le 4, 1 \le j \le 4 \tag{2}$$

Whereas setting first row of U equal to zero i.e. $\{u_{1p} = 0 | 1 \le p \le 4\}$, will reduce (1) into (3) as shown below.

$$\begin{matrix} a_{1j} = 0 \\ a_{ij} = \sum_{p=2}^{4}\sum_{q=1}^{4} u_{ip}\lambda_{pq}v_{jq} \end{matrix} \quad 2 \le i \le 4, 1 \le j \le 4 \tag{3}$$

It can be seen from (2) that the impact of modifications made in first column of U is evenly distributed among all elements of A, consequently, the difference between original and modified A is visually imperceptible to human eye. Whereas from (3), it can be deduced that changing row of U makes corresponding row of A equal to zero, which is a substantial change and hence clearly perceivable by human eye. Keeping this in view it can be concluded that modifying columns of U has less visible impact on A as compared to changing rows of A. The same conclusion can be made for V as well.

Remark 2: It has been found in Remark 1 that changing column of U has less perceiveable impact on A as compared to changing row of U. Now, it is investigated that changes made in the elements of columns of U lasts or losts during reconstruction and decomposition of A_w.

Let U_w where $\{uw_{i1} \in U_w | 1 \le i \le 4\}$ represents modified version of U, obtained as a result of changing first column of U in such a way that following condition is satisfied.

$$uw_{11} \le uw_{21} \le uw_{31} \le uw_{41} \tag{4}$$

The modified matrix A_w where $\{aw_{ij} \in A_w | 1 \le i \le 4, 1 \le j \le 4\}$ is obtained from V, S and modified U_w.

$$aw_{ij} = uw_{i1}\lambda_{11}v_{j1} + \sum_{p=2}^{4}\sum_{q=2}^{4} u_{ip}\lambda_{pq}v_{jq} \qquad \begin{matrix} 1 \le i \le 4, 1 \le j \le 4 \\ \lambda_{ij} = 0 \qquad if \ i \ne j \end{matrix} \tag{5}$$

Again using SVD to decompose the altered A_w into $\hat{U}_w$, $\hat{S}$ and $\hat{V}$

$$A_w = \hat{U}_w\hat{S}\hat{V} \tag{6}$$

where,

$$aw_{ij} = \sum_{p=1}^{4}\sum_{q=1}^{4} \widehat{uw}_{ip}\hat{\lambda}_{pq}\hat{v}_{jq} \qquad 1 \le i \le 4, 1 \le j \le 4 \tag{7}$$

From (5) and (7), it can be seen that the left hand sides of both equations are equal, however, their constituents on right hand side are no longer same.

$$\widehat{uw}_{ij} \neq uw_{ij}, \qquad \hat{\lambda}_{ij} \neq \lambda_{ij}, \qquad \hat{v}_{ij} \neq v_{ij}$$

Consequently the relationship that was introduced among elements of first left singular vector shown in (4) may no longer holds true. This loss of information is due to the fact that the changes that were introduced in U are distributed among other elements of U, S and V during construction and decomposition of A_w. However, the relationship may continue to exist if same amount of change is introduced in corresponding elements of right singular vectors V as well.

The conclusion drawn above is further explained with help of an example. Let a matrix A be composed using SVD

$$A = USV^T \tag{8}$$

where,

$$A = \begin{bmatrix} 81 & 66 & 74 & 131 \\ 54 & 56 & 76 & 126 \\ 147 & 189 & 155 & 65 \\ 80 & 166 & 209 & 180 \end{bmatrix}, \quad U = \begin{bmatrix} -0.3549 & -0.3685 & 0.6353 & 0.5785 \\ -0.3205 & -0.4471 & 0.2786 & -0.7873 \\ -0.5666 & 0.7766 & 0.2463 & -0.1232 \\ -0.6711 & -0.2473 & -0.6769 & 0.1741 \end{bmatrix}$$

$$S = \begin{bmatrix} 488.329 & 0 & 0 & 0 \\ 0 & 120.808 & 0 & 0 \\ 0 & 0 & 61.7657 & 0 \\ 0 & 0 & 0 & 0.4347 \end{bmatrix}, V = \begin{bmatrix} -0.3748 & 0.3343 & 0.7861 & 0.3604 \\ -0.5321 & 0.4666 & -0.1342 & -0.6936 \\ -0.5707 & 0.0616 & -0.5685 & 0.5893 \\ -0.5007 & -0.8165 & 0.2023 & -0.2044 \end{bmatrix}$$

Using (9), the second and third elements of first column of U are modified according to the watermark bit. For instance if watermarking bit is 0 then condiction $u_{21} > u_{31}$ is set and for watermarking bit 1, the condition $u_{21} < u_{31}$ is set. At the time of watermark extraction these conditions are checked and watermarking bits are extracted accordingly. Keeping this in view, the values of U are modified.

$$\left.\begin{aligned} uw_{21} &= sgn(u_{21}) \times \left(\overline{U} - \frac{\gamma}{2}\right) = -0.4385 \\ uw_{31} &= sgn(u_{31}) \times \left(\overline{U} + \frac{\gamma}{2}\right) = -0.4485 \end{aligned}\right\} \begin{array}{c} Given\ that\ watermarking\ bit\ is\ zero \\ \gamma = 0.01 \end{array} \tag{9}$$

Here the condition $uw_{21} > uw_{31}$is introduced, which indicates that the embedding bit is 0. Now replace second $(u_{21})$and third (u_{31}) elements of first column of U with (uw_{21}) and (uw_{31}) respectively to obtain U_w.

The S, V and modified U_w are combined to form a modified version A_w of A as shown below.

$$A_w = U_w S V^T = \begin{bmatrix} 81 & 66 & 74 & 131 \\ 75.6049 & 86.6740 & 108.8982 & 154.8610 \\ 125.3951 & 158.3260 & 122.1018 & 36.1390 \\ 80 & 166 & 209 & 180 \end{bmatrix}$$

At receiver side the modified A_w is decomposed in order to check the relationship $uw_{21} > uw_{31}$ is still there or it is lost during construction of A_w and then its decomposition. Decompose A_w using SVD

$$A_w = \hat{U}_w \times \hat{S} \times \hat{V}^T$$

where,

$$\widehat{U}_w = \begin{bmatrix} -0.3635 & -0.3154 & 0.6341 & 0.6052 \\ -0.4491 & -0.3815 & 0.2772 & -0.7589 \\ -0.4471 & 0.8571 & 0.2438 & -0.0772 \\ -0.6828 & -0.1425 & -0.6795 & 0.2275 \end{bmatrix}, \hat{S} = \begin{bmatrix} 481.2392 & 0 & 0 & 0 \\ 0 & 119.4149 & 0 & 0 \\ 0 & 0 & 61.7652 & 0 \\ 0 & 0 & 0 & 0.4333 \end{bmatrix}$$

$$\hat{V} = \begin{bmatrix} -0.3618 & 0.3491 & 0.7857 & 0.3604 \\ -0.5134 & 0.4871 & -0.1347 & -0.6935 \\ -0.5675 & 0.0837 & -0.5688 & 0.5894 \\ -0.5324 & -0.7961 & 0.2023 & -0.2044 \end{bmatrix}$$

It can be seen that $uw_{21} \not> uw_{31}$, which indicates that the embedding bit was 1, whereas, in actual the embedding bit was 0. Moreover, $\widehat{U}_w$ is not same as U_w, $\widehat{S}$ is not same as S, and $\widehat{V}$ is not same as V. To avoid this loss of information that causes incorrect identification of watermarking bit, same amount of modification that is made between the elements of U, must be introduced between corresponding elements of V so that relationship introduced between elements of U persists. For instance, second and third elements of first row of V are modified as shown below.

$$\left.\begin{aligned} vw_{12} &= sgn(v_{12}) \times \left(\bar{V} - \frac{\gamma}{2}\right) = 0.5552 \\ vw_{13} &= sgn(v_{13}) \times \left(\bar{V} + \frac{\gamma}{2}\right) = 0.5652 \end{aligned}\right\} \begin{matrix} Given\ that\ watermarking\ bit\ is\ zero \\ \gamma = 0.01 \end{matrix} \quad (10)$$

Now U_w, S and V_w are combined to form modified matrix $A1_w$.

$$A1_w = U_w S V_w^T = \begin{bmatrix} 62.5018 & 66 & 74 & 131 \\ 59.8766 & 86.6740 & 108.8982 & 154.8610 \\ 142.7575 & 158.3260 & 122.1018 & 36.1390 \\ 82.6349 & 166 & 209 & 180 \end{bmatrix}$$

It can be seen from $A1_w$, that involving V in modification process does not alter A that much ($A1_w$ and A_w are same except first column of A, which is slightly different). Additionally, involving V helps in keeping the relationship between elements of U intact. Let $A1_w$ be decomposed using SVD

$$A1_w = \widehat{U}_w \times \hat{S} \times \hat{V}_w^T$$

where

$$\widehat{U}_w = \begin{bmatrix} -0.3500 & -0.3047 & 0.6462 & 0.6058 \\ -0.4382 & -0.3827 & 0.2934 & -0.7586 \\ -0.4616 & 0.8545 & 0.2253 & -0.0773 \\ -0.6873 & -0.1747 & -0.6675 & 0.2270 \end{bmatrix} \quad (11)$$

It can be seen that $uw_{21} > uw_{31}$, which indicates that the embedding bit was 0, and that is true. Hence, it can be concluded that involving V along with U in watermark embedding, process increases the robustness. It should be noted that the relationship information between elements of U is not always lost, however, involving V is an additional step to increase robustness.

Remark 3: The experimentatl results suggest improvement in terms of imperceptibility if elements chosen from U are based on the correlation matrix of A.

The imperceptible quality is improved if two elements from U chosen for watermark embedding are based on the correlation matrix of A. For instance if a_{23} and a_{13} are least correlated elements of A, where the subscripts are used to represent locations. Keeping their location in view, for better imperceptibility the elements u_{23} and u_{13} of U from same locations should be opted for modifications. This assumption can further be explained and

verified with the help of example. Consider 200 distinct matrix blocks A of sizes 4×4. Decompose A into U, S and V using SVD, and then modify two values of U for following cases. After modification, reconstruct A using modified U.
Case 1: Second and third elements from first column of U are chosen for modification using (9).
Case 2: The location of two least correlated elements from first column of A is used to select two elements of U from same location for modification using (9).
Case 3: Based on the location of two least correlated elements from least correlated column of A, two corresponding elements of U are selected for modification using (9).

The covariance matrix is calculated in order to find the correlation among elements of A. The PSNR for each block A for each of the above mentioned cases is calculated and plotted as shown in **Fig. 1**.

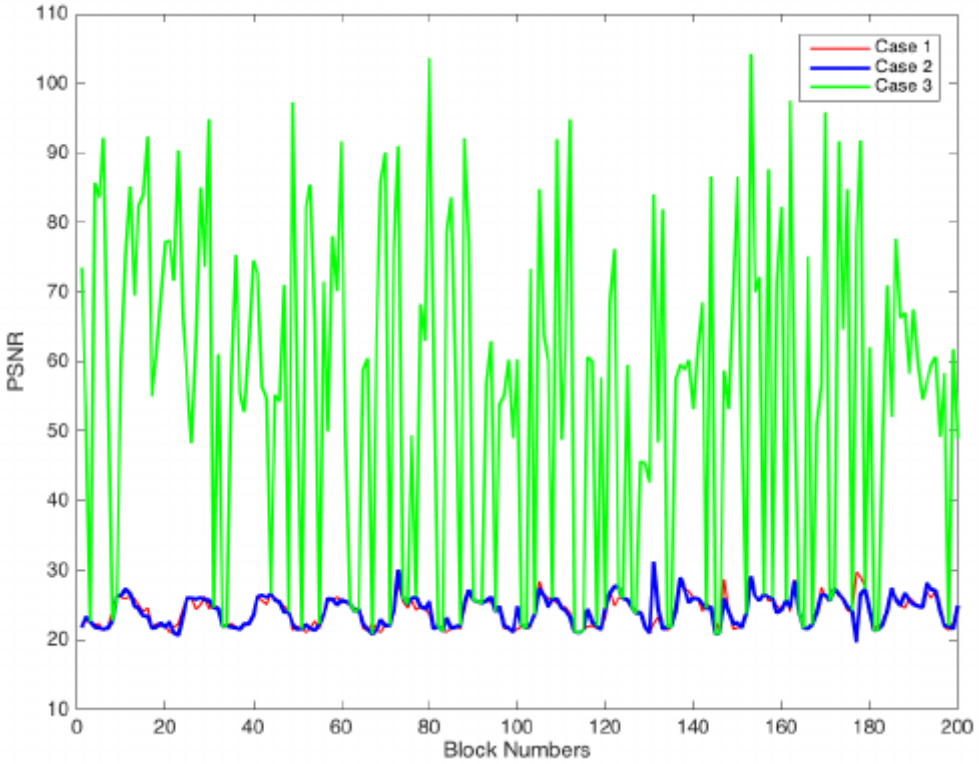


Fig. 1. PSNR for three different cases of 200 distinct blocks

From **Fig. 1**, it is clear that the PSNR for case 3 is larger than the rest in most cases. Therefore, in proposed scheme, Case 3 is adapted for watermark embedding.
In above remarks three points are made.

1. Modifying columns of U has less impact on A as compared to alteration made in rows U [28]. Likewise, introducing changes in rows of V has less adverse effects on A than changing columns of V
2. Involving both U and V in watermark embedding process increases robustness.
3. Elements from U are chosen based on the location of least correlated elements of A, have less visible effects on modified A_w.

Now keeping the points proved above in view, watermark embedding and extraction procedure are discussed in detail in following sections.

2.2 Watermark Embedding

1. Let one-level Haar DWT is used to decompose the cover image I of size $M \times N$ into four sub-bands (i.e. LL, LH, HL and HH).

$$(LL, LH, HL, HH) = DWT(I) \tag{12}$$

The use of DWT here is to improve imperceptibility and robustness [17]. Keeping edge information (LH, HL and HH) unchanged causes improvement in terms of imperceptibility, whereas, the irregular distribution of watermark over the image during inverse transform [29-30] provides good result in terms of robustness.

2. The LL band is decomposed into non-overlapping blocks A_s of size 4×4

$$LL = [A_s] \qquad 1 \le s \le (MN)/(8 \times 8) \tag{13}$$

where

$$\{a_{pq} \in A | 1 \le p \le 4, 1 \le q \le 4\}.$$

3. Let watermark W of size $m \times n$, where, $m \le \frac{M}{32}, n \le \frac{N}{32}$ is decomposed into 8-bit planes, consequently, $8 \times m \times n$ bits are formed.

4. Make a set $\mathcal{X}$ containing unique positive permuted integers such that $\mathcal{X}_x = \{x | x \in \mathbb{Z}^+ \wedge 1 \le x \le \frac{MN}{16}\}$. Select first $\mathcal{K}$ values, where, $\mathcal{K} = 8 \times m \times n$ from set $\mathcal{X}$, as shown below.

$$\boldsymbol{P} = \{\boldsymbol{\mathcal{X}}(1), \mathcal{X}(2), \cdots, \boldsymbol{\mathcal{X}}(\boldsymbol{\mathcal{K}})\}$$

To ensure security, random blocks based on set $\boldsymbol{P}$ are chosen for watermark embedding, and later at the time of watermark extraction, same set $\boldsymbol{P}$ serve as secret key.

5. Selected blocks are decomposed into U, S and V using SVD.

$$\left.\begin{aligned} U_z S_z V_z^T &= SVD(A_z) \\ \mathbb{C}_z &= \frac{1}{4 \times 4} A_z A_z^T \end{aligned}\right\} \; \mathrm{z} = \boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(\mathcal{K}) \tag{14}$$

where, $\mathbb{C}_z$ represents the correlation matrix.

6. For selected block, two least correlated number from a least correlated column are found based on covariance matrix $\mathbb{C}_z$. The position of least correlated elements is used to select two numbers from U for modifications. For instance, $\mathrm{Q}2(z)$ and $\mathrm{Q}3(z)$ represents the location of least correlated elements from a least correlated column number $\mathrm{Q}1(z)$ for block z, where, $z = \boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(\mathcal{K})$ and $\mathrm{Q}2(z) > \mathrm{Q}3(z)$. The locations are saved as secrete keys; $\mathbb{K}\mathrm{e}\mathrm{y} = \{\mathrm{Q}1(z), \mathrm{Q}2(z), \mathrm{Q}3(z)\}, where, z = \boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(\mathcal{K})$.

7. The locations of least correlated elements found in Step 6, are used to select elements from U, S and V (calculated in Step 5 using (14)) for modification based on watermarking bit.

$$\left.\begin{aligned} U_{wz}(\mathrm{Q2}(z),\mathrm{Q1}(z)) &= sgn\left(U_z(\mathrm{Q2}(z),\mathrm{Q1}(z))\right)\times\left(\bar{U}_z+\frac{\alpha}{2}\right)\\ U_{wz}(\mathrm{Q3}(z),\mathrm{Q1}(z)) &= sgn\left(U_z(\mathrm{Q3}(z),\mathrm{Q1}(z))\right)\times\left(\bar{U}_z-\frac{\alpha}{2}\right)\\ V_{wz}(\mathrm{Q1}(z),\mathrm{Q2}(z)) &= sgn\left(V_z(\mathrm{Q1}(z),\mathrm{Q2}(z))\right)\times\left(\bar{V}_z+\frac{0.01\alpha}{2}\right)\\ V_{wz}(\mathrm{Q1}(z),\mathrm{Q3}(z)) &= sgn\left(V_z(\mathrm{Q1}(z),\mathrm{Q3}(z))\right)\times\left(\bar{V}_z-\frac{0.01\alpha}{2}\right)\\ S_{wz}(\mathrm{Q2}(z),\mathrm{Q2}(z)) &= 2\times S_{wz}(\mathrm{Q3}(z),\mathrm{Q3}(z)) \end{aligned}\right\} \begin{matrix} WatermarkingBit=1\\ z=\boldsymbol{P}(1),\boldsymbol{P}(2),\dots,\boldsymbol{P}(\mathcal{K}) \end{matrix} \quad (15)$$

$$\left.\begin{aligned} U_{wz}(\mathrm{Q2}(z),\mathrm{Q1}(z)) &= sgn\left(U_z(\mathrm{Q2}(z),\mathrm{Q1}(z))\right)\times\left(\bar{U}_z-\frac{\alpha}{2}\right)\\ U_{wz}(\mathrm{Q3}(z),\mathrm{Q1}(z)) &= sgn\left(U_z(\mathrm{Q3}(z),\mathrm{Q1}(z))\right)\times\left(\bar{U}_z+\frac{\alpha}{2}\right)\\ V_{wz}(\mathrm{Q1}(z),\mathrm{Q2}(z)) &= sgn\left(V_z(\mathrm{Q1}(z),\mathrm{Q2}(z))\right)\times\left(\bar{V}_z-\frac{0.01\alpha}{2}\right)\\ V_{wz}(\mathrm{Q1}(z),\mathrm{Q3}(z)) &= sgn\left(V_z(\mathrm{Q1}(z),\mathrm{Q3}(z))\right)\times\left(\bar{V}_z+\frac{0.01\alpha}{2}\right)\\ S_{wz}(\mathrm{Q3}(z),\mathrm{Q3}(z)) &= 0.5\times S_{wz}(\mathrm{Q2}(z),\mathrm{Q2}(z)) \end{aligned}\right\} \begin{matrix} Watermarking\ Bit=0\\ z=\ \boldsymbol{P}(1),\boldsymbol{P}(2),\dots,\boldsymbol{P}(\mathcal{K}) \end{matrix} \quad (16)$$

where

$$sgn(y) = \begin{cases} -1 & if\ y<0\\ 0 & if\ y=0\\ 1 & if\ y>0 \end{cases} \quad and \quad \begin{cases} \bar{U}_z = \dfrac{\left|U_z(\mathrm{Q2}(z),\mathrm{Q1}(z))+U_z(\mathrm{Q3}(z),\mathrm{Q1}(z))\right|}{2}\\ \bar{V}_z = \dfrac{\left|V_z(\mathrm{Q1}(z),\mathrm{Q2}(z))+V_z(\mathrm{Q1}(z),\mathrm{Q3}(z))\right|}{2} \end{cases}$$

For watermarking bit 1, (15) is used, and for watermarking bit 0, (16) is utilized for modifications.

8. Once the singular values and vectors are modified based on watermarking information, the modified blocks are obtained as follows.

$$A_{wz} = U_{wz}S_{wz}V_{wz}^{T} \qquad z=\boldsymbol{P}(1),\boldsymbol{P}(2),\dots,\boldsymbol{P}(\mathcal{K}) \quad (17)$$

Where, 'w' is used to denote watermark addition and the α is a scaling factor control the amount of alternation in values depending on watermarking bit.

9. The modified and unmodified A_{wz} blocks are combined to form watermark added approximation band LL_w.

10. Finally, all bands are combined to get watermarked image.

$$I_w = IDWT(LL_w, LH, HL, HH) \quad (18)$$

2.3 Watermark Extraction

1. Let one-level Haar DWT is used to decompose the watermarked (possibly distorted) image $\hat{I}_w$ into four sub-bands (i.e. LL, LH, HL and HH).

$$\left(\widehat{LL}_w, \widehat{LH}, \widehat{HL}, \widehat{HH}\right) = DWT\left(\hat{I}_{\boldsymbol{w}}\right) \tag{19}$$

2. The $\widehat{LL}_w$ band is decomposed into non-overlapping blocks $\hat{A}_s$ of sizes 4×4.

$$\widehat{LL}_w = \left[\hat{A}_s\right]\} \qquad \begin{matrix} 1 \le s \le (MN)/(8 \times 8) \\ \{\hat{a}_{pq} \in \hat{A} | 1 \le p \le 4, 1 \le q \le 4\} \end{matrix} \tag{20}$$

3. The location of blocks which was saved as key $\boldsymbol{P}$ at Step 4 during watermark embedding process is used to find blocks in which watermark was embedded. The blocks based on key $\boldsymbol{P}$ are decomposed using SVD.

$$\hat{A}_{wz} = \hat{U}_{wz}\hat{S}_{wz}\hat{V}_{wz}^T \qquad z = \boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(\mathcal{K}) \tag{21}$$

4. Once all the watermark added blocks are decomposed, the $\mathbb{K}\mathbb{e}\mathbb{y} = \{\mathrm{Q}1(z), \mathrm{Q}2(z), \mathrm{Q}3(z)\}$ is used to extract the hidden data.

$$\xi = \begin{cases} 1 & if\ \hat{U}_{wz}\left(\mathrm{Q}2(z), \mathrm{Q}1(z)\right) \le \hat{U}_{wz}\left(\mathrm{Q}3(z), \mathrm{Q}1(z)\right) \\ 0 & otherwise \end{cases} \tag{22}$$

$$\zeta = \begin{cases} 1 & if\ \hat{V}_{wz}\left(\mathrm{Q}1(z), \mathrm{Q}2(z)\right) \le \hat{V}_{wz}\left(\mathrm{Q}1(z), \mathrm{Q}3(z)\right) \\ 0 & otherwise \end{cases} \tag{23}$$

$$\psi = \begin{cases} 1 & if\ \hat{S}_{wz}\left(\mathrm{Q}2(z), \mathrm{Q}2(z)\right) \le \hat{S}_{wz}\left(\mathrm{Q}3(z), \mathrm{Q}3(z)\right) \\ 0 & otherwise \end{cases} \tag{24}$$

Based on ξ, ζ and ψ, the watermarking bits are extracted as follows

$$\widehat{W}_z = \begin{cases} \psi & if \quad (\xi \equiv \psi) \vee (\zeta \equiv \psi) \\ \vartheta & otherwise \end{cases} \tag{25}$$

where, $\vartheta = Mode\{\xi, \psi, \zeta\}$.

5. After calculating total $8 \times m \times n$ bits, they are combined to form 8-bit planes. The final watermark is obtained by combining 8-bit planes.

3. Experimental Results and Analysis

In order to analyze the performance of proposed schemes, various experiments were performed. For this purpose four different images shown in **Fig. 2 (a)-(d)**, each of size 2048×2048, were used as host images. Whereas, two images of sizes 64×64, shown in **Fig. 3(p)** and **Fig. 4(p)**, were utilized as watermarks. The data bank [31] was used to acquire test images. The quality of proposed scheme is measured in terms of robustness, security and imperceptibility. The performance of proposed scheme in respect of above mentioned requirements are discussed in detail in following sections.

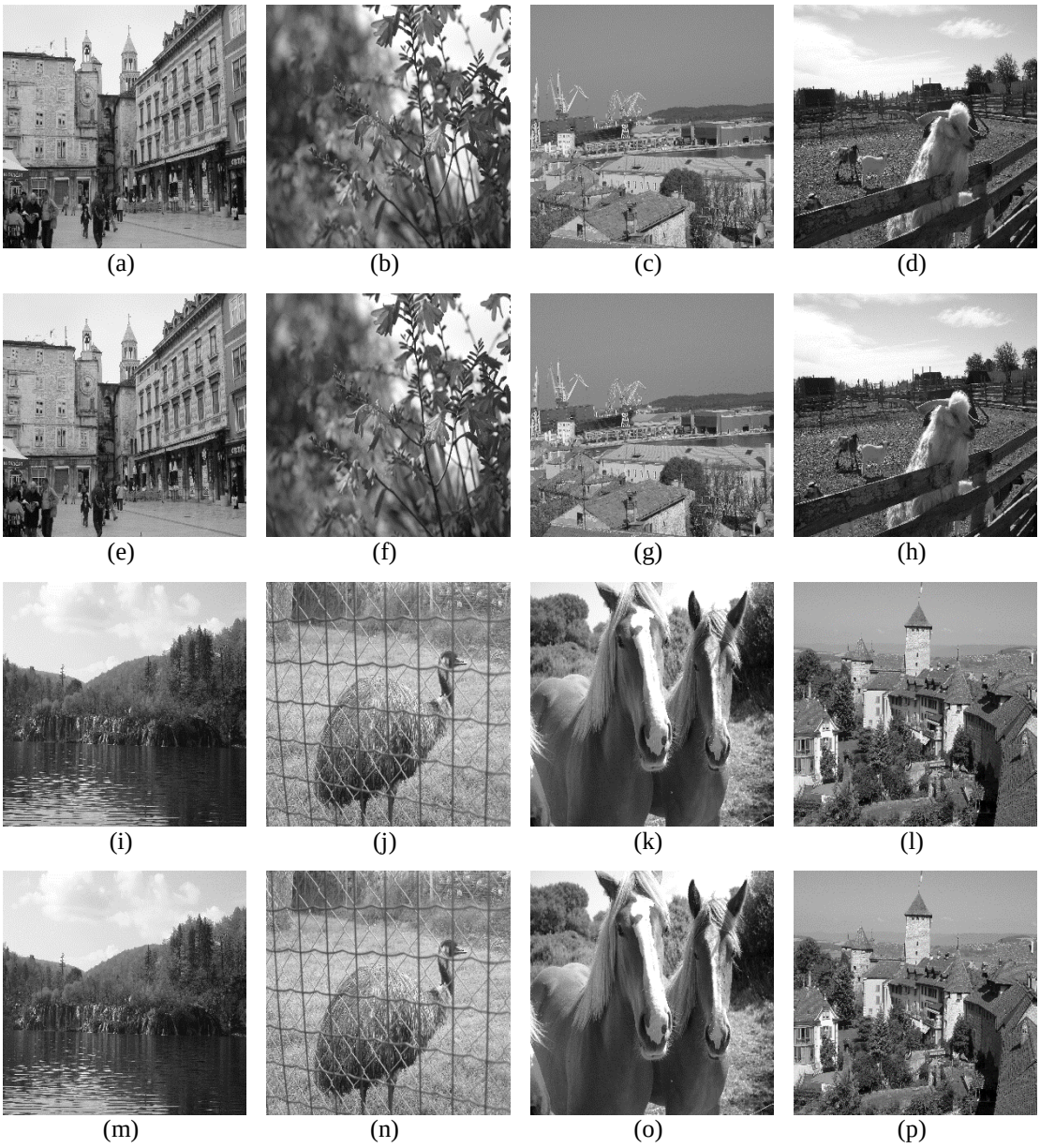


Fig. 2. Original and Watermarked Images (2048×2048): (a) Test Image 1 (b) Test Image 2 (c) Test Image 3 (d) Test Image 4 (e) Test Image 1 (Watermarked) (f) Test Image 2 (Watermarked) (g) Test Image 3 (Watermarked) (h) Test Image 4 (Watermarked) (i) Test Image 5 (j) Test Image 6 (k) Test Image 7 (l) Test Image 8 (m) Test Image 5 (Watermarked) (n) Test Image 6 (Watermarked) (o) Test Image 7 (Watermarked) (p) Test Image 8 (Watermarked)

3.1 Robustness

The capability of watermarking technique to resist attacks applied on watermarked images to destroy or remove the watermark is called robustness [4, 32]. It can either be measured quantitatively using normalized correlation (NC) [1, 4, 12] shown in (26), where, W and $\widehat{W}$ denotes embedded and extracted watermark respectively, or qualitatively by examining the

extracted watermarks. A watermarking scheme is considered good if the extracted watermarks either are easily recognizable or having higher NC values.

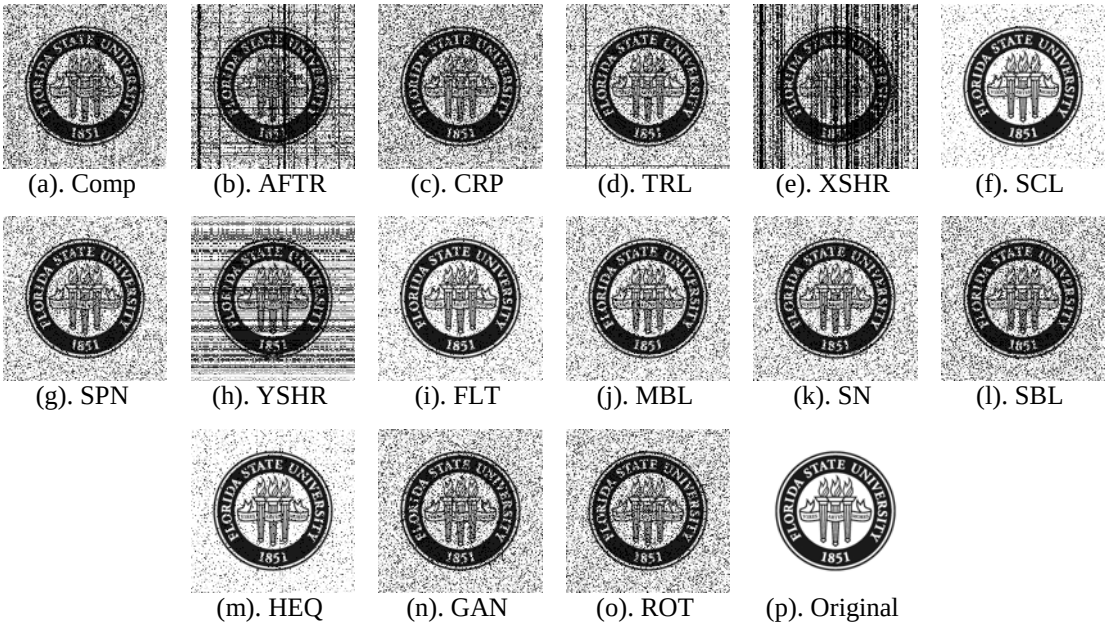


Fig. 3. Original and extracted watermarks 1 after applying different attacks on watermarked images

$$NC = \frac{\sum_{i=1}^{I}\sum_{j=1}^{J}\left(W(i,j)\times\widehat{W}(i,j)\right)}{\sqrt{\sum_{i=1}^{I}\sum_{j=1}^{J}W^{2}(i,j)}\times\sqrt{\sum_{i=1}^{I}\sum_{j=1}^{J}\widehat{W}^{2}(i,j)}} \tag{26}$$

Various attacks like -- compression (JPEG Comp), affine transformation (AFTR), cropping (CRP), translation (TRL), X shearing (XSHR), scaling (SCL), salt&pepper (SPN), Y shearing (YSHR), filtering (FLT), motion blurring (MBL), speckle noise (SN), simple blurring (SBL), histogram equalization (HEQ), Gaussian noise (GAN), rotation (ROT) -- were applied on watermarked images using different parameters. Afterwards watermarks taken out from attacked watermarked images were used to analyze the robustness of proposed watermarking technique. From, **Table 1**, showing NC values for extracted watermarks, it is clear that almost for all cases the NC values are reasonable.

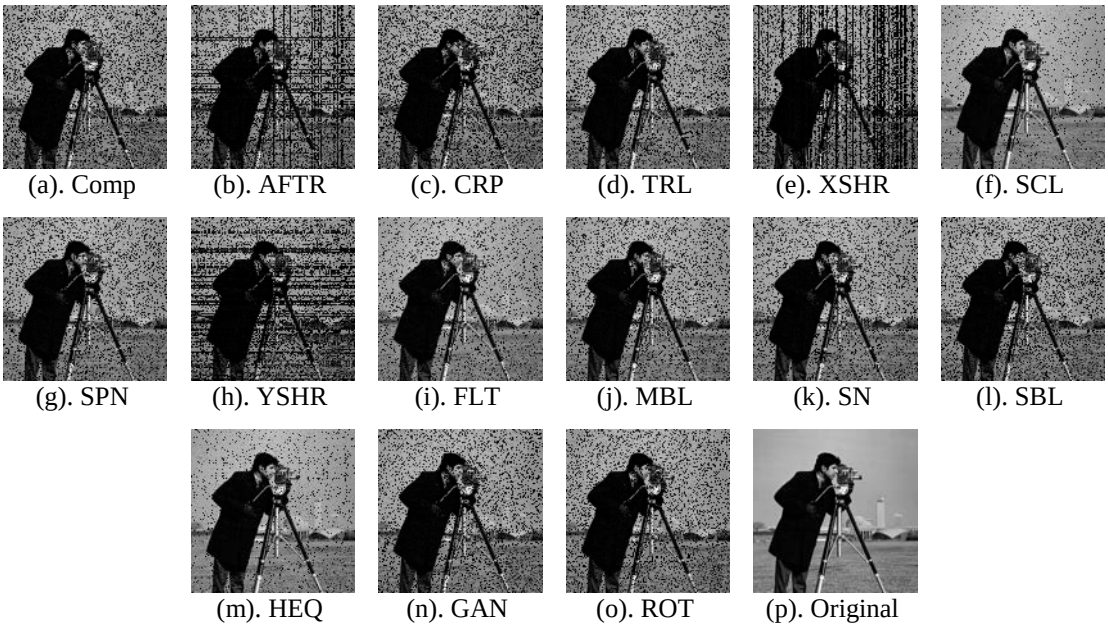
Table 1. NC for different attacks

Attacks		**Constant Scaling Factor (α)**				
Attack Type	**Attack's Parameter**	**0.01**	**0.03**	**0.05**	**0.07**	**0.09**
JPEG Comp	QF=50	0.9511	0.9513	0.9514	0.9516	0.9531
AFTR	Transforming Factor =0.1	0.9035	0.8887	0.8995	0.9069	0.8995
	Transforming Factor =0.3	0.7988	0.7855	0.8055	0.8058	0.7925
CRP (Centered)	10%	0.9427	0.9436	0.9431	0.9439	0.9427
	25%	0.9419	0.9430	0.9432	0.9436	0.9499
TRL	Right Side Shifting 60%	0.9485	0.9378	0.9395	0.9522	0.9502
	Left Side Shifting 120%	0.9421	0.9310	0.9264	0.9417	0.9363

Table 1. Continued...

Attacks		Constant Scaling Factor (α)				
Attack Type	**Attack's Parameter**	**0.01**	**0.03**	**0.05**	**0.07**	**0.09**
XSHR	Shearing Value = 0.4	0.8504	0.9396	0.8612	0.8572	0.8406
	Shearing Value = -0.5	0.8327	0.8230	0.8435	0.8395	0.8204
SCL	Scaling 2 times	0.9950	0.9951	0.9947	0.9944	0.9948
	Scaling 0.5 times	0.9824	0.9828	0.9835	0.9824	0.9837
SPN	Noise Density = 0.1	0.9570	0.9583	0.9603	0.9613	0.9619
	Noise Density = 0.5	0.9554	0.9565	0.9566	0.9575	0.9565
YSHR	Shearing Value = -0.4	0.8868	0.8802	0.8844	0.8857	0.8831
	Shearing Value = 0.5	0.8723	0.8640	0.8679	0.8696	0.8677
FLT (Average)	Window Size 5 × 5	0.9672	0.9712	0.9724	0.9739	0.9741
	Window Size 7× 7	0.9605	0.9603	0.9619	0.9625	0.9631
MBL		0.9614	0.9623	0.9627	0.9631	0.9641
SN	Noise Density = 0.1	0.9586	0.9588	0.9608	0.9620	0.9625
	Noise Density = 0.5	0.9562	0.9566	0.9580	0.9602	0.9604
SBL		0.9553	0.9546	0.9556	0.9545	0.9557
HEQ		0.9821	0.9810	0.9812	0.9815	0.9817
GAN	Mean = 0.4, Var = 0.01	0.9559	0.9578	0.9581	0.9589	0.9598
	Mean = 0.5, Var = 0.5	0.9554	0.9564	0.9570	0.9571	0.9580
ROT	Rotation Angle = 20°	0.8223	0.8520	0.8303	0.8240	0.8123
	Rotation Angle = 45°	0.7682	0.7487	0.7745	0.7615	0.7638
	Rotation Angle = 90°	0.9553	0.9550	0.9559	0.9563	0.9549

Additionally extracted watermarks showing in **Fig. 3** and **Fig. 4** are clearly recognizable and proving the good quality of proposed scheme in terms of robustness.



(a). Comp (b). AFTR (c). CRP (d). TRL (e). XSHR (f). SCL

(g). SPN (h). YSHR (i). FLT (j). MBL (k). SN (l). SBL

(m). HEQ (n). GAN (o). ROT (p). Original

Fig. 4. Original and extracted 2 watermarks after applying different attacks on watermarked images

The comparision of proposed technique with state-of-the-art watermarking schemes is shown in **Table 2**. The comparision shows clear improvement of proposed technique over existing schemes in respect of robustness.

Table 2. Comparision of different watermarking techniques in terms of NC

Attack Types	Constant Scaling Factor ($\alpha = 0.05$)		
	Proposed Technique	Technique Presented in [18]	Technique Presented in [26]
JPEG Comp	0.9514	0.8485	0.5624
AFTR	0.8995	0.8643	0.6329
CRP	0.9430	0.8757	0.6982
TRL	0.9395	0.8034	0.7045
XSHR	0.8612	0.8236	0.7586
SCL	0.9835	0.8534	0.7152
SPN	0.9566	0.8326	0.5369
YSHR	0.8844	0.8172	0.7429
FLT	0.9619	0.8304	0.5826
MBL	0.9627	0.7769	0.4985
SN	0.9580	0.8267	0.5528
SBL	0.9556	0.7442	0.5427
HEQ	0.9812	0.8437	0.5894
GAN	0.9581	0.8216	0.5328
ROT	0.8745	0.8035	0.6894

3.2 Security

The sole purpose of watermarking is to ensure copyright protection, which is possible if only intended user can take out the watermark, and the hidden information cannot be removed. The property of watermarking technique to endure such attacks, which are applied either to remove the watermark or to extract a false watermark, is called security [9]. To ensure security of proposed scheme, the location where watermark is added is kept private, so that no one can remove or extract the hidden information. In [26] a false watermark can be extracted with fake keys as proved by [24] and [25]. This completely destroys the purpose of watermarking; anyone can extract watermark of their choice and can claim ownership

Similarly, in [18] with different key, a different watermark can be extracted, however, in [18] a mechanism is introduced to authenticate the watermark extraction key. The key which is used to authenticate the watermark extraction key has length 8. The length of key plays an important role in security; lengthy key means more security [9]. In the proposed scheme, random blocks are selected for watermark embedding, and their position serves as key during watermark extraction. The length of key is subject to the size of watermark ($m \times n$). It means for a small size, like, 32×32 watermark, the length of key for proposed scheme is $8 \times 32 \times 32$. Which clearly indicates the difficulty level of proposed scheme is much greater than that of presented in [18]. Hence, the proposed scheme gives better results in terms of security as well.

Additionally, to validate the security of proposed scheme multiple random generated keys were applied to extract the watermark. In not a single case neither false or true watermark was extracted. However, for simplicity watermark extracted for 8 different fake keys are shown in **Fig. 5**. This also shows the security of proposed scheme.

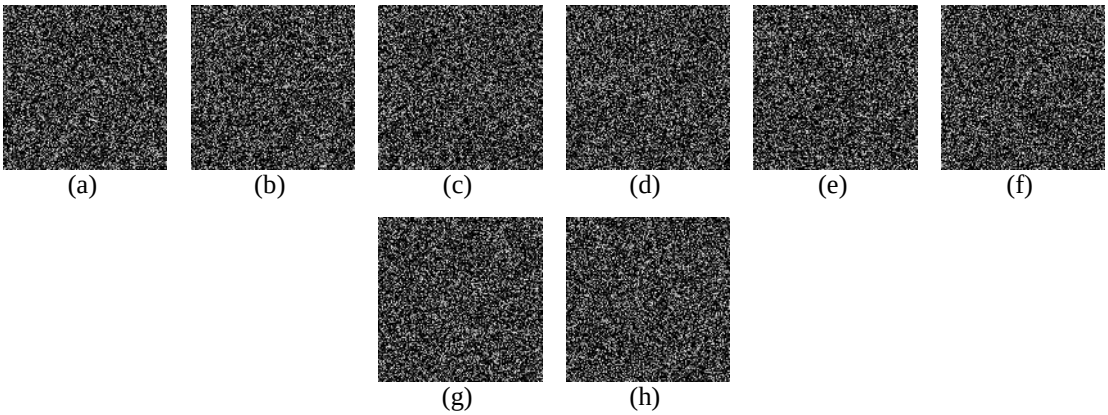


Fig. 5. Watermarks Extracted Using Fake Secrete Keys From Different Watermarked Images

3.3 Imperceptibility

One of the challenge in the field of watermarking is that despite of altering the host image for watermark embedding, watermarked and original host image should look identical to end user. This property is known as imperceptibility [2], [4], [10], and [17]. Like robustness, imperceptibility can be measured quantitatively using PSNR [19] shown in (27), where, I and I_w represent original and watermarked images, and qualitatively by examining the watermarked images.

$$PSNR = 10\log_{10}\left(\frac{\max_m \max_n I(m,n)}{\frac{1}{M \times N}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(I(m,n) - I_w(m,n)\right)^2}\right) \tag{27}$$

Table 3 showing the PSNR for different images for a range of scaling factors. The watermarked images shown in **Fig. 2(e)-(h)**, for scaling factor 0.05, looks almost same as those original images shown in **Fig. 2(a)-(d)**.

Table 3. PSNR of proposed scheme for different test images using different scaling factors

Test Images	Range of Constant Scaling Factor (α)				
	0.01	**0.03**	**0.05**	**0.07**	**0.09**
Image 1	45.8246	44.3390	42.4450	40.4450	39.0743
Image 2	51.9097	48.3317	45.5606	43.1498	41.3155
Image 3	45.7751	43.9280	41.9883	40.2355	38.8682
Image 4	43.1163	41.8139	40.4360	39.2225	38.0834
Image 5	44.2772	42.6467	41.4543	40.3351	39.1475
Image 6	45.7692	43.0170	40.6809	38.8317	37.1122
Image 7	51.1319	47.5126	44.8399	42.7063	41.0445
Image 8	45.0763	43.0695	41.2733	39.8484	38.5460

The comparision of proposed scheme with state-of-the-art techniques shown in **Table 4** indicates the out performance of proposed technique over existing techniques.

Table 4. Comparision of different watermarking techniques in terms of PSNR

Different Test Images ($\alpha = 0.05$)	**Watermark Techniques**		
	Proposed Technique	Technique Presented in	
		[18]	in [26]
Test Image 1	42.2658	39.9821	33.2508
Test Image 2	45.5606	40.2863	37.6810
Test Image 3	41.9883	38.9116	35.1126
Test Image 4	40.4360	37.6196	32.6812
Test Image 5	41.4543	39.7651	33.5108
Test Image 6	40.6809	36.9784	32.8759
Test Image 7	44.8399	39.7862	36.2109
Test Image 8	41.2733	38.0878	35.8703

4. Conclusion

In this paper, a blind and secure watermarking scheme based on DWT and SVD is proposed. In devising the proposed technique, special attention to security along with other requirements: robustness and imperceptibility. Involving only approximation band (LL) in watermark embedding process, and keeping other bands (LH, HL and HH) intact not only causes improvement in robustness but also imperceptibility is improved. Likewise, participation of singular values and vectors improves capacity and robustness. To achieve security, random blocks of LL band are selected and the elements within chosen blocks are opted for modification based on their independence. The location of elements are saved and serves as keys at the time of watermark extraction. The proposed scheme is tested against different attacks and compared with state-of-the-art watermarking schemes. The experimental results suggest improvement of proposed scheme over existing watering techniques.

References

[1] Huawei Tian, Yao Zhao, Rongrong Ni, Lunming Qin, Xuelong Li, "LDFT-based watermarking resilient to local de-synchronization attacks," *IEEE Transactions on Cybernetics*, vol. 43, no. 6, pp. 2190-2201, December, 2013. Article (CrossRef Link).

[2] Xinshan Zhu, Jie Ding, Honghui Dong, Kongfa Hu, "Normalized correlation-based quantization modulation for robust watermarking," *IEEE Transactions on Multimedia*, vol. 16, no. 7, pp. 1888-1904, November, 2014. Article (CrossRef Link).

[3] Nazeer Muhammad, Nargis Bibi, "Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain," *IET Image Processing*, vol. 9, no. 9, pp. 795-803, September, 2015. Article (CrossRef Link).

[4] Mehran Andalibi, Damon M. Chandler, "Digital image watermarking via adaptive logo texturization," *IEEE Transactions on Image Processing*, vol. 24, no. 12, pp. 5060-5073, December 2015. Article (CrossRef Link).

[5] Yasunori Ishikawa, Kazutake Uehira, Kazuhisa Yanaka, "Optimization of size of pixel blocks for orthogonal transform in optical watermarking technique," *IEEE Journal of Display Technology*, vol. 8, no. 9, pp. 505-510, September, 2012. Article (CrossRef Link).

[6] Sangita Zope-Chaudhari, Parvatham Venkatachalam, Krishna Mohan Buddhiraju, "Secure dissemination and protection of multi-spectral images using crypto-watermarking," *IEEE Journal*

of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 8, no. 11, pp. 5388-5394, November, 2015. Article (CrossRef Link).

[7] Beijing Chen, Gouenou Coatrieux, Gang Chen, Xingming Sun, Jean Louis Coatrieux, Huazhong Shu, "Full 4-d quaternion discrete Fourier transform based watermarking for color images," *Journal of Digital Signal Processing*, vol. 28, pp. 106-119, June, 2014. Article (CrossRef Link).

[8] Shabir Parah, Javaid Sheikh, Nazir Loan, Ghulam Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Journal of Digital Signal Processing*, vol. 53, pp. 11-24, June 2016. Article (CrossRef Link).

[9] Patrick Bas, Teddy Furon, "A New Measure of Watermarking Security: The Effective Key Length," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp.1306-1317, June 2013. Article (CrossRef Link).

[10] Nasrin M. Makbol, Bee Ee Khoo, Taha H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Processing*, vol. 10, no. 1, pp. 34-52, January, 2016. Article (CrossRef Link).

[11] Chuntao Wang, Jiangqun Ni, Jiwu Huang, "An informed watermarking scheme using hidden markov model in the wavelet domain," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 853-867, June, 2012. Article (CrossRef Link).

[12] Matthieu Urvoy, Dalila Goudia, Florent Autrusseau, "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1108-1119, May, 2014. Article (CrossRef Link).

[13] Jian Cao, Jiwu Huang, "Controllable secure watermarking technique for trade-o_ between robustness and security," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 821-826, April, 2012. Article (CrossRef Link).

[14] Yu-Hsun Lin, Ja-Ling Wu, "A digital blind watermarking for depth-image-based rendering 3d images," *IEEE Trans. on Broadcasting*, vol. 57, no. 2, pp. 602-611, June, 2011. Article (CrossRef Link).

[15] Shankar Parimi, A. SaiKrishna, N. Rajesh Kumar, N. R. Raajan, "An imperceptible watermarking technique for copyright content using discrete cosine transformation," in *Proc. of IEEE Int. Conf. on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1-5, March 19-20, 2015. Article (CrossRef Link).

[16] Veysel Aslantas, Saban Ozer, Serkan Ozturk, "A novel image watermarking method based on discrete cosine transform using genetic algorithm," in *Proc. of 17th IEEE Int. Conf. on Signal Processing and Communications Applications*, pp. 285-288, April 9-11, 2009. Article (CrossRef Link).

[17] Chih-Chin Lai, Cheng-Chih Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060-3063, November, 2010. Article (CrossRef Link).

[18] Nasrin M. Makbol, Bee Ee Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," *Journal of Digital Signal Processing*, vol. 33, pp. 134-147, October, 2014. Article (CrossRef Link).

[19] Yuan-Gen Wang, Guopu Zhu, Jiwu Huang, "An improved sample projection approach for image watermarking," Journal *of Digital Signal Processing*, vol. 24, pp. 135-143, January, 2014. Article (CrossRef Link).

[20] Tsz Kin Tsui, Xiao-Ping Zhang, Dimitrios Androutsos, "Color image watermarking using multidimensional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16-28, March 2008. Article (CrossRef Link).

[21] Ruizhen Liu, Tieniu Tan, "An SVD based watermarking scheme for protecting rightful ownership," *IEEE Trans. on Multimedia*, vol. 4, no. 1, pp. 121-128, March, 2002. Article (CrossRef Link).

[22] Xiao-Ping Zhang, Kan Li, "Comments on 'An SVD based watermarking scheme for protecting rightful ownership'," *IEEE Trans. on Multimedia*, vol. 5, no. 2, pp. 593-594, June, 2005. Article (CrossRef Link).

[23] Roman Rykaczewski, "Comments on 'An SVD-based watermarking scheme for protecting rightful ownership'," *IEEE Trans. Multimedia*, vol. 9, no. 2, pp. 421-423, February, 2007. Article (CrossRef Link).
[24] Khaled Loukhaoukha, "Comments on 'A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm'," *Journal of Digital Signal Processing*, vol. 23, no. 4, pp. 1334, July, 2013. Article (CrossRef Link).
[25] Erkan Yavuz, Ziya Telatarb, "Comments on 'A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm'," *Journal of Digital Signal Processing*, vol. 23, no. 4, pp. 1335-1336, July, 2013. Article (CrossRef Link).
[26] Chih-Chin Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Journal of Digital Signal Processing*, vol. 21, no. 4, pp. 522-527, January, 2011. Article (CrossRef Link).
[27] Mohamed Neji Maatouk, Najoua Essoukri Ben Amara, "Intelligent hybrid watermarking ancient-document wavelet packet decomposition-singular value decomposition-based schema," *IET Image Processing*, vol. 8, no. 12, pp. 708-717, December 2014. Article (CrossRef Link).
[28] Qingtang Su, Yugang Niu, Hailin Zou, Xianxi Liu, "A blind dual color image watermarking based on singular value decomposition," *Journal of Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8455-8466, April, 2013. Article (CrossRef Link).
[29] Kamran Hameed, Adeel Mumtaz, S.A.M. Gilani, "Digital image watermarking in the wavelet transform domain," *World Academy of Science, Engineering and Technology*, vol. 13, pp. 86-89, 2006. Article (CrossRef Link).
[30] Santa Agreste, Guido Andaloro, Daniela Prestipino, Luigia Puccio, "An image adaptive, wavelet-based watermarking of digital images," *Journal of Computational and Applied Mathematics*, vol. 210, no. 1-2, pp. 13-21, December, 2007. Article (CrossRef Link).
[31] Hervé Jégou, Matthijs Douze, Cordelia Schmid, "Hamming embedding and weak geometric consistency for large scale image search," *A. Z. David Forsyth*, Philip Torr (Ed.), in *Proc. of European Conference on Computer Vision*, vol. I of LNCS, Springer, pp. 304-317, 2008. Article (CrossRef Link).
[32] Saman Iftikhar, M. Kamran, Zahid Anwar, "Rrw - a robust and reversible watermarking technique for relational data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 4, pp. 1132-1145, April, 2015. Article (CrossRef Link).

Muhammad Imran received the B.Eng. degree in electronic engineering from Mehran University of Engineering and Technology (MUET), Jamshoro, Pakistan, in 2007 and the M. Sci. degree in electrical engineering from National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2012. He is currently pursuing the PhD degree in electrical engineering at the Florida State University. He is a research assistant in Image Processing and Communication Research Laboratory. His research interests are in digital image processing, digital image watermarking and steganography.

Bruce A. Harvey received the B.E.E. (Co-op, Highest Honor) from Auburn University in 1984, the M.S.E.E. from the University of Alabama in Huntsville in 1987 and the Ph.D. in Electrical Engineering from Georgia Institute of Technology in 1991. He was a Research Engineer I at the Georgia Tech Research Institute (GTRI) from 1984-1986 and a Lead Engineer at Phase IV Systems, Inc. from 1986- 1988. From 1991-1997 he was a Research Engineer in the Communications Division of GTRI. In 1997 he joined the Department of Electrical and Computer Engineering at the FAMU-FSU College of Engineering in Tallahassee, Florida, and currently holds the rank of Associate Professor. His current fields of interest include lightning surge suppression, wireless communication, error control coding, wireless networks, modulation techniques, digital image processing, digital image watermarking, and modeling and analysis. Dr. Harvey is a member of the IEEE Communications and Edu- cation Societies.