A Novel Secure and Robust Image Watermarking Method Based on Decorrelation of Channels, Singular Vectors, and Values

Muhammad IMRAN, Bruce A. HARVEY
Department of Computer & Electrical Engineering, College of Engineering
Florida State University, Tallahassee, Florida, USA
iimran@fsu.edu

***Abstract*—A novel secure and robust image watermarking technique for color images is presented in this paper. Besides robustness and imperceptibility (which are the most important requisites of any watermarking scheme), there are two other challenges a good watermarking scheme must meet: security and capacity. Therefore, in devising the presented scheme, special consideration is also given to above-mentioned requirements. In order to do so, principal component analysis is involved to enhance imperceptibility and the unique utilization of singular value decomposition is done to achieve better performance in regard to capacity and robustness. Finally, a novel method is proposed to select constituents of an image for watermark embedding, which further improves the security. As a consequence, four essential requisites of a good watermarking scheme are achieved as visible from experimental results. To measure the behavior of presented watermarking scheme, a number of experiments were conducted by utilizing several color images as host images and as watermarks. The presented technique is compared with the latest available watermarking techniques and attained better results than them.**

***Index Terms*—authentication, data security, image decomposition, image forensic, watermarking.**

I. INTRODUCTION

The information available online as digital books, photos, videos, audios, etc. can easily be accessed from across the globe. A vast number of pirated copies of such information once accessed and downloaded can be made. This pirated data can then be redistributed either freely or at very low cost. Additionally, for an end user, the original and pirated data look alike. As a result, the economy suffers and the industries must bear loss every year [1]. To cater these problems, watermarking is suggested as a prominent solution [2—5].

Watermarking is simply a process of concealing some sort of data (watermark) into either of the same kind or of different type data (host) [3]. In case if host data is an image then watermarking is said to be image watermarking and the image obtained because of watermark embedding is called watermarked-image. A good watermarking technique must full fill four essential conditions; capacity, robustness, imperceptibility, and security, simultaneously [2, 6, 7]. Whenever an image is added with watermark, its perceptual quality degrades (known as imperceptibility [8]), and keeping the quality intact is a challenge in the field of watermarking. Furthermore, watermarking techniques for color images [2, 4—6] must meet one additional challenge as compared to their counterparts [7]. That challenge is that the three-color channels, Red (R), Green (G) and Blue (B), are extremely depended on each other [9]. Modifying any one of them has adverse effects on other two channels, which in turn destroy the quality of original image. However, this dependency can be avoided if the three channels are decorrelated. To do so, different approaches were proposed. Such as YIQ color model [5], YC_bC_r color model [9] were used to decorrelate these dependent color channels. In contrast, few researchers tried to embed a watermark in original color channels (R, G, and B), without going to any other color-model. For example, in [4], modified RGB channels were used and a very bad perceptual quality of watermarked-image resulted. On the other hand, the presented watermarking technique utilized Principal Component Analysis (PCA) to decorrelate these three dependent channels, and attained improved imperceptibility as compared to [4] and [5], as evident from results in Section V.

Getting a perceptually good watermarked-image is a challenge, but once achieved, watermarking may be subjected to other challenges, like, to destroy or to remove the watermark, the watermarked-image may be attacked. Therefore, the watermarking scheme must be designed in such a way that despite being attacked, the watermark should be extractable and recognizable so that it can be used to prove ownership. This property is called robustness of watermarking scheme [7]. In the presented technique, Singular Value Decomposition (SVD) is used to get satisfactory results of robustness. There are certain properties of SVD which make their use in image watermarking schemes ideal [5, 10—12]. For instance, alteration in singular values does not affect the original image significantly and same is true otherwise [7]. Additionally, singular values and vectors possess luminance and geometric information respectively [8].

Though using SVDs gives satisfactory results in respect of robustness, but it is inefficient to provide security (the property of a watermarking scheme to nullify the chances of watermark extraction completely, is referred as security [2, 7]). For instance, in 2002, a spatial watermarking scheme [10] was proposed. In [10], the singular values of an original image are modified to embed watermark, without modifying the singular vectors. The singular vectors were saved as security key and utilized when watermark was to be extracted. Later, it is found that using entirely different

Digital Object Identifier 10.4316/AECE.2017.04013

1582-7445 © 2017 AECE

singular vectors can lead to the extraction of a watermark, that was not even embedded [13, 14]. That means unauthorized users with their choice of singular vectors can extract watermark of their own, and in turn, they can claim ownership. As a result, the main objective of any watermarking scheme (ensuring copyright protection) is completely ruined. An advanced version of [10] was presented in 2010, utilizing Discrete Wavelet Transform (DWT) in addition to SVD [11]. Nevertheless, the flaw that was with scheme [10] was also present in [11]. A slightly modified technique [15], was also vulnerable to these kinds of flaws [13,16]. In [4], a different approach is adapted to cater above-mentioned flaw. For that purpose, instead of singular values, first and second values of singular vectors were chosen for watermark embedding. Although, this scheme somehow was successful against that flaw, but unable to provide security. As the locations of watermarking bits are known, anyone can extract and therefore destroy the watermark. To meet all these challenges, in the presented technique, to reject the false positive extraction of watermark both right and left singular vectors are employed in watermark embedding procedure, which in turn, improved the robustness. For the detailed explanation, Appendix A can be referred. Furthermore, security is ensured by opting elements with least correlation with each other to embed the watermark. While keeping the location of those elements secret and needed when the watermark is to be extracted. Thereby, ensuring the security, which is also evident from results. The last requisite is capacity (the information a host image can conceal without being degraded in quality). Involving right and left singular vectors enhanced the capacity of the presented technique, which can also be seen from results in Section V. The presented technique is analyzed in following sections.

II. PROPOSED TECHNIQUE

In the presented watermarking scheme, the three mutually dependent channels of a color image are first decorrelated, so that alteration in any one of them has no adverse effects on others. Hence, the perceptual quality of watermarked-image is improved drastically. The advantage of decorrelation of color channels resulted in terms of extremely improved imperceptibility, especially over [5]. (based on YIQ color model) and over [4]. In [4], values of left singular vectors are changed without changing singular values or right singular vectors. The data embedded in left singular vectors are distributed among singular values and right singular vectors, during the reconstruction of the image. Which results in the form of information loss when again SVD is used to obtain singular vectors and values. This phenomenon is discussed in detail in Appendix A. To overcome this challenge of loss of information along with other requirements mentioned-above, not only left but right singular vectors are employed in a unique and novel way (mentioned in Section III), to ensure that no significant information is lost and the correct watermark is extracted. Additionally, in [4], the location where the watermark is embedded is known, which means anyone can extract and hence destroy the watermark. To meet this challenge a novel approach (see Appendix A) is adapted to select elements for watermark embedding and the location is kept confidential and needed when watermark needs to be extracted. Consequently, security is ensured, and it is evident from results. This novel procedure of elements selection provides better results in respect of imperceptibility and robustness, that can further be ensured from results in Section V. Involving right and left singular vectors in the novel way is presented in this paper also doubles the capacity than those techniques proposed in [4] and [5]. The detailed explanation of embedding and extraction of the watermark is discussed in subsequent sections.

III. WATERMARK EMBEDDING

1. The watermark $(W_{m\times n})$ is decomposed into its constituents, as shown below

$$\left.\begin{array}{l} W_r = [r_W(i,j)] \\ W_g = [g_W(i,j)] \\ W_b = [b_W(i,j)] \end{array}\right\} \quad 1 \le (i,j) \le m,n. \tag{1}$$

2. Host image $(I_{M\times N})$, such that $M \ge 16\times m$ and $N \ge 16 \times n$, is broken down into its constituents, where,

$$\left.\begin{array}{l} I_r = r(i,j) \\ I_g = g(i,j) \\ I_b = b(i,j) \end{array}\right\} \quad 1 \le (i,j) \le M,N. \tag{2}$$

3. The covariance matrix $\mathbb{C}$ is computed as follows for a given matrix $\mathbb{B}$,

$$\mathbb{C} = \frac{1}{MN}\left(\mathbb{B}\mathbb{B}^T\right) = Q\Lambda Q^{-1}, \tag{3}$$

where,

$$\mathbb{B} = \begin{bmatrix} r_{1,1} & \cdots & r_{1,N} & r_{2,1} & \cdots & r_{2,N} & \cdots & r_{M,1} & \cdots & r_{M,N} \\ g_{1,1} & \cdots & g_{1,N} & g_{2,1} & \cdots & g_{2,N} & \cdots & g_{M,1} & \cdots & g_{M,N} \\ b_{1,1} & \cdots & b_{1,N} & b_{2,1} & \cdots & b_{2,N} & \cdots & b_{M,1} & \cdots & b_{M,N} \end{bmatrix},$$

$$Q = [q_{i,j}]_{\substack{1\le i\le m3 \\ 1\le i\le m3}},$$

$$\Lambda = \begin{cases} \lambda_{i,j} & when\ i=j \\ 0 & otherwise \end{cases} \quad 1 \le (i,j) \le 3.$$

4. The covariance matrix $\mathbb{C}$ is decomposed into three principal components using PCA [17] as shown below

$$\delta = \begin{bmatrix} \delta_r \\ \delta_g \\ \delta_b \end{bmatrix} = Q^T \mathbb{B} =$$

$$\begin{bmatrix} \delta r_{1,1} & \cdots & \delta_{1,N} & \delta r_{2,1} & \cdots & \delta r_{2,N} & \cdots & \delta r_{M,1} & \cdots & \delta r_{M,N} \\ \delta g_{1,1} & \cdots & \delta g_{1,N} & \delta g_{2,1} & \cdots & \delta g_{2,N} & \cdots & \delta g_{M,1} & \cdots & \delta g_{M,N} \\ \delta b_{1,1} & \cdots & \delta b_{1,N} & \delta b_{2,1} & \cdots & \delta b_{2,N} & \cdots & \delta b_{M,1} & \cdots & \delta b_{M,N} \end{bmatrix}.$$

Comment 1: Altering one color channel causes degradation in other two-color channels, and as a result when three channels are combined the quality of the original image is ruined [18]. It indicated that three color channels are extremely corelated and hence if un-correlated properly, this flaw can be overcome [19].

5. The matrices δ_{rn}, δ_{gn} and δ_{bn} are obtained from δ_r, δ_g, and δ_b respectively, as shown below

$$\left.\begin{aligned}\delta_{rn} &= [\delta_r(i,j)]\\ \delta_{gn} &= [\delta_g(i,j)]\\ \delta_{bn} &= [\delta_b(i,j)]\end{aligned}\right\}\quad \begin{aligned}1 \le i \le m\\ 1 \le j \le n\end{aligned}. \tag{4}$$

Since δ_{rn}, δ_{gn} and δ_{bn} are un-correlated representations of the three-color channels, and therefore, modifying any one of them for watermark embedding will not cause any other channel to suffer. As a consequence, the quality of the watermarked image will not be ruined.

6. Let W_r is broken down into 8-bit planes BP_0, BP_1, $\cdots$, BP_7, where BP_0 carries least information and BP_7 possesses most information [20]. As a consequence, $8 \times m \times n$ bits are created, where, m and n denote the dimensions of W_r.
7. Distinct blocks, $\mathbb{A}_b$ where, $b \in [1, MN/16]$ of sizes 4×4 are created by dividing δ_{rn}.
8. One-half that is $(MN/32)$ blocks of total created blocks $(MN/16)$ are randomly selected, and their locations are saved as secret keys Z_e and needed when the watermark is to be extracted. Afterwards, chosen blocks are broken down into singular vectors and values as shown below
$$\mathbb{A}_k = U_k S_k V_k^T,\ \ k = Z_e(1), Z_e(1), \cdots, Z_e\left(\frac{MN}{32}\right). \tag{5}$$
9. For each block $\mathbb{A}_k$ two least co-related values are found for watermark embedding. The locations of those values are again saved as keys and used when watermark needs to be extracted. For example, $Z_h(k)$ and $Z_q(k)$ denote the location of two least co-related element, from least correlated column $Z_r(k)$, chosen from block 'k', where, $k \in [1, MN/32]$ It should be ensured that $Z_h(k) > Z_q(k)$.
10. Using the location of least-correlated elements found in Step 9, the values at same locations from U_k, S_k, and V_k^T (computed in Step 8) are opted for watermark-embedding. The watermark bits are embedded in the chosen values according to the way defined below.
Case 1: For watermark-embedding bit 1. $(W_k = 1)$
$$U_{wk}(Z_q(k), Z_h(k)) = \operatorname{sgn}\{U_k(Z_h(k), Z_h(k))\} \times \left(\overline{U}_k + \gamma/2\right),$$
$$U_{wk}(Z_r(k), Z_h(k)) = \operatorname{sgn}\{U_k(Z_r(k), Z_h(k))\} \times \left(\overline{U}_k - \gamma/2\right),$$
$$V_{wk}(Z_h(k), Z_q(k)) = \operatorname{sgn}\{V_k(Z_h(k), Z_q(k))\} \times \left(\overline{V}_k + \gamma/2\right),$$
$$V_{wk}(Z_h(k), Z_r(k)) = \operatorname{sgn}\{V_k(Z_h(k), Z_r(k))\} \times \left(\overline{V}_k - \gamma/2\right),$$
$$\lambda_{wk}(Z_q(k), Z_q(k)) = \{2\lambda_k(Z_h(k), Z_h(k))\}.$$
Case 2: For watermark-embedding bit is 0 $(W_k = 0)$
$$U_{wk}(Z_q(k), Z_h(k)) = \operatorname{sgn}\{U_t(Z_h(k), Z_h(k))\} \times \left(\overline{U}_k + \gamma/2\right),$$
$$U_{wk}(Z_r(k), Z_h(k)) = \operatorname{sgn}\{U_t(Z_r(k), Z_h(k))\} \times \left(\overline{U}_k - \gamma/2\right),$$
$$V_{wk}(Z_h(k), Z_q(k)) = \operatorname{sgn}\{v_t(Z_h(k), Z_q(k))\} \times \left(\overline{V}_k + \gamma/2\right),$$
$$V_{wk}(Z_h(k), Z_r(k)) = \operatorname{sgn}\{V_t(Z_h(k), Z_r(k))\} \times \left(\overline{V}_k - \gamma/2\right),$$
$$\lambda_{wk}(Z_q(k), Z_q(k)) = \{2\lambda_k(Z_h(k), Z_h(k))\},$$
where,
$$\overline{U}_k = \frac{\left|U_k(Z_q(k), Z_h(k)) + U_k(Z_r(k), Z_h(k))\right|}{2},$$
$$\overline{V}_k = \frac{\left|V_k(Z_h(k), Z_q(k)) + V_k(Z_h(k), Z_r(k))\right|}{2}.$$
Where γ defines the amount of change that can be introduced without degrading the quality of the watermarked image, and w represents the addition of the watermark.
The least-correlated elements are chosen for watermark embedding to improve imperceptibility and that is enhanced extremely as evident from results in Section V. Furthermore, to ensure security random blocks were chosen and again least-correlated elements form those random blocks are selected for watermark embedding. The location of those random blocks and the location of those least-correlated elements are saved as secret keys. This novel approach indeed improved security drastically, which is experimentally demonstrated in results' section. In the end, right singular vectors (V^T) and left singular vectors (U) are opted for modification, to boost robustness and capacity. The detailed explanation is given in Appendix A and verified from experimental results as well.
11. The watermark added singular vectors and values are used to reconstruct respective blocks,
$$\mathbb{A}_{wk} = U_{wk} S_{wk} V_{wk}^T,\ \ k = Z_e(1), Z_e(1), \cdots, Z_e\left(\frac{MN}{32}\right). \tag{6}$$
12. The watermark-added blocks and unchanged blocks are used to construct the watermark-added first principal component δ_{rnw}, where,
$$\delta_{rnw} = [\delta_{rw}(i,j)] \qquad 1 \le (i,j) \le M, N.$$
13. To embed W_g and W_b into δ_{gn} and δ_{bn} respectively, follow Step-6 through Step-12. Simply replace W_r with W_g, δ_{rn} with δ_{gn}, W_r with W_b, and δ_{rn} with δ_{bn} from Step-6 to Step-12. As a consequence, watermark-added principal components δ_{gnw} and δ_{bnw} are created, where,
$$\begin{aligned}\delta_{gnw} &= [\delta_{gw}(i,j)]\\ \delta_{bnw} &= [\delta_{bw}(i,j)]\end{aligned} \qquad 1 \le (i,j) \le M, N. \tag{7}$$
14. The δ_w is obtained by combing all three watermark-added principal components; δ_{rnw}, δ_{gnw}, and δ_{bnw}.
$$\delta_w = \begin{bmatrix}\delta_{rw}\\ \delta_{gw}\\ \delta_{bw}\end{bmatrix} =$$

$$\begin{bmatrix} \delta rw_{1,1} & \cdots & \delta rw_{1,N} & \delta rw_{2,1} & \cdots & \delta rw_{2,N} & \cdots & \delta rw_{M,1} & \cdots & \delta rw_{M,N} \\ \delta gw_{1,1} & \cdots & \delta gw_{1,N} & \delta gw_{2,1} & \cdots & \delta gw_{2,N} & \cdots & \delta gw_{M,1} & \cdots & \delta gw_{M,N} \\ \delta bw_{1,1} & \cdots & \delta bw_{1,N} & \delta bw_{2,1} & \cdots & \delta bw_{2,N} & \cdots & \delta bw_{M,1} & \cdots & \delta bw_{M,N} \end{bmatrix},$$

where, δ_{rw}, δ_{gw} and δ_{bw} are obtained from δ_{rnw}, δ_{gnw} and δ_{bnw} respectively.

15. The matrix is obtained as

$$\mathbb{B}_w = Q\delta_w =$$

$$\begin{bmatrix} rw_{1,1} & \cdots & rw_{1,N} & rw_{2,1} & \cdots & rw_{2,N} & \cdots & rw_{M,1} & \cdots & rw_{M,N} \\ gw_{1,1} & \cdots & gw_{1,N} & gw_{2,1} & \cdots & gw_{2,N} & \cdots & gw_{M,1} & \cdots & gw_{M,N} \\ bw_{1,1} & \cdots & bw_{1,N} & bw_{2,1} & \cdots & bw_{2,N} & \cdots & bw_{M,1} & \cdots & bw_{M,N} \end{bmatrix}.$$

16. Finally, the watermarked image I_w is obtained by combining the three watermark-added channels; I_{rw}, I_{gw} and I_{bw}, where

$$\left.\begin{aligned} I_{rw} &= r_w(i,j) \\ I_{gw} &= g_w(i,j) \\ I_{bw} &= b_w(i,j) \end{aligned}\right\} \quad \begin{aligned} 1 \le i \le M \\ 1 \le j \le N \end{aligned}. \tag{8}$$

IV. Watermark Extraction

1. Let $\hat{I}_W$ (possibly attacked watermarked-image) is broken down into its constituents $\hat{I}_{rw}$ $\hat{I}_{gw}$ and $\hat{I}_{bw}$, where,

$$\left.\begin{aligned} \hat{I}_{rw} &= \hat{r}_w(i,j) \\ \hat{I}_{gw} &= \hat{g}_w(i,j) \\ \hat{I}_{bw} &= \hat{b}_w(i,j) \end{aligned}\right\} \quad \begin{aligned} 1 \le i \le M \\ 1 \le j \le N \end{aligned}. \tag{9}$$

2. The covariance matrix $\hat{\mathbb{C}}$ is computed as follows for a given matrix $\hat{\mathbb{B}}$

$$\hat{\mathbb{C}} = \frac{1}{MN}\left(\hat{\mathbb{B}}\hat{\mathbb{B}}^T\right) = \hat{Q}\hat{\Lambda}\hat{Q}^{-1}, \tag{10}$$

where,

$$\hat{\mathbb{B}} = \begin{bmatrix} \hat{r}w_{1,1} & \cdots & \hat{r}w_{1,N} & \hat{r}w_{2,1} & \cdots & \hat{r}w_{2,N} & \cdots & \hat{r}w_{M,1} & \cdots & \hat{r}w_{M,N} \\ \hat{g}w_{1,1} & \cdots & \hat{g}w_{1,N} & \hat{g}w_{2,1} & \cdots & \hat{g}w_{2,N} & \cdots & \hat{g}w_{M,1} & \cdots & \hat{g}w_{M,N} \\ \hat{b}w_{1,1} & \cdots & \hat{b}w_{1,N} & \hat{b}w_{2,1} & \cdots & \hat{b}w_{2,N} & \cdots & \hat{b}w_{M,1} & \cdots & \hat{b}w_{M,N} \end{bmatrix},$$

$$\hat{Q} = [\hat{q}_{i,j}]_{\substack{1 \le i \le m3 \\ 1 \le i \le m3}},$$

$$\hat{\Lambda} = \begin{cases} \hat{\lambda}_{i,j} & when\ i = j \\ 0 & otherwise \end{cases} \quad 1 \le (i,j) \le 3.$$

3. The covariance matrix $\hat{\mathbb{C}}$ is decomposed into its principal components as shown below.

$$\hat{\delta}_w = \begin{bmatrix} \hat{\delta}_{rw} \\ \hat{\delta}_{gw} \\ \hat{\delta}_{bw} \end{bmatrix} = \hat{Q}\hat{\mathbb{B}}^T$$

$$\begin{bmatrix} \hat{\delta} rw_{1,1} & \cdots & \hat{\delta} rw_{1,N} & \hat{\delta} rw_{2,1} & \cdots & \hat{\delta} rw_{2,N} & \cdots & \hat{\delta} rw_{M,1} & \cdots & \hat{\delta} rw_{M,N} \\ \hat{\delta} gw_{1,1} & \cdots & \hat{\delta} gw_{1,N} & \hat{\delta} gw_{2,1} & \cdots & \hat{\delta} gw_{2,N} & \cdots & \hat{\delta} gw_{M,1} & \cdots & \hat{\delta} gw_{M,N} \\ \hat{\delta} bw_{1,1} & \cdots & \hat{\delta} bw_{1,N} & \hat{\delta} bw_{2,1} & \cdots & \hat{\delta} bw_{2,N} & \cdots & \hat{\delta} bw_{M,1} & \cdots & \hat{\delta} bw_{M,N} \end{bmatrix}.$$

4. The 1st, 2nd, and 3rd rows of $\hat{\delta}_w$ are converted into matrices $\hat{\delta}_{rnw}$, $\hat{\delta}_{gnw}$ and $\hat{\delta}_{bnw}$ respectively, each of size $M \times N$.

$$\begin{aligned} \hat{\delta}_{rnw} &= [\hat{\delta}_{rw}(i,j)] \\ \hat{\delta}_{gnw} &= [\hat{\delta}_{gw}(i,j)] \quad 1 \le (i,j) \le M, N. \\ \hat{\delta}_{bnw} &= [\hat{\delta}_{bw}(i,j)] \end{aligned} \tag{11}$$

5. Distinct blocks, $\hat{\mathbb{A}}_b$ where, $b \in [1, MN/16]$ of sizes 4×4 are created by dividing $\hat{\delta}_{rnw}$.
6. Based on key Z_e, the watermark-added blocks are found and then decomposed as follows

$$\hat{\mathbb{A}}_k = \hat{U}_k \hat{S}_k \hat{V}_k^T, \quad k = Z_e(1), Z_e(1), \cdots, Z_e\left(\frac{MN}{32}\right). \tag{12}$$

7. Afterwards, using keys; , the locations of watermark-added elements are found, and watermarking bits form those elements are extracted using following conditions:

$$\Phi = \begin{cases} 1 & \text{if} \quad \hat{U}_{wk}(Z_q(k), Z_h(k)) \le \hat{U}_{wk}(Z_r(k), Z_h(k)), \\ 0 & \quad otherwise. \end{cases}$$

$$\Gamma = \begin{cases} 1 & \text{if} \quad \hat{V}_{wk}(Z_h(k), Z_q(k)) \le \hat{V}_{wk}(Z_h(k), Z_r(k)), \\ 0 & \quad otherwise. \end{cases}$$

$$\Delta = \begin{cases} 1 & \text{if} \quad \hat{\lambda}_{wk}(Z_q(k), Z_q(k)) \le \hat{\lambda}_{wk}(Z_r(k), Z_r(k)), \\ 0 & \quad otherwise. \end{cases}$$

The bits are extracted using Φ, Γ, and Δ as shown below

$$\Phi = \begin{cases} \Omega & \text{if} \quad (\Phi = \Delta) \vee (\Gamma = \Delta), \\ \Psi & \quad otherwise. \end{cases} \tag{13}$$

where,

$$\Psi = Mode\{\Phi, \Gamma, \Delta\}. \tag{14}$$

8. Eight $m \times n$, 8-bit planes are formed by arranging the bits calculated in last step (a total of $8 \times m \times n$ bits). Afterwards, those eight planes are used to create the 1st color channel of extracted watermark $(\hat{W}_r)$, where,

$$\hat{W}_r = [\hat{r}w_{i,j}] \qquad 1 \le (i,j) \le M, N.$$

9. To extract other two channels ($\hat{W}_g$ and $\hat{W}_b$), follow Step-5 to Step-8, just replace $\hat{\delta}_{rnw}$ with $\hat{\delta}_{gnw}$ for $\hat{W}_g$, and replace $\hat{\delta}_{rnw}$ with $\hat{\delta}_{bnw}$ for $\hat{W}_b$, as shown below

$$\begin{aligned} \hat{W}_g &= [\hat{g}w_{i,j}] \\ \hat{W}_b &= [\hat{b}w_{i,j}] \end{aligned} \qquad 1 \le (i,j) \le M, N. \tag{15}$$

10. Finally, the extracted color watermark ($\hat{W}$) is obtained from three color channels; $\hat{W}_r$, $\hat{W}_g$ and $\hat{W}_b$.

V. Experimental Results

A number of experimentations were conducted to measure the performance of the presented technique. To do so, six images (shown in Fig. 1) of dimensions (1024×1024) were utilized as host images. The average running time to embed a watermark into an image on a computer with specifications: i7 3.8 GHz processor, 8 GB RAM, and 64-bit

(i) (ii) (iii) (iv) (v) (vi)

Figure 1. Test images (1024 × 1024) (i). people, (ii). church, (iii). mountains, (iv). sea, (v). building, (vi). sunset

operating system is 8.23 seconds. While for extracting the watermark from a watermarked image it takes 4.25 seconds. Likewise, two different watermarks (shown in Fig. 2) of dimensions (64×64) were used. The databank [21] was used to obtain these images.

(i) (ii)

Figure 2: Watermarks (64×64) (a). Butterfly, (b). Log

The working of presented watermarking technique regarding capacity, robustness, security, and imperceptibility, is examined. The detailed discussion is in the subsequent sections.

A. Imperceptibility

The visual quality of watermarked-image is called imperceptibility [8, 22] and to examine the imperceptibility quantitatively, Peak-Signal-to-Noise-Ratio (PSNR), shown in (16), is used [7, 22]. The higher the PSNR value, the better is the imperceptibility.

The PNSR (measured in decibels) values of the presented technique for a range of scaling factor, which is used to control the amount of information embedded into the host image, is shown in Table I.

$$\mathrm{PSNR} = 10\log_{10}\left\{ \frac{\max\left[\max\{I(i,j)\}\right]}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\{I(i,j) - I_w(i,j)\}} \right\}. \tag{16}$$

The PNSR values of the presented technique for a range of scaling factor is shown in Table I.

TABLE I. PSNR (IN DECIBELS) VALUES USING DIVERSE SCALING FACTORS

Test-Images	**(γ)**				
	0.02	**0.04**	**0.06**	**0.08**	**0.1**
People	45.49	44.50	43.48	42.51	41.59
Church	46.52	45.56	44.58	43.64	42.73
Mountains	46.37	45.49	44.61	43.77	42.96
Sea	60.34	57.32	54.83	52.79	51.15
Building	45.64	44.77	43.92	43.09	42.30
Sunset	56.44	54.304	52.18	50.37	48.78

On contrary, to analyze the imperceptibility of presented scheme qualitatively, the original host images shown in Fig. 1 and their respective watermarked images are shown in Fig. 3.

(i) (ii) (iii) (iv) (v) (vi)

Figure 3: Watermarked Images (1024 × 1024) (a). People, (b). Church, (c). Mountains, (d). Sea, (e). Building, (f). Sunset

It is clear that human eye cannot see any dissimilarity between original images (Fig. 1) and watermarked images (Fig. 3). Moreover, the comparison of the presented scheme with [4, 5] in respect of PSNR values (shown in Table II), shows significant improvement of proposed scheme over the existing techniques.

TABLE II. PSNR (IN DECIBELS) VALUES FOR DIFFERENT TECHNIQUES FOR SCALING FACTORS 0.06

Test Images	Proposed Scheme	Presented in	
		[4]	[5]
People	43.4878	35.8533	28.4232
Church	44.5871	35.1059	27.8682
Mountains	44.6116	35.4712	27.3109
Sea	54.8339	36.8526	29.4537
Building	43.9181	34.3124	26.5556
Sunset	52.1849	38.1190	30.0461

B. Robustness

Robustness (ability to withstand against attacks applied to destroy or remove the watermark [7]) is also an important requisite any good watermarking scheme must meet. Again, to measure the robustness quantitatively, normalized co-relation (NC), shown in (17), where, W and $\hat{W}$ represent original and extracted watermarks respectively, used [29]. Higher the NC values, better the robustness. Normally, NC values lay between 0 and 1.

$$NC = \frac{\sum_{x=0}^{X}\sum_{y=0}^{Y}\left(W(x,y)\times\hat{W}(x,y)\right)}{\sqrt{\sum_{x=0}^{X}\sum_{y=0}^{Y}W^2(x,y)\times\sum_{x=0}^{X}\sum_{y=0}^{Y}\hat{W}^2(x,y)}}. \quad (17)$$

To examine the robustness of presented technique many attacks such as average filtering (AVGFL), Joint Photographic Expert Group (PEG) compression (JPEGC) rotation (ROT), simple blurring (SPBL), Y-Shearing (YSHR), motion blurring (MOBL), scaling (SCAL), salt & pepper noise (S&PNO), Cropping (CROP), affine transformation (AFTRA), Gaussian noise (GANO), X-shearing (XSHR), histogram equalization (HEQ) and, translation (TRL), were used to destroy the watermarks. The NC values for different scaling factors against all above-mentioned attacks are shown in Table III.

In contrast, to see the performance of presented scheme qualitatively, above-mentioned attacks were applied on watermarked images. Afterwards, the watermarks were extracted (shown in Fig. 4 and Fig. 5) from those attacked watermarked-images.

TABLE III: NC VALUES FOR DIVERSE VALUE OF γ

Attacks and their parameters		γ				
Different Types of Attacks	**Parameters**	**0.02**	**0.04**	**0.06**	**0.08**	**0.1**
ROT	**θ = 45**	0.9391	0.9383	0.9392	0.9384	0.9360
	θ = 125	0.9365	0.9345	0.9359	0.9340	0.9367
TRL	**Displayed by 40%**	0.9446	0.9443	0.9451	0.9444	0.9444
	Displayed by 120%	0.9351	0.9366	0.9355	0.9379	0.9367
XSHR	**Sheared by factor 0.4**	0.9467	0.9465	0.9463	0.9457	0.9456
	Sheared by factor -0.5	0.9472	0.9464	0.9474	0.9463	0.9469
YSHR	**Sheared by factor -0.4**	0.9398	0.9388	0.9389	0.9387	0.9397
	Sheared by factor 0.5	0.9331	0.9310	0.9328	0.9309	0.9296
AFTRA	**Transformed by 0.4**	0.9269	0.9272	0.9261	0.9268	0.9274
	Transformed by 0.5	0.9402	0.9405	0.9400	0.9403	0.9400
SCAL	**Scaled up by3 times**	0.9824	0.9838	0.9852	0.9853	0.9863
	Scaled down 0.5 times	0.9625	0.9637	0.9647	0.9649	0.9658
CROP	**10% cropping from center**	0.9473	0.9475	0.9477	0.9487	0.9471
	25% cropping from sides	0.9479	0.9489	0.9494	0.9482	0.9477
GANO	**Mean is 0.4 & variance is .01**	0.9453	0.9468	0.9472	0.9457	0.9458
	Mean is 0.5 & variance is 0.5	0.9443	0.9433	0.9431	0.9446	0.9440
S&PNO	**10% density**	0.9501	0.9515	0.9515	0.9513	0.9501
	50% density	0.9452	0.9447	0.9444	0.9448	0.9443
SPNO	**10% density**	0.9511	0.9507	0.9515	0.9522	0.9514
	50% density	0.9439	0.9436	0.9434	0.9444	0.9447
Blurring	**SPBL**	0.9560	0.9563	0.9573	0.9560	0.9565
	MOBL	0.9523	0.9519	0.9518	0.9523	0.9517
AVGFL	**5×5**	0.9558	0.9557	0.9553	0.9562	0.9560
	7×7	0.9534	0.9520	0.9523	0.9534	0.9541
HEQ		0.9741	0.9756	0.9759	0.9763	0.9768
JPEGC	**QF = 50**	0.9558	0.9560	0.9560	0.9555	0.9550

Every watermark is recognizable despite being extracted from attacked watermarked-images. This clearly means that the robustness of proposed scheme is satisfactory.

The comparison of the presented scheme with existing schemes [4, 5], in terms of NC values, and shown in Table IV, shows that presented scheme's improvement over the existing watermarking techniques.

C. Security

The third requirement in digital watermarking is that no one should be able to extract either false positive or true positive watermark with any fake key. This is known as security [7]. To examine the security of proposed scheme, several fake keys were applied and tried to extract the watermark. It is found that neither the true nor the false watermark was extracted. The extracted watermarks for fifteen false keys only are shown in Fig. 6. It is clear from Fig. 6, that none of the watermarks is recognizable, hence no recognizable watermark can be extracted.

D. Capacity

The fourth and last requirement is capacity, which refers to the capability of a watermarking scheme to accept any change with being degraded in quality. The capacity of the proposed scheme is two times more than [4, 5] and that is due to the involvement of both singular vectors and values in a novel and efficient way, as discussed in Section III.

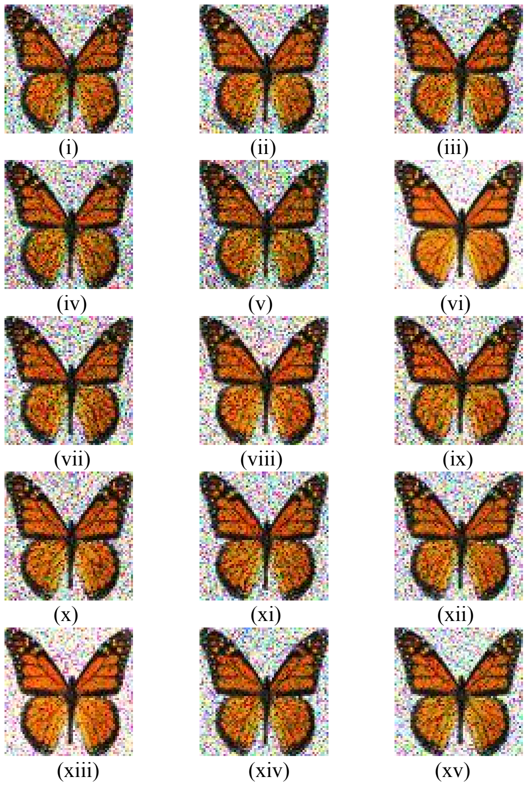


Figure 4. Watermarks (butterfly) extracted from watermarked-image attacked by: (i). ROT (ii). TRL (iii) XSHR (iv) YSHR (v) AFTRA (vi) SCAL (vii) CROP (viii) GANO (ix) S&PNO (x) SPNO (xi) SPBL (xii) MOBL (xiii) HEQ (xiv) JPEGC (xv) AVGFL

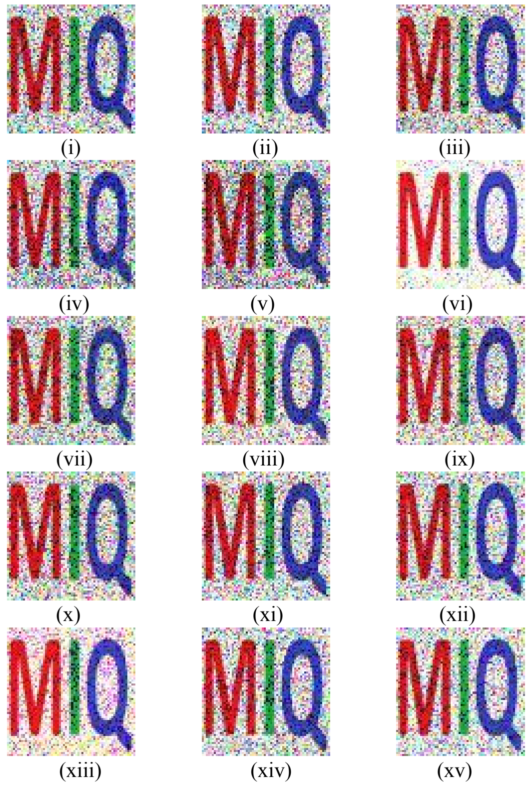
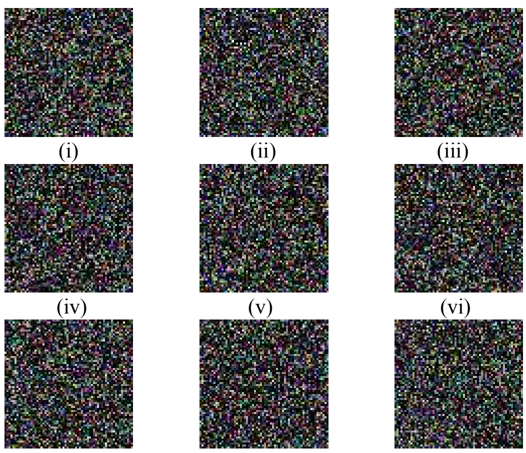


Figure 5. Watermarks (butterfly) extracted from watermarked-image attacked by: (i). ROT (ii). TRL (iii) XSHR (iv) YSHR (v) AFTRA (vi) SCAL (vii) CROP (viii) GANO (ix) S&PNO (x) SPNO (xi) SPBL (xii) MOBL (xiii) HEQ (xiv) JPEGC (xv) AVGFL

TABLE IV. NC VALUES FOR COMPARISON USING DIFFERENT IMAGES FOR SCALING FACTOR 0.006

Different Types of Attacks	Image: Church			Image: Mountains			Image: Sea		
	Proposed Scheme	Presented in [4]	Presented in [5]	Proposed Scheme	Presented in [4]	Presented in [5]	Proposed Scheme	Presented in [4]	Presented in [5]
ROT	0.9238	0.6725	0.6350	0.9016	0.6554	0.6405	0.9159	0.6320	0.5994
TRL	0.9430	0.8059	0.7136	0.9427	0.7938	0.7282	0.9429	0.8058	0.7444
XSHR	0.9454	0.8212	0.6990	0.9375	0.8284	0.7050	0.9434	0.8317	0.7398
YSHR	0.9319	0.6758	0.7292	0.9195	0.6973	0.6861	0.9218	0.6335	0.7202
AFTRA	0.9239	0.6769	0.6943	0.9156	0.6685	0.6844	0.9265	0.6939	0.6526
SCAL	0.9850	0.8445	0.7540	0.9813	0.8430	0.7318	0.9775	0.8481	0.7445
CROP	0.9416	0.7312	0.6335	0.9431	0.7499	0.6459	0.9453	0.7294	0.6488
GANO	0.9433	0.7618	0.6332	0.9440	0.7570	0.6490	0.9437	0.7623	0.6597
S&PNO	0.9441	0.7482	0.6800	0.9447	0.7462	0.6814	0.9443	0.7503	0.6537
SPNO	0.9446	0.7572	0.6499	0.9457	0.7558	0.6899	0.9440	0.7582	0.6944
MOBL	0.9539	0.6695	0.5990	0.9518	0.6903	0.6034	0.9553	0.5568	0.6389
SPBL	0.9513	0.7024	0.6196	0.9529	0.6918	0.6133	0.9366	0.6375	0.6255
AVGFL	0.9642	0.7177	0.6650	0.9542	0.7223	0.6336	0.9502	0.7187	0.6545
HEQ	0.9732	0.8458	0.7292	0.9651	0.8461	0.6989	0.9610	0.8434	0.7027
JPEGC	0.9539	0.7295	0.6746	0.9518	0.7271	0.6649	0.9261	0.7065	0.6324



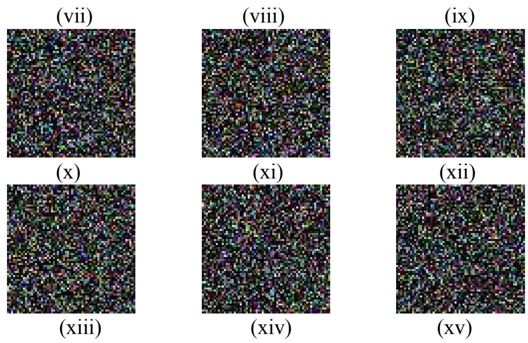


Figure 6: Watermarks tried to extract using fake (false) keys

VI. Conclusion

A novel secure and blind dual watermarking scheme for color images based on decorrelation of channels, singular values, and vectors is proposed. Heretofore, the attention was given only to either one or two requirements, while other requirements were ignored altogether, in designing the watermarking scheme. However, in devising the proposed technique it was made sure that all requirements (security, robustness, capacity, and imperceptibility) are met simultaneously, and it is evident from experimental results. To do so, a novel approach is devised to get satisfactory results in respect of security, imperceptibility, capacity, and robustness. Several experiments were conducted to validate the performance of presented watermarking technique and the comparison of the presented scheme with the latest watermarking schemes shows significant improvement.

Appendix A

Let a matrix A is broken down into its singular vectors (U, V) and singular values (S), as shown in (A.1).

$$\begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \alpha_{1,4} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \alpha_{2,4} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} & \alpha_{3,4} \\ \alpha_{4,1} & \alpha_{4,2} & \alpha_{4,3} & \alpha_{4,4} \end{bmatrix} = \tag{A.1}$$

$$\begin{bmatrix} \mu_{1,1} & \mu_{1,2} & \mu_{1,3} & \mu_{1,4} \\ \mu_{2,1} & \mu_{2,2} & \mu_{2,3} & \mu_{2,4} \\ \mu_{3,1} & \mu_{3,2} & \mu_{3,3} & \mu_{3,4} \\ \mu_{4,1} & \mu_{4,2} & \mu_{4,3} & \mu_{4,4} \end{bmatrix} \begin{bmatrix} s_{1,1} & 0 & 0 & 0 \\ 0 & s_{2,2} & 0 & 0 \\ 0 & 0 & s_{3,3} & 0 \\ 0 & 0 & 0 & s_{4,4} \end{bmatrix} \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} & v_{1,4} \\ v_{2,1} & v_{2,2} & v_{2,3} & v_{2,4} \\ v_{3,1} & v_{3,2} & v_{3,3} & v_{3,4} \\ v_{4,1} & v_{4,2} & v_{4,3} & v_{4,4} \end{bmatrix}.$$

A. *Finding 1:* Modifying elements of left singular vectors' columns results in the negligible distortion in original matrix *A*. On contrary, *A* suffers through sever distortion if the values of rows of left singular vectors (U) are changed [4].

Combining U, S and V can result in the reconstruction of *A*. The first and second row of A can be reconstructed as shown in (A.2) and (A.3).

$$\begin{cases} \alpha_{1,1} = \mu_{1,1}s_{1,1}v_{1,1} + \mu_{1,2}s_{2,2}v_{1,2} + \mu_{1,3}s_{3,3}v_{1,3} + \mu_{1,4}s_{4,4}v_{1,4}, \\ \alpha_{1,2} = \mu_{1,1}s_{1,1}v_{2,1} + \mu_{1,2}s_{2,2}v_{2,2} + \mu_{1,3}s_{3,3}v_{2,3} + \mu_{1,4}s_{4,4}v_{2,4}, \\ \alpha_{1,3} = \mu_{1,1}s_{1,1}v_{3,1} + \mu_{1,2}s_{2,2}v_{3,2} + \mu_{1,3}s_{3,3}v_{3,3} + \mu_{1,4}s_{4,4}v_{3,4}, \\ \alpha_{1,4} = \mu_{1,1}s_{1,1}v_{4,1} + \mu_{1,2}s_{2,2}v_{4,2} + \mu_{1,3}s_{3,3}v_{4,3} + \mu_{1,4}s_{4,4}v_{4,4}. \end{cases} \tag{A.2}$$

$$\begin{cases} \alpha_{2,1} = \mu_{2,1}s_{1,1}v_{1,1} + \mu_{2,2}s_{2,2}v_{1,2} + \mu_{2,3}s_{3,3}v_{1,3} + \mu_{2,4}s_{4,4}v_{1,4}, \\ \alpha_{2,2} = \mu_{2,1}s_{1,1}v_{2,1} + \mu_{2,2}s_{2,2}v_{2,2} + \mu_{2,3}s_{3,3}v_{2,3} + \mu_{2,4}s_{4,4}v_{2,4}, \\ \alpha_{2,3} = \mu_{2,1}s_{1,1}v_{3,1} + \mu_{2,2}s_{2,2}v_{3,2} + \mu_{2,3}s_{3,3}v_{3,3} + \mu_{2,4}s_{4,4}v_{3,4}, \\ \alpha_{2,4} = \mu_{2,1}s_{1,1}v_{4,1} + \mu_{2,2}s_{2,2}v_{4,2} + \mu_{2,3}s_{3,3}v_{4,3} + \mu_{2,4}s_{4,4}v_{4,4}. \end{cases} \tag{A.3}$$

If 0 is put in place of the first row of U in (A.1) will reduce (A.2) to (A.4).

$$\alpha_{1,1} = \alpha_{1,2} = \alpha_{1,3} = \alpha_{1,4} = 0. \tag{A.4}$$

On contrary, putting zero for the first column of U will reduce (A.2) and (A.3) to (A.5) and (A.6) respectively,

$$\begin{cases} \alpha_{1,1} = \mu_{1,2}s_{2,2}v_{1,2} + \mu_{1,3}s_{3,3}v_{1,3} + \mu_{1,4}s_{4,4}v_{1,4}, \\ \alpha_{1,2} = \mu_{1,2}s_{2,2}v_{2,2} + \mu_{1,3}s_{3,3}v_{2,3} + \mu_{1,4}s_{4,4}v_{2,4}, \\ \alpha_{1,3} = \mu_{1,2}s_{2,2}v_{3,2} + \mu_{1,3}s_{3,3}v_{3,3} + \mu_{1,4}s_{4,4}v_{3,4}, \\ \alpha_{1,4} = \mu_{1,2}s_{2,2}v_{4,2} + \mu_{1,3}s_{3,3}v_{4,3} + \mu_{1,4}s_{4,4}v_{4,4}. \end{cases} \tag{A.5}$$

$$\begin{cases} \alpha_{2,1} = \mu_{2,2}s_{2,2}v_{1,2} + \mu_{2,3}s_{3,3}v_{1,3} + \mu_{2,4}s_{4,4}v_{1,4}, \\ \alpha_{2,2} = \mu_{2,2}s_{2,2}v_{2,2} + \mu_{2,3}s_{3,3}v_{2,3} + \mu_{2,4}s_{4,4}v_{2,4}, \\ \alpha_{2,3} = \mu_{2,2}s_{2,2}v_{3,2} + \mu_{2,3}s_{3,3}v_{3,3} + \mu_{2,4}s_{4,4}v_{3,4}, \\ \alpha_{2,4} = \mu_{2,2}s_{2,2}v_{4,2} + \mu_{2,3}s_{3,3}v_{4,3} + \mu_{2,4}s_{4,4}v_{4,4}. \end{cases} \tag{A.6}$$

From (A.4) — (A.6) it is obvious that modifying rows of (U) has significant consequences on (A), whereas, modifying rows, instead, has a subtle effect on (A). The opposite holds true for V.

B. *Finding 2: It is found that the robustness of a watermarking scheme further improves if both U and V are considered equally for watermark embedding.*

To prove the Finding-2, let a matrix A is broken down to singular values and vectors, as shown below

$$A = USV^T, \tag{A.7}$$

where,

$$A = \begin{bmatrix} 90 & 67 & 77 & 133 \\ 56 & 71 & 86 & 138 \\ 160 & 203 & 171 & 73 \\ 87 & 172 & 220 & 184 \end{bmatrix}, U = \begin{bmatrix} -0.344 & -0.362 & 0.667 & 0.552 \\ -0.340 & -0.459 & 0.227 & -0.788 \\ -0.581 & 0.769 & 0.227 & -0.132 \\ -0.654 & -0.254 & -0.671 & 0.236 \end{bmatrix}$$

$$S = \begin{bmatrix} 521.78 & 0 & 0 & 0 \\ 0 & 123.77 & 0 & 0 \\ 0 & 0 & 65.80 & 0 \\ 0 & 0 & 0 & 7.149 \end{bmatrix},$$

$$V = \begin{bmatrix} -0.385 & 0.333 & 0.782 & 0.359 \\ -0.532 & 0.448 & -0.128 & -0.706 \\ -0.573 & 0.065 & -0.576 & 0.578 \\ -0.489 & -0.826 & 0.199 & -0.192 \end{bmatrix}.$$

Given that the watermarking bit is 0, modify second and third element from the first column of U using (4) – (7) in such a way that the second element of the first column of U becomes greater than the third element of the first column of U i.e. $U_{2,1} > U_{3,1}$. This condition is checked at watermark extracting stage to find out either bit-0 was embedded or bit-1. The new modified values of are as follows:

$$\left.\begin{aligned} U_{w(2,1)} &= \mathrm{sgn}(U_{2,1}) \times \left(\overline{U} - T/2\right) = -0.4558 \\ U_{w(3,1)} &= \mathrm{sgn}(U_{3,1}) \times \left(\overline{U} + T/2\right) = -0.4658 \end{aligned}\right\} T = 0.01.$$

Here the condition $U_{w(2,1)} > U_{w(3,1)}$ is satisfied, which indicates that bit 0 was embedded, and that is exactly the case. Now, modified U_w is used to reconstruct contaminated (watermark added) *A*, i.e. A_w

$$A_w = U_w S V^T = \begin{bmatrix} 90 & 67 & 77 & 133 \\ 82.2738 & 103.1629 & 120.6323 & 167.5851 \\ 136.7262 & 170.8371 & 136.3677 & 43.4149 \\ 87 & 172 & 220 & 184 \end{bmatrix},$$

where,

$$U_w = \begin{bmatrix} -0.344 & -0.362 & 0.667 & 0.552 \\ -0.455 & -0.459 & 0.227 & -0.788 \\ -0.465 & 0.769 & 0.227 & -0.132 \\ -0.654 & -0.254 & -0.671 & 0.236 \end{bmatrix}.$$

Based on the relationship between two elements of U, the receiver decides regarding extracting bit information.

$$ExtractingBit = \begin{cases} 1 & if \quad U_{2,1} < U_{3,1} \\ 0 & if \quad U_{2,1} > U_{3,1} \end{cases}.$$

The receiver decomposed A_w to extract the hidden information; $A_w = \hat{U}_w \hat{S} \hat{V}^T$. Here, $\hat{U}_{w(2,1)} > \hat{U}_{w(3,1)}$, that is the indication that embedded bit is 1, however, in reality, the embedded bit was 0. The reason for this false detection is that the changes introduced between elements of U is divided among other elements of S, and V as well, during construction and reconstruction of A_w. The fragility of watermark embedding can extraction can be avoided if the same amount of change that was introduced between two elements of U, is also introduced between two elements of V as shown below

$$\left.\begin{aligned} V_{w(1,2)} &= \mathrm{sgn}(V_{1,2}) \times \left(\overline{V} - T/2\right) = 0.5526 \\ V_{w(1,3)} &= \mathrm{sgn}(V_{1,3}) \times \left(\overline{V} + T/2\right) = 0.5626 \end{aligned}\right\} T = 0.01.$$

Now, using both modified singular vectors U_w and V_w to get the modified image A, i.e. A_{w1}, as shown below

$$A_w = U_w S V_w^{\,T} = \begin{bmatrix} 70.5306 & 67 & 77 & 133 \\ 66.5047 & 103.1629 & 120.6323 & 167.5851 \\ 154.3358 & 170.8371 & 136.3677 & 43.4149 \\ 89.7841 & 172 & 220 & 184 \end{bmatrix}.$$

The receiver decomposes A_{w1} to extract the hidden information, i.e. $A_w = \hat{U}_w \hat{S} \hat{V}_w^{\,T}$.

This time $\hat{U}_{w(2,1)} > \hat{U}_{w(3,1)}$, indicating extracting bit is 0 and which is correct. It is hence proved that employing right singular vectors (V), in addition to left singular vector (U), improves the robustness significantly.

C. Finding 3: Modification of two elements from a column of U with lowest covariance value results in minor degradation in A as compared to modification in any other two elements of U.

It has been shown in observation 1 that changing column of left singular vectors (U) results in terms of negligible distortion in A, in contrast, altering rows of U makes significant changing in A. The next task is to select the column. For this reason, three cases are analyzed and the case with the good result is adapted in watermark embedding process.

1) Case 1: Two elements (2^{nd} and 3^{rd}) from the first column of U are selected for modification.

2) Case 2: A column with lowest covariance value is selected, and then two elements with lowest covariance values within the selected column are chosen for modification.

3) Case 3: Any two elements with lowest covariance values from the first column of U are selected for modification.

Let the image I is decomposed into blocks of size 4×4. Based on the covariance matrix of each block, two elements for each case discussed above are modified, then reconstruct the blocks from modified values for each case. In Fig. A.1, the PSNR of first 200 blocks are calculated and plotted. From Fig. A.1, it is clear, that the PSNR for Case 2 is better as compared to other two cases. Therefore, Case 2 was adopted in this paper for watermark embedding.

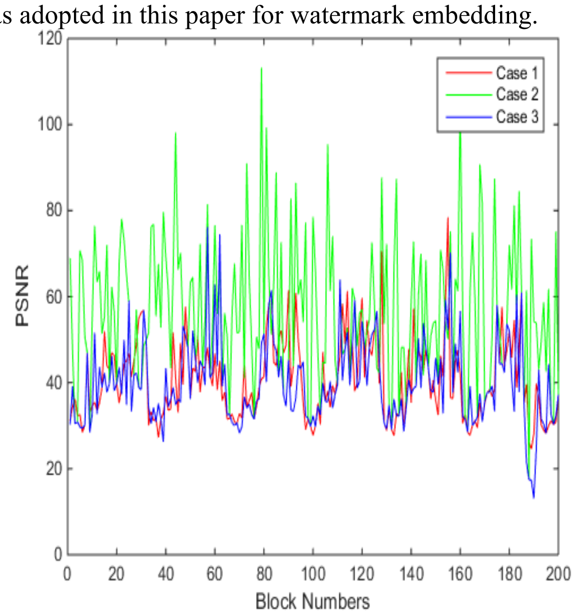


Figure A.1: Graphical illustration of Finding 3

REFERENCES

[1] Mayer, Trisha, “The politics of online copyright enforcement in the EU”, Springer, pp. 25—36, 2017. doi: 10.1007/978-3-319-50974-7

[2] J. Ouyang, G. Coatrieux, B. Chen, H. Shu, “Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping,” Journal of Computers & Electrical Engineering, vol. 46, pp. 419–432, 2015. doi: 10.1016/j.compeleceng.2015.03.004.

[3] C. S. Chang, J. J. Shen, “Features classification forest: A novel development that is adaptable to robust blind watermarking techniques,” IEEE Transactions on Image Processing, vol. 26, no. 8, pp. 3921—3935, 2017. doi: 10.1109/TIP.2017.2706502

[4] Q. Su, Y. Niu, H. Zou, X. Liu, “A blind dual color image watermarking based on singular value decomposition,” Elsevier Journal of Applied Mathematics and Computation, vol. 219, no. 16, pp. 8455–8466, 2013. doi: 10.1016/j.amc.2013.03.013.

[5] Q. Su, Y. Niu, X. Liu, T. Yao, “A novel blind digital watermarking algorithm for embedding color image into color image,” International Journal for Light and Electron Optics, vol. 124, no. 18, pp. 3254–3259, 2013. doi: 10.1016/j.ijleo.2012.10.005.

[6] B. Chen, G. Coatrieux, G. Chen, X. Sun, J. L. Coatrieux, H. Shu, Full 4-d quaternion discrete Fourier transform based watermarking for color images, Journal of Digital Signal Processing, vol. 28 pp. 106–119, 2014. doi: 10.1016/j.dsp.2014.02.010.

[7] N. M. Makbool, B. E. Khoo, “A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition,” Elsevier Journal of Digital Signal Processing, vol. 33, pp. 134–147, 2014. doi: 10.1016/j.dsp.2014.06.012.

[8] H. Qi, D. Zheng, J. Zhao, “Human visual system based adaptive digital image watermarking,” Elsevier Journal of Signal Processing, vol. 88, no. 1, pp. 174–188, 2008. doi: 10.1016/j.sigpro.2007.07.020.

[9] A. Roy, A. K. Maiti, K. Ghosh, “A perception based color image adaptive watermarking scheme in ycbcr space,” International Conference on Signal Processing and Integrated Networks, pp. 304–317, 2015. doi:10.1109/SPIN.2015.7095399.

[10] R. Liu, T. Tan, “An svd based watermarking scheme for protecting rightful ownership,” IEEE Trans. on Multimedia, vol. 4, no. 1, pp. 121–128, 2002. doi:10.1109/6046.985560.

[11] C. C. Lai, C. C. Tai, “Digital image watermarking using discrete wavelet transform and singular value decomposition,” IEEE Trans. on Instrumentation and Measurement, vol. 59, no. 11, pp. 3060–3060, 2010. doi: 10.1109/TIM.2010.2066770.

[12] K. Loukhaoukha, Comments on a digital watermarking scheme based on singular value decomposition and tiny genetic algorithm, Elsevier Journal of Digital Signal Processing vol. 23, no. 4 pp. 1334, 2013. doi: 10.1016/j.dsp.2013.02.006.

[13] X. P. Zhang, K. Li, “Comments on ‘an svd based watermarking scheme for protecting rightful ownership,’” IEEE Trans. on Multimedia, vol. 5, no. 2 pp. 593–594, 2005. doi:10.1109/TMM.2005.843357.

[14] C. C. Lai, “A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm,” Elsevier Journal of Digital Signal Processing, vol. 21, no. 4 pp. 522–527, 2011. doi: 10.1016/j.dsp. 2011.01.017.

[15] R. Rykaczewski, “Comments on ‘an SVD based watermarking scheme for protecting rightful ownership,’” IEEE Trans. on Multimedia, vol. 9 no. 2 pp. 421–423, 2007. doi:10.1109/TMM.2006.886297.

[16] E. Yavuz, Z. Telatar, “Comments on ‘a digital watermarking scheme based on singular value decomposition and tiny genetic algorithm,’” Elsevier Journal of Digital Signal Processing, vol. 23 no. 4 pp. 1335–1336, 2013. doi: 10.1016/j.dsp.2013.02.009.

[17] R. Vidal, Y. Ma, S. S. Sastry, “Generalized principal component analysis”, Introduction, Springer, pp. 25—54, 2016. doi: 10.1007/978-0-387-87811-9.

[18] B. K. Gunturk, X. Li, “Image Restoration: Fundamentals and Recent Advances,” Taylor & Francis Group, pp. 168—172, 2013.

[19] B. Schauerte, “Multimodal computational attention for scene understanding and robotics,” Springer, pp. 115—175, 2016. doi: 10.1007/978-3-319-33796-8.

[20] S. Jayaraman, S. Esakkirajan, T. Veerakumar, “Image Enhancement”, in Digital Image Processing, McGraw-Hill Education, pp. 243—297, 2011.

[21] H. Jegou, M. Douze, C. Schmid, “Hamming embedding and weak geometric consistency for large scale image search,” in: A. Z. David Forsyth, Philip Torr (Ed.), European Conference on Computer Vision, Vol. I of LNCS, Springer, pp. 304–317, 2008. URL http://lear.inrialpes.fr/pubs/2008/JDS08, doi: 10.1007/978-3-540-88682-2_24.

[22] C. S. Chang, J. J. Shen, “Feature classification forest: A novel development that is adaptable to robust blind watermarking techniques,” IEEE Transaction on Image Processing, vol. 26, no. 8, pp. 3921—3935, 2017. doi: 10.1109/TIP.2017.2706502.