A Blind Adaptive Color Image Watermarking Scheme Based on Principal Component Analysis, Singular Value Decomposition and Human Visual System

Muhammad IMRAN, Bruce A. HARVEY

Department of Electrical & Computer Engineering, College of Engineering
Florida State University, 2525 Pottsdamer St, Tallahassee, FL 32310, USA

mi14@my.fsu.edu, bharvey@fsu.edu

Submitted February 26, 2016 / Accepted July 11, 2017

Abstract. *A blind adaptive color image watermarking scheme based on principal component analysis, singular value decomposition, and human visual system is proposed. The use of principal component analysis to decorrelate the three color channels of host image, improves the perceptual quality of watermarked image. Whereas, human visual system and fuzzy inference system helped to improve both imperceptibility and robustness by selecting adaptive scaling factor, so that, areas more prone to noise can be added with more information as compared to less prone areas. To achieve security, location of watermark embedding is kept secret and used as key at the time of watermark extraction, whereas, for capacity both singular values and vectors are involved in watermark embedding process. As a result, four contradictory requirements; imperceptibility, robustness, security and capacity are achieved as suggested by results. Both subjective and objective methods are acquired to examine the performance of proposed schemes. For subjective analysis the watermarked images and watermarks extracted from attacked watermarked images are shown. For objective analysis of proposed scheme in terms of imperceptibility, peak signal to noise ratio, structural similarity index, visual information fidelity and normalized color difference are used. Whereas, for objective analysis in terms of robustness, normalized correlation, bit error rate, normalized hamming distance and global authentication rate are used. Security is checked by using different keys to extract the watermark. The proposed schemes are compared with state-of-the-art watermarking techniques and found better performance as suggested by results.*

Keywords

Image watermarking, principal component analysis, singular value decomposition, human visual system, imperceptibility, robustness

1. Introduction

The enormous usage and afford-ability of Internet across the world, has made it easy to access online literature in the form of pictures, audios, videos, books, etc. The data available online can be downloaded, and then can be redistributed its copies multiple times, without any distinguishable difference between original and copied material. This illegal distribution and copyright violation results in the form of millions of dollars loss [1]. To overcome this illicit distribution and copyright violation digital watermarking is proposed as a prominent solution [2–7].

Watermarking is the way of embedding some information (image, audio, strings) into another data (image, audio, video, pdf file). The embedded data can later be extracted to prove the ownership. If the data which is being protected by embedding information in it is image, then this type of watermarking is called image watermarking. The information which is being hidden is called watermark, and the image in which watermark is hidden is called host image, and the resultant image is known as watermarked image. In terms of information required at the time of watermark extraction, watermarking is divided into blind and non-blind [2]. In later case, original image is required (and may be key) at the time of watermark extraction, whereas in former watermarking type there is no need of original image for extraction of watermark [3]. Therefore, blind watermarking is considered to be more secure and convenient, hence in this paper blind watermarking schemes are proposed.

The watermarking scheme for gray scale [2], [4], [5] and for color images [1], [3], [6], [7] are available in literature. One additional challenge of color image watermarking is that the three channels R, G, and B are highly correlated [3], [8], hence modification of one channel affects other channels severally and as a result the quality of whole image is compromised. This adverse effect can be avoided if Principal Component Analysis (PCA) [9] is used. In the proposed scheme PCA is used to decorrelate the three channels. In most cases either the same amount of information is embedded or modification in host image is made, same is case with [3], [6]. Whereas in actual there are some regions in image which are more tolerable to noise as compared to others. Therefore embedding more information in areas which are more prone to noise and less data into regions which are more susceptible to alterations. In this way both imperceptibility and robustness can be achieved simultaneously. For this purpose Human Visual System (HVS) and Fuzzy Inference System (FIS) are used to find adaptive scaling factor so that the amount of information is embedded according to the acceptability of host image.

In addition to perceptual quality of watermarked image and robustness, an other concern is that neither original nor false watermark should be extracted intentionally or unintentionally as was the case with [10–12]. Where, with the help of fake keys (singular vectors) a watermark different than the embedded watermark is extracted, which completely destroys the purpose of copyright protection. Therefore in designing proposed scheme, special attention is given to security and it is ensured that neither original nor false watermark is extracted as suggest by results in Sec. 5.3. The proposed scheme is discussed in detail in the following sections.

2. Proposed Scheme

In this paper two watermarking schemes are proposed. In proposed scheme 1, HVS and FIS are used together to find the areas where more information can be embedded, and regions where less data should be concealed. In this way two contradictory requirements of watermarking techniques; imperceptibility and robustness can be achieved. The perceptual quality of watermarked image is also improved due to the use of PCA. The third and utmost important quality is the security of watermarking scheme, which is given special attention in designing both the techniques. To achieve security, a different way of choosing elements for modifications from U, S and V are selected. In this way not only security but robustness and capacity are also improved as suggested by results in Sec. 5.2 and 5.3. In proposed scheme 2, HVS and FIS are not employed to find adaptive scaling factors, hence proposed scheme 1 is general case of proposed scheme 2. Since the proposed schemes are mostly relying on SVD, therefore, techniques chosen for comparision are also based on SVD. Both schemes are compared with state-of-the-art techniques [3], [6], [13], [14] and found that proposed schemes outperform. As HVS and FIS are used in this paper, therefore, they are discussed in following sections.

2.1 Human Visual System

Given an image I of size $M \times N$, the luminance masking [15] M_L, is calculated as follows:

$$M_L(x, y) = \max\{f_1(bg(x, y), mg(x, y)), f_2(bg(x, y))\} \quad (1)$$

where

$$f_1(bg(x, y), mg(x, y)) = mg(x, y)\alpha\{bg(x, y)) + \beta(bg(x, y)\},$$

$$f_2(bg(x, y)) = \begin{cases} T_o\left(1 - \left(\frac{bg(x,y)}{127}\right)^{0.5}\right) + 3, & bg(x, y) \le 127, \\ \gamma(bg(x, y) - 127) + 3, & bg(x, y) > 127, \end{cases}$$

$$\alpha(bg(x, y)) = \left\{ \begin{array}{l} 0.0001bg(x, y) + 0.115, \\ 1 \le x \le H, 1 \le y \le W, \end{array} \right.$$

$$\beta(bg(x, y)) = \lambda - 0.01bg(x, y),$$

f_1 is the spatial masking function, $bg(x, y)$ is the background luminance, $mg(x, y)$ is the maximum weighted average of luminance differences around the pixel at location (x, y), $W = M/2$ and $H = N/2$. f_2, α and β are the background luminance dependent functions. The value of some other parameters are: $T_0 = 17$, $\gamma = 3/128$, and $\lambda = 1/2$. In order to know about the selection of parameter's values readers may refer [15]. $mg(x, y)$ and $bg(x, y)$ are calculated as follows:

$$\begin{aligned} mg(x, y) &= \max_{k=1,2,3,4}\{|\mathrm{grad}_k(x, y)|\}, \\ \mathrm{grad}_k(x, y) &= \frac{1}{16}\sum_{i=1}^{5}\sum_{j=1}^{5} I(x - 3 + i, y - 3 + j)G_k(i, j), \\ bg(x, y) &= \frac{1}{32}\sum_{i=1}^{5}\sum_{j=1}^{5} I(x - 3 + i, y - 3 + j)B(i, j). \end{aligned}$$

The values of G_1, G_2, G_3, G_4 and B are shown below:

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 8 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & -3 & -8 & -3 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, G_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 8 & 3 & 0 & 0 \\ 1 & 3 & 0 & -3 & -1 \\ 0 & 0 & -3 & -8 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix},$$

$$G_3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 8 & 0 \\ -1 & -3 & 0 & 3 & 1 \\ 0 & -8 & -3 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, G_4 = \begin{bmatrix} 0 & 1 & 0 & -1 & 0 \\ 0 & 3 & 0 & -3 & 0 \\ 0 & 8 & 0 & -8 & 0 \\ 0 & 3 & 0 & -3 & 0 \\ 0 & 1 & 0 & -1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 1 \\ 1 & 2 & 0 & 2 & 1 \\ 1 & 2 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Remark 1: Since, darkness is more tolerable (then brightness) to watermark [15], [16]. More alternation can be made into dark areas as compared to bright regions of image, in this way, imperceptibility and robustness can be achieved.

2.2 Fuzzy Inference System

Mamdani fuzzy inference system [17] is used to find the adaptive scaling factor α_{M_L} using luminance masking shown in (1). The membership functions for luminance masking is shown in Fig. 1.

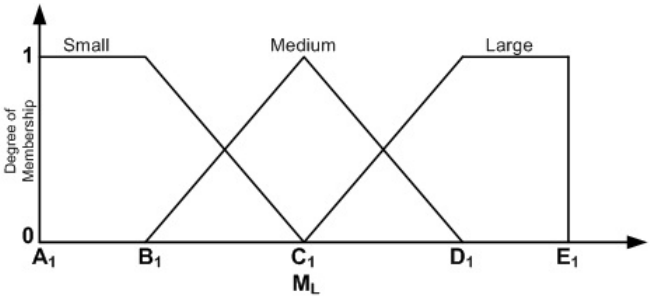


Fig. 1. Membership function for luminance masking.

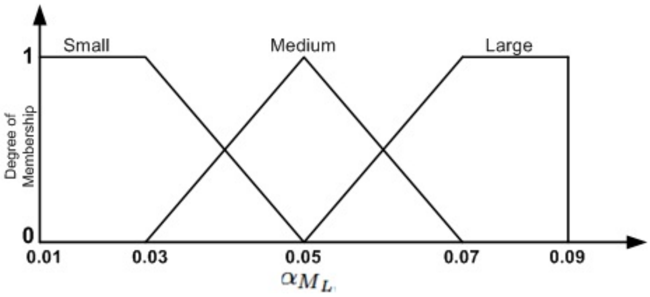


Fig. 2. Membership function for α_{M_L}.

Where the values A_1, B_1, C_1, D_1 and E_1 are calculated as:

$$A_1 = \min_{x=1}^{W} \min_{y=1}^{H} (M_L), \tag{2}$$

$$C_1 = \frac{1}{WH} \sum_{x=1}^{W} \sum_{y=1}^{H} M_L(x, y), \tag{3}$$

$$E_1 = \max_{x=1}^{W} \max_{y=1}^{H} M_L(x, y). \tag{4}$$

In order to chose B_1 and D_1, following condition must be satisfied

$$C_1 - B_1 = D_1 - C_1.$$

The membership function for adaptive scaling factor α_{M_L} is shown in Fig. 2.

The rules used for calculating α_{M_L} are as follows:

Ru^1 : IF M_L is large, THEN α_{M_L} is large,
Ru^2 : IF M_L is medium, THEN α_{M_L} is medium,
Ru^3 : IF M_L is small, THEN α_{M_L} is small.

The detailed procedure of watermark embedding and extraction are discussed in following sections.

3. Proposed Scheme 1

In proposed scheme 1, human visual system is used to find the areas of image which are more prone to alterations, and areas which are less prone to disturbances. The information of HVS is then used in FIS to find adaptive scaling factor for watermark embedding, so that the areas which are more prone to noise, can be embedded with more information as compared to areas which are less prone. In this way both; imperceptibility and robustness can be achieved as suggested by results in Sec. 5. The detailed procedure of watermark embedding and extraction are discussed in Sec. 3.1 and 3.2 respectively.

3.1 Watermark Embedding

1. Let the original image I is decomposed into three channels R, G, and B

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1N} \\ r_{21} & r_{22} & \dots & r_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ r_{M1} & r_{M2} & \dots & r_{MN} \end{bmatrix},$$

$$G = \begin{bmatrix} g_{11} & g_{12} & \dots & g_{1N} \\ g_{21} & g_{22} & \dots & g_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ g_{M1} & g_{M2} & \dots & g_{MN} \end{bmatrix},$$

$$B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1N} \\ b_{21} & b_{22} & \dots & b_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ b_{M1} & b_{M2} & \dots & b_{MN} \end{bmatrix},$$

M and N defines the size of image.

2. Let a covariance matrix C be computed as

$$C = \frac{1}{MN}(AA^{\mathrm{T}}) = Q \wedge Q^{-1} \tag{5}$$

where

A =

$$\begin{bmatrix} r_{11} & \dots & r_{1N} & r_{21} & \dots & r_{2N} & \dots & r_{M1} & \dots r_{MN} \\ g_{11} & \dots & g_{1N} & g_{21} & \dots & g_{2N} & \dots & g_{M1} & \dots g_{MN} \\ b_{11} & \dots & b_{1N} & b_{21} & \dots & b_{2N} & \dots & b_{M1} & \dots b_{MN} \end{bmatrix},$$

$$Q = \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{32} & q_{33} \\ q_{31} & q_{32} & q_{33} \end{bmatrix}, \qquad \wedge = \begin{bmatrix} \lambda_{11} & 0 & 0 \\ 0 & \lambda_{22} & 0 \\ 0 & 0 & \lambda_{33} \end{bmatrix},$$

$\lambda_{11} \geq \lambda_{22} \geq \lambda_{33}$ are eigenvalues in descending order.

3. The principal components [18] of covariance matrix C are calculated as

$$P = \begin{bmatrix} P_r \\ P_g \\ P_r \end{bmatrix} = Q^{\mathrm{T}} A =$$

$$= \begin{bmatrix} p_{r_{11}} & \dots & p_{r_{1N}} & p_{r_{21}} & \dots \\ p_{g_{11}} & \dots & p_{g_{1N}} & p_{g_{21}} & \dots \\ p_{b_{11}} & \dots & p_{b_{1N}} & p_{b_{21}} & \dots \end{bmatrix}$$

$$\begin{matrix} \dots & p_{r_{2N}} & \dots & p_{r_{M1}} & \dots & p_{r_{MN}} \\ \dots & p_{g_{2N}} & \dots & p_{g_{M1}} & \dots & p_{g_{MN}} \\ \dots & p_{b_{2N}} & \dots & p_{b_{M1}} & \dots & p_{b_{MN}} \end{matrix} \Bigg].$$

Remark 2: Since R, G and B components are highly correlated [3], [7] and [8], modification in one channel causes alteration in other two channels, as a result imperceptibility is affected severely. However, this can be avoided if PCA [9] is used to decorrelate these R, G and B components.

4. Let matrix $\mathbf{P_{rn}}$ is formed from row vector $\mathbf{P_r}$ of matrix $\mathbf{P}$ as shown below

$$P_{rn} = \begin{bmatrix} p_{r_{11}} & p_{r_{12}} & \cdots & p_{r_{1N}} \\ p_{r_{21}} & p_{r_{22}} & \cdots & p_{r_{2N}} \\ \vdots & \vdots & \ddots & \vdots \\ p_{r_{M1}} & p_{r_{M2}} & \cdots & p_{r_{MN}} \end{bmatrix}.$$

Remark 3: Since $\mathbf{P_{rn}}$ is composed of components from $\mathbf{P_r}$ and contains most of the information [9], therefore it is chosen for watermark embedding.

5. Let $\mathbf{P_{rn}}$ is divided into non-overlapping blocks $\mathbb{A}_\mathbf{1}$, $\mathbb{A}_\mathbf{2}, \ldots \mathbb{A}_\mathbf{pq}$. Where the size of each block is 4×4, $p \leq M/4$ and $q \leq N/4$.

6. Let each block is decomposed using SVD as follows

$$\mathbb{A}_i = U_i S_i V_i^{\mathrm{T}}, \quad i = 1, 2, \ldots, pq \tag{6}$$

where S is a diagonal matrix containing singular values in descending order, whereas, U and V represent the left and right singular vectors respectively.
Remark 4: Small perturbation in image does not cause large variation in singular values and vice versa [5], [7].
Remark 5: Singular values contain intrinsic properties of image, whereas geometric information is maintained by corresponding singular vectors [5], [7].

7. Compute the covariance matrix of each block $\mathbb{A}_i$. Select the column number with lowest covariance (variance) value, and then location of two values with lowest covariance values within that selected column from covariance matrix of each block. In this way three numbers are selected for each block, and those selected locations will later be used as key at the time of watermark extraction. For instance (f, e and g) are selected, where, 'f' represents the column number with lowest covariance value, 'e' and 'g' denoting the locations of two values with lowest covariance values from selected columns. These three numbers are used to select two numbers from U and V for modifications. For example in case of (f, e, and g), tow numbers at location (e, f) and (g, f) from U, similarly two values from location (f, e) and (f, g) from V are selected for watermark embedding. In addition to that singular values either at location (e, e) or (g, g) based on embedding bits are modified as shown in (7)–(10). It is shown in result in Sec. 5 that the procedure described above for choosing two numbers for modifications gives better results in terms of imperceptibility.

8. Let the luminance masking M_{L_i} for each block $\mathbb{A}_\mathbf{i}$, where $i = 1, 2, 3, \ldots, pq$ is calculated using (1).

9. The adaptive scaling factor $\alpha_{ML_i}(g, f)$, $\alpha_{ML_i}(e, f)$, $\alpha_{ML_i}(f, g)$ and $\alpha_{ML_i}(f, e)$ of each block $\mathbb{A}_\mathbf{i}$ for values of selected positions are calculated by utilizing luminance masking values M_{L_i} of block 'i'.

10. Given a watermark W of size $M/4 \times N/4$, the watermarking bits W_i are embedded as described below in (7)–(10).

Case 1: If embedding bit is 1 i.e. $(W_i = 1)$.

$$\overbrace{\begin{aligned} u_{wi(e,f)} &= \mathrm{sgn}\big(u_{i(e,f)}\big) \times \big(\bar{U}_i + (\beta\alpha_{ML_i}(e,f))/2\big) \\ u_{wi(g,f)} &= \mathrm{sgn}\big(u_{i(g,f)}\big) \times \big(\bar{U}_i - (\beta\alpha_{ML_i}(g,f))/2\big) \\ v_{wi(f,e)} &= \mathrm{sgn}\big(v_{i(f,e)}\big) \times \big(\bar{V}_i + (\beta\alpha_{ML_i}(f,e))/2\big) \\ v_{wi(f,g)} &= \mathrm{sgn}\big(v_{i(f,g)}\big) \times \big(\bar{V}_i - (\beta\alpha_{ML_i}(f,g))/2\big) \\ s_{wi(g,g)} &= 3 \times s_{i(e,e)} \end{aligned}}^{\text{if } e < g} \tag{7}$$

$$\overbrace{\begin{aligned} u_{wi(g,f)} &= \mathrm{sgn}\big(u_{i(g,f)}\big) \times \big(\bar{U}_i + (\beta\alpha_{ML_i}(g,f))/2\big) \\ u_{wi(e,f)} &= \mathrm{sgn}\big(u_{i(e,f)}\big) \times \big(\bar{U}_i - (\beta\alpha_{ML_i}(e,f))/2\big) \\ v_{wi(f,g)} &= \mathrm{sgn}\big(v_{i(f,g)}\big) \times \big(\bar{V}_i + (\beta\alpha_{ML_i}(f,g))/2\big) \\ v_{wi(f,e)} &= \mathrm{sgn}\big(v_{i(f,e)}\big) \times \big(\bar{V}_i - (\beta\alpha_{ML_i}(f,e))/2\big) \\ s_{wi(e,e)} &= 3 \times s_{i(g,g)} \end{aligned}}^{\text{If } e > g} \tag{8}$$

Case 2: If embedding bit is 0 i.e. $(W_i = 0)$.

$$\overbrace{\begin{aligned} u_{wi(e,f)} &= \mathrm{sgn}\big(u_{i(e,f)}\big) \times \big(\bar{U}_i - (\beta\alpha_{ML_i}(e,f))/2\big) \\ u_{wi(g,f)} &= \mathrm{sgn}\big(u_{i(g,f)}\big) \times \big(\bar{U}_i + (\beta\alpha_{ML_i}(g,f))/2\big) \\ v_{wi(f,e)} &= \mathrm{sgn}\big(v_{i(f,e)}\big) \times \big(\bar{V}_i - (\beta\alpha_{ML_i}(f,e))/2\big) \\ v_{wi(f,g)} &= \mathrm{sgn}\big(v_{i(f,g)}\big) \times \big(\bar{V}_i + (\beta\alpha_{ML_i}(f,g))/2\big) \\ s_{wi(g,g)} &= 3 \times s_{i(e,e)} \end{aligned}}^{\text{If } e < g} \tag{9}$$

$$\overbrace{\begin{aligned} u_{wi(g,f)} &= \mathrm{sgn}\big(u_{i(g,f)}\big) \times \big(\bar{U}_i - (\beta\alpha_{ML_i}(g,f))/2\big) \\ u_{wi(e,f)} &= \mathrm{sgn}\big(u_{i(e,f)}\big) \times \big(\bar{U}_i + (\beta\alpha_{ML_i}(e,f))//2\big) \\ v_{wi(f,g)} &= \mathrm{sgn}\big(v_{i(f,g)}\big) \times \big(\bar{V}_i - (\beta\alpha_{ML_i}(f,g))//2\big) \\ v_{wi(f,e)} &= \mathrm{sgn}\big(v_{i(f,e)}\big) \times \big(\bar{V}_i + (\beta\alpha_{ML_i}(f,e))//2\big) \\ s_{wi(e,e)} &= 3 \times s_{i(g,g)} \end{aligned}}^{\text{If } e > g} \tag{10}$$

where

$$\mathrm{sgn}(x) = \begin{cases} -1, & \text{if} x < 0, \\ 0, & \text{if} x = 0, \\ 1, & \text{if} x > 0, \end{cases}$$

$$\bar{U}_i = \frac{|u_{i(e,f)} + u_{i(g,f)}|}{2}, \quad \bar{V}_i = \frac{|v_{i(f,e)} + v_{i(f,g)}|}{2}.$$

W_i represents the watermark bit, where $1 \leq i \leq MN/16$. In (7)–(10), β represents the threshold defining the amount of change in values, whereas, $u_{wi(e,f)}$, $u_{wi(g,f)}$, $v_{wi(f,e)}$, $v_{wi(f,g)}$, $s_{wi(e,e)}$, and $s_{wi(g,g)}$ represents the modified (watermark added) values at locations (e, f), (g, f), (f, e), (f, g), (e, e) and (g, g) respectively for block i. For (7) and (9) the key would be

$\mathbb{K}_i = \{f, e, g\}$ whereas in case of (8) and (10) key would be $\mathbb{K}_i = \{f, g, e\}$ for block i.

Remark 6: Modification in columns of U as compared to rows of U are less visible, likewise, in V the modification in rows are less visible as compared to changes in columns in V [4].

11. Let the modified blocks are formed as follows

$$\mathbb{A}_{wi} = U_{wi} S_{wi} V_{wi}^{\mathrm{T}}, \qquad i = 1, 2, \ldots pq, \tag{11}$$

where, the subscript 'w' is representing the modified (or watermark added) blocks.

12. The modified blocks $\mathbb{A}_{w1}, \mathbb{A}_{w2}, \ldots, \mathbb{A}_{wpq}$ are combined to form modified first principal component P_{rnw}, where

$$P_{rnw} = \begin{bmatrix} P_{rw_{11}} & P_{rw_{12}} & \ldots & P_{rw_{1N}} \\ P_{rw_{21}} & P_{rw_{22}} & \ldots & P_{rw_{2N}} \\ \vdots & \vdots & \ddots & \vdots \\ P_{rw_{M1}} & P_{rw_{M2}} & \ldots & P_{rw_{MN}} \end{bmatrix}.$$

13. The modified principal components are obtained as

$$P_w = \begin{bmatrix} P_{rw} \\ P_g \\ P_b \end{bmatrix}$$

where $\mathbf{P_{rw}}$ is a row vector, obtained from $\mathbf{P_{rnw}}$.

14. The matrix A_w is obtained as

$$A_w = Q P_w =$$

$$= \left[\begin{matrix} rw_{11} & \ldots & rw_{1N} & rw_{21} & \ldots \\ g_{11} & \ldots & g_{1N} & g_{21} & \ldots \\ b_{11} & \ldots & b_{1N} & b_{21} & \ldots \end{matrix} \right.$$

$$\left. \begin{matrix} \ldots & rw_{2N} & \ldots & rw_{M1} & \ldots rw_{MN} \\ \ldots & g_{2N} & \ldots & g_{M1} & \ldots g_{MN} \\ \ldots & b_{2N} & \ldots & b_{M1} & \ldots b_{MN} \end{matrix} \right].$$

15. Finally, R_W, G and B channels are combined to form the watermarked image I_w, where

$$R_W = \begin{bmatrix} rw_{11} & rw_{11} & \ldots & rw_{1N} \\ rw_{21} & rw_{22} & \ldots & rw_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ rw_{M1} & rw_{M2} & \ldots & rw_{MN} \end{bmatrix}.$$

3.2 Watermark Extraction

1. Let received watermarked image $\hat{I}_w$ be decomposed into its components $\hat{R}_w$, $\hat{G}$, and $\hat{B}$, where

$$\hat{R}_w = \begin{bmatrix} r\hat{w}_{11} & r\hat{w}_{12} & \ldots & r\hat{w}_{1N} \\ r\hat{w}_{21} & r\hat{w}_{22} & \ldots & r\hat{w}_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ r\hat{w}_{M1} & r\hat{w}_{M2} & \ldots & r\hat{w}_{MN} \end{bmatrix},$$

$$\hat{G} = \begin{bmatrix} \hat{g}_{11} & \hat{g}_{12} & \ldots & \hat{g}_{1N} \\ \hat{g}_{21} & \hat{g}_{22} & \ldots & \hat{g}_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{g}_{M1} & \hat{g}_{M2} & \ldots & \hat{g}_{MN} \end{bmatrix},$$

$$\hat{B} = \begin{bmatrix} \hat{b}_{11} & \hat{b}_{12} & \ldots & \hat{b}_{1N} \\ \hat{b}_{21} & \hat{b}_{22} & \ldots & \hat{b}_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{b}_{M1} & \hat{b}_{M2} & \ldots & \hat{b}_{MN} \end{bmatrix}.$$

2. Let a covariance matrix $\hat{C}$ be computed as

$$\hat{C} = \frac{1}{MN}(\hat{A}\hat{A}^{\mathrm{T}}) = \hat{Q}\hat{\wedge}\hat{Q}^{-1} \tag{12}$$

where

$$\hat{A} = \left[\begin{matrix} r\hat{w}_{11} & \ldots & r\hat{w}_{1N} & r\hat{w}_{21} & \ldots \\ \hat{g}_{11} & \ldots & \hat{g}_{1N} & \hat{g}_{21} & \ldots \\ \hat{b}_{11} & \ldots & \hat{b}_{1N} & \hat{b}_{21} & \ldots \end{matrix} \right.$$

$$\left. \begin{matrix} \ldots & r\hat{w}_{2N} & \ldots & r\hat{w}_{M1} & \ldots r\hat{w}_{MN} \\ \ldots & \hat{g}_{2N} & \ldots & \hat{g}_{M1} & \ldots \hat{g}_{MN} \\ \ldots & \hat{b}_{2N} & \ldots & \hat{b}_{M1} & \ldots \hat{b}_{MN} \end{matrix} \right].$$

$$\hat{Q} = \begin{bmatrix} \hat{q}_{11} & \hat{q}_{12} & \hat{q}_{13} \\ \hat{q}_{21} & \hat{q}_{32} & \hat{q}_{33} \\ \hat{q}_{31} & \hat{q}_{32} & \hat{q}_{33} \end{bmatrix}, \qquad \hat{\wedge} = \begin{bmatrix} \hat{\lambda}_{11} & 0 & 0 \\ 0 & \hat{\lambda}_{22} & 0 \\ 0 & 0 & \hat{\lambda}_{33} \end{bmatrix},$$

$\hat{\lambda}_{11} \geq \hat{\lambda}_{22} \geq \hat{\lambda}_{33}$ are eigenvalues in descending order.

3. The principal components of covariance matrix $\hat{C}$ are calculated as

$$\hat{P}_w = \begin{bmatrix} \hat{P}_{rw} \\ \hat{P}_g \\ \hat{P}_b \end{bmatrix} = \hat{Q}^{\mathrm{T}}\hat{A} =$$

$$= \left[\begin{matrix} \hat{P}_{rw_{11}} & \ldots & \hat{P}_{rw_{1N}} & \hat{P}_{rw_{21}} & \ldots \\ \hat{P}_{g_{11}} & \ldots & \hat{P}_{g_{1N}} & \hat{P}_{g_{21}} & \ldots \\ \hat{P}_{b_{11}} & \ldots & \hat{P}_{b_{1N}} & \hat{P}_{b_{21}} & \ldots \end{matrix} \right.$$

$$\left. \begin{matrix} \ldots & \hat{P}_{rw_{2N}} & \ldots & \hat{P}_{rw_{M1}} & \ldots & \hat{P}_{rw_{MN}} \\ \ldots & \hat{P}_{g_{2N}} & \ldots & \hat{P}_{g_{M1}} & \ldots & \hat{P}_{g_{MN}} \\ \ldots & \hat{P}_{b_{2N}} & \ldots & \hat{P}_{b_{M1}} & \ldots & \hat{P}_{b_{MN}} \end{matrix} \right].$$

4. Let matrix $\hat{\mathbf{P}}_{\mathbf{rnw}}$ is obtained by converting row vector $\mathbf{P_{rw}}$ into a matrix of size $M \times N$ as shown below

$$\hat{P}_{rnw} = \begin{bmatrix} \hat{P}_{rw_{11}} & \hat{P}_{rw_{12}} & \ldots & \hat{P}_{rw_{1N}} \\ \hat{P}_{rw_{21}} & \hat{P}_{rw_{22}} & \ldots & \hat{P}_{rw_{2N}} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{P}_{rw_{M1}} & \hat{P}_{rw_{M2}} & \ldots & \hat{P}_{rw_{MN}} \end{bmatrix}.$$

5. The $\hat{\mathbf{P}}_{\mathbf{rnw}}$ is divided into non-overlapping blocks $\hat{\mathbb{A}}_{w1}, \hat{\mathbb{A}}_{w2}, \ldots \hat{\mathbb{A}}_{wpq}$, each of size 4×4. Using SVD, each block is decomposed as follows:

$$\hat{A}_{wi} = \hat{U}_{wi}\hat{S}_{wi}\hat{V}_{wi}^{\mathrm{T}}, \quad i = 1, 2, \ldots, pq. \tag{13}$$

6. Based on keys: $\mathbb{K}_i = \{k_1, k_2, k_3\}$, the watermarking bits are extracted as follows:

$$\xi = \begin{cases} 1, & \text{if} \quad \hat{u}_{wi(k_2,K_1)} \leq \hat{u}_{wi(k_3,K_1)}, \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

$$\zeta = \begin{cases} 1, & \text{if} \quad \hat{v}_{wi(k_1,K_2)} \leq \hat{v}_{wi(k_1,K_3)}, \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

$$\psi = \begin{cases} 1, & \text{if} \quad \hat{s}_{wi(k_2,K_2)} \leq \hat{s}_{wi(k_3,K_3)}, \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

Once three values ξ, ζ, and ψ are calculated for each block, then watermarking bits are extracted as follows.

$$\hat{W}_i = \begin{cases} \psi, & \text{if} \quad (\xi = \psi) \vee (\zeta = \psi), \\ \vartheta, & \text{otherwise} \end{cases} \tag{17}$$

where

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

4. Proposed Scheme 2

The only difference in proposed scheme 1 and 2 is that, in scheme 2 neither HVS nor FIS used to find adaptive factor α_{M_L} for watermark embedding. Instead only constant scaling factor β having values from 0.1 to 0.9 with a step size of 0.2 is used. The watermark embedding and extraction procedure are described in following sections.

4.1 Watermark Embedding

Eliminating step 8 and step 9, and the terms $\alpha_{M L_i}(g, f)$, $\alpha_{M L_i}(e, f)$, $\alpha_{M L_i}(f, g)$ and $\alpha_{M L_i}(f, e)$ from (7)–(10) of Sec. 3.1 will reduce to watermark embedding procedure of proposed scheme 2.

4.2 Watermark Extraction

The watermark extraction procedure of proposed scheme 2 is same as of proposed scheme 1 which is described in Sec. 3.2.

5. Experimental Results

In order to test the performance of proposed schemes a number of experiments were performed. For this purpose six different images shown in Fig. 3, each of size 512×512 were used as host images. Whereas for watermark a binary image shown in Fig. 4(a) of size 64×64 was used. The performance of proposed schemes is evaluated in terms of imperceptibility, robustness, security and capacity, which are discussed in following sections.

5.1 Imperceptibility

To end user the original and watermarked image should look similar, in other words, there should be no visible difference between original and watermarked images [3], this is referred as imperceptibility. For qualitative analysis watermarked images are shown in Fig. 3, whereas, for quantitative evaluation Peak-Signal-to-Noise-Ration (PSNR) [7] shown in (18) is used to measure imperceptibility. The PSNR for proposed scheme 1 for different images and for distinct constant scaling factor is shown in Tab. 1. The use of constant scaling factor here is only for reference, otherwise, proposed scheme 1 performs well without constant scaling factor. The watermarked images are shown for proposed scheme 1, however, the watermarked images obtained from proposed scheme 2 also have good perceptual quality.

$$PSNR(\text{dB}) = 10 \log_{10}\left(\frac{G^2}{H}\right) \tag{18}$$

where

$$G = \max\{I(m,n) : 1 \leq m \leq M, 1 \leq n \leq N\},$$

$$H = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} (I(m,n) - I_w(m,n))^2.$$

Images	**Constant Scaling Factor** (β)				
	0.1	**0.3**	**0.5**	**0.7**	**0.9**
Lena	57.2311	56.5784	55.9255	55.2696	54.6518
Baboon	46.7905	46.5187	46.2263	45.9465	45.6602
Autumn	55.6855	53.8721	51.8756	50.1673	48.5929
Airplane	55.0401	54.4737	53.9122	53.3167	52.7232
Peppers	59.5511	58.4239	57.2720	56.1712	55.0926
Crane	54.5905	54.1370	53.6779	53.2249	52.7693

Tab. 1. PSNR for different values of scaling factors (Proposed scheme 1).

The proposed schemes are compared with state-of-the-art schemes in terms of PSNR as shown in Tab. 2. It is clearly visible that both proposed schemes performs well with the compared techniques in terms of PSNR. However, the proposed scheme 1 outperforms proposed scheme 2 in terms of imperceptibility, and that is due to the use of HVS and FIS to find adaptive scaling factors.

Images	**For Constant Scaling Factor** $\beta = 0.5$					
	Proposed		Presented in			
	1	2	[6]	[3]	[13]	[14]
Lena	55.9255	42.0455	38.7070	36.1329	38.9620	34.3263
Baboon	46.2263	37.3587	30.2003	27.5918	33.0635	27.3159
Autumn	51.8756	41.7374	37.9715	35.0159	36.0157	33.6153
Airplane	53.9122	39.9456	38.8983	35.4927	37.3391	34.7828
Peppers	57.2720	39.6113	38.6906	34.2894	38.8031	33.2607
Crane	53.6779	45.7264	44.9576	38.5728	40.0731	37.0299

Tab. 2. PSNR for different techniques.

Generally the quality of watermarked images can either be evaluated qualitatively or qualitatively. For qualitative evaluation of proposed scheme both original and watermarked images are shown in Fig. 3. For quantitative measurement, PSNR shown in (18) is used, the results and comparision are shown in Tab. 1 and Tab. 2 respectively. However, PSNR is not only the metric to measure the quality of watermarked images, Structural Similarity Index (SSIM), Visual

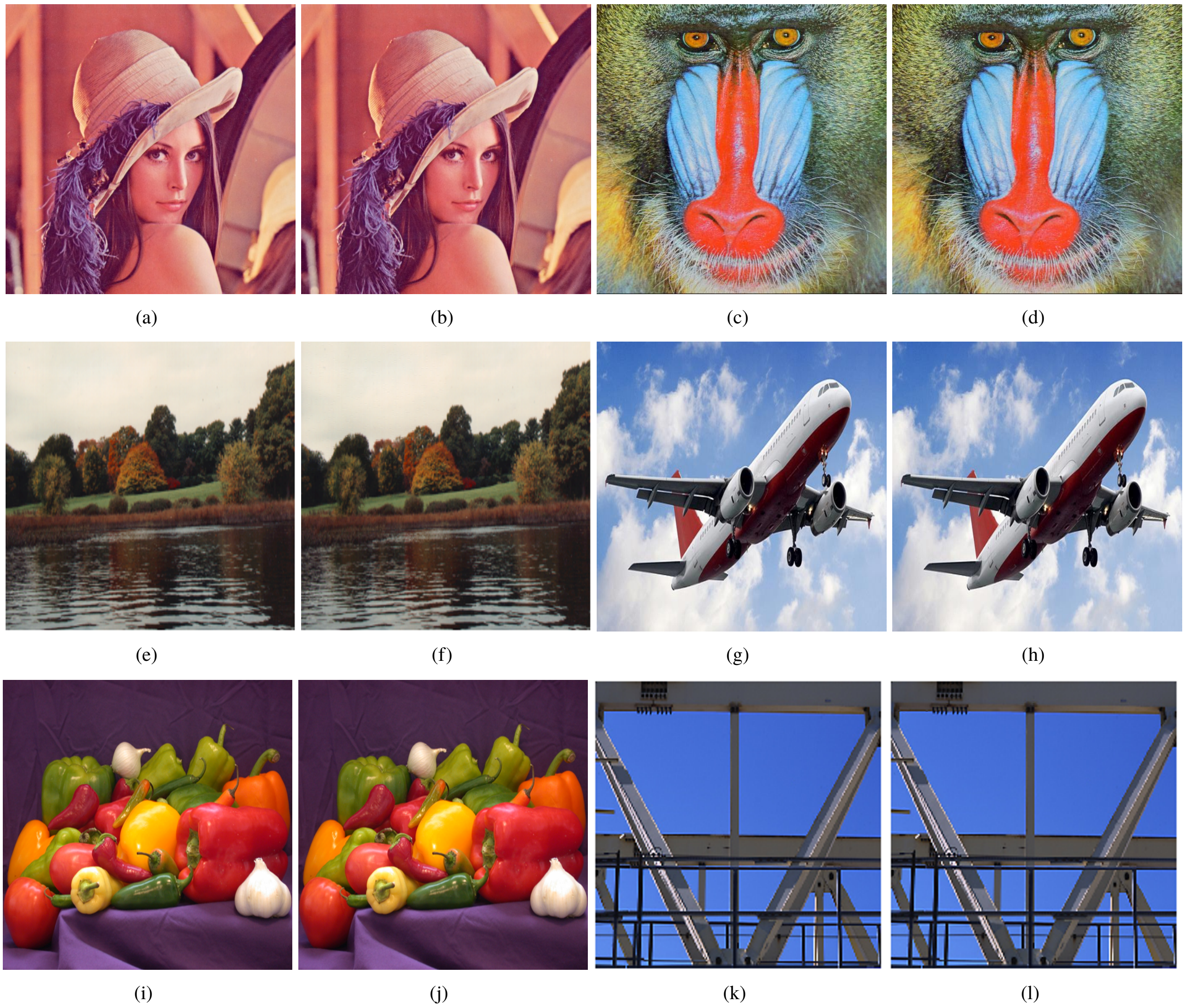


Fig. 3. Host and watermarked images (512×512) for proposed scheme 1 (β = 0.5) (a). Lena (original), (b). Lena (watermarked) (c). Baboon (original) (d). Baboon (watermarked) (e). Autumn (original) (f). Autumn (watermarked) (g). Airplane (original) (h). Airplane (watermarked) (i). Peppers (original) (j). Peppers (watermarked) (k). Crane (original) (l). Crane (watermarked).

Information Fidelity (VIF) and Normalized Color Difference (NCD) also used to examine the quality of watermarked images, quantitatively. Therefore, in this paper in addition to PSNR, SSIM, VIF and NCD are also utilized for evaluation [3]. SSIM [19] utilizes luminance ($\mathcal{L}$), contrast (C) and structural information ($\mathcal{S}$) to find the distortion introduced in watermarked images. Given original I and watermarked I_w images, the SSIM can be calculated using (19).

$$SSIM(I, Iw) = \mathcal{L}(I, I_w)^{\gamma_{\mathcal{L}}} \times \mathcal{S}(I, I_w)^{\gamma_{\mathcal{S}}} \times C(I, I_w)^{\gamma_C} \quad (19)$$

where $\gamma_{\mathcal{L}} > 0$, $\gamma_{\mathcal{L}} > 0$ and $\gamma_{\mathcal{L}} > 0$, are constant used to describe the dependency of each component. For equal contribution of $\mathcal{L}$, $\mathcal{S}$ and C in the calculation of SSIM, $\gamma_{\mathcal{L}} = \gamma_{\mathcal{S}} = \gamma_C = 1$ are set equal to 1. The $\mathcal{L}$, C and $\mathcal{S}$ defined in (19) are calculated as follows.

$$\mathcal{L}(I, I_w) = \frac{2\mu_I \mu_{I_w} + C_1}{\mu_I^2 + \mu_{I_w}^2 + C_1}, \; C(I, I_w) = \frac{2\rho_I \rho_{I_w} + C_2}{\rho_I^2 + \rho_{I_w}^2 + C_2},$$
$$\mathcal{S}(I, I_w) = \frac{\rho_{II_w} + C_3}{\rho_I^2 \rho_{I_w}^2 + C_3} \quad (20)$$

where μ_I, μ_{I_w}, ρ_I and ρ_{I_w} denotes the mean and covariance of host and watermarked images respectively. C_1, C_2 and C_3 are small constants used to avoid the situations where the sum of means or covariances can be zero. Using (20) and setting $C_3 = C_2/2$ in (19), will result in the form of equation shown below

$$SSIM = \frac{(2\mu_I \mu_{I_w} + C_1) \times (2\rho_I \rho_{I_w} + C_2)}{(2\mu_I^2 + \mu_{I_w}^2 + C_1) \times (2\rho_I^2 + \rho_{I_w}^2 + C_2)}. \quad (21)$$

Images	For Constant Scaling Factor $\beta = 0.5$					
	Proposed		Presented in			
	1	2	[6]	[3]	[13]	[14]
Lena	0.9580	0.9088	0.8366	0.7810	0.8422	0.6881
Baboon	0.9118	0.8796	0.7911	0.7228	0.8661	0.5972
Autumn	0.9439	0.9279	0.8442	0.7785	0.8007	0.7266
Airplane	0.9428	0.8921	0.8687	0.7926	0.8338	0.7383
Peppers	0.9653	0.9130	0.8918	0.7904	0.8944	0.6775
Crane	0.9259	0.9033	0.8574	0.7356	0.7642	0.6797

Tab. 3. SSIM for different techniques.

The comparision of proposed schemes with existing techniques in terms of SSIM shown in Tab. 3, clearly demonstrates the improvement of proposed schemes over present watermarking techniques.

VIF [20] introduced in 2006 is also used to asses the quality of images. In this paper VIF shown in (22), is also used to examine the quality of watermarked images with respect to original host images

$$VIF = \frac{\sum_{j \in \text{channels}} \mathbb{I}(\overrightarrow{C}^{N,j}, \overrightarrow{I}^{N,j} | s^{N,j})}{\sum_{j \in \text{channels}} \mathbb{I}(\overrightarrow{C}^{N,j}, \overrightarrow{I_w}^{N,j} | s^{N,j})} \tag{22}$$

where $\mathbb{I}(\overrightarrow{C}^{N,j}, \overrightarrow{I}^{N,j}|s)$ and $\mathbb{I}(\overrightarrow{C}^{N,j}, \overrightarrow{I}^{N,j}|s)$ represent the information that a brain can extract from images using HVS of original and watermarked images respectively, $\overrightarrow{C}^{N,j}$ represents the N elements of random field C_j for $j - th$ sub-band. For detailed description of parameters and calculation of information $\mathbb{I}$ from host and watermarked images, [20] can be referred.

The comparison in terms of VIF of proposed schemes with that of state-of-the-art techniques is shown in Tab. 4. The better visual quality of watermarked images obtained from proposed schemes is clearly visible from the results shown in Tab. 4.

Finally, NCD [3] shown in (23), is also used to evaluate the quality of watermarked images.

$$NCD = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{(\mathcal{L}(i,j) - \mathcal{L}_w(i,j))^2 + (a(i,j) - a_w(i,j))^2 + (b(i,j) - b_w(i,j))^2}}{\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{(\mathcal{L}(i,j))^2 + (a(i,j))^2 + (b(i,j))^2}} \tag{23}$$

where $\mathcal{L}$ represents the luminance, a and b denote the chrominance. It should be noted that in order to calculate NCD, the RGB color model must be converted to Lab color space. The performance of proposed scheme is calculated in terms of NCD and compared with existing schemes as shown in Tab. 5.

Images	For Constant Scaling Factor $\beta = 0.5$					
	Proposed		Presented in			
	1	2	[6]	[3]	[13]	[14]
Lena	0.8959	0.8423	0.7954	0.7425	0.8006	0.7053
Baboon	0.8584	0.8154	0.7592	0.6936	0.7811	0.6866
Autumn	0.8764	0.8282	0.7535	0.6948	0.7146	0.6670
Airplane	0.8886	0.8343	0.8124	0.7413	0.7799	0.7265
Peppers	0.9138	0.8779	0.8575	0.7600	0.8600	0.7372
Crane	0.8805	0.8548	0.8404	0.7210	0.7490	0.6921

Tab. 4. VIF for different techniques.

Images	For Constant Scaling Factor $\beta = 0.5$					
	Proposed		Presented in			
	1	2	[6]	[3]	[13]	[14]
Lena	0.0233	0.0408	0.0784	0.1516	0.0619	0.1164
Baboon	0.0716	0.1295	0.2342	0.4482	0.1889	0.3450
Autumn	0.0579	0.1045	0.1996	0.3837	0.2110	0.4079
Airplane	0.0209	0.0364	0.0718	0.1373	0.0671	0.1296
Peppers	0.0448	0.0758	0.1498	0.2826	0.0972	0.1805
Crane	0.0268	0.0496	0.0984	0.1828	0.0871	0.1676

Tab. 5. NCD for different techniques.

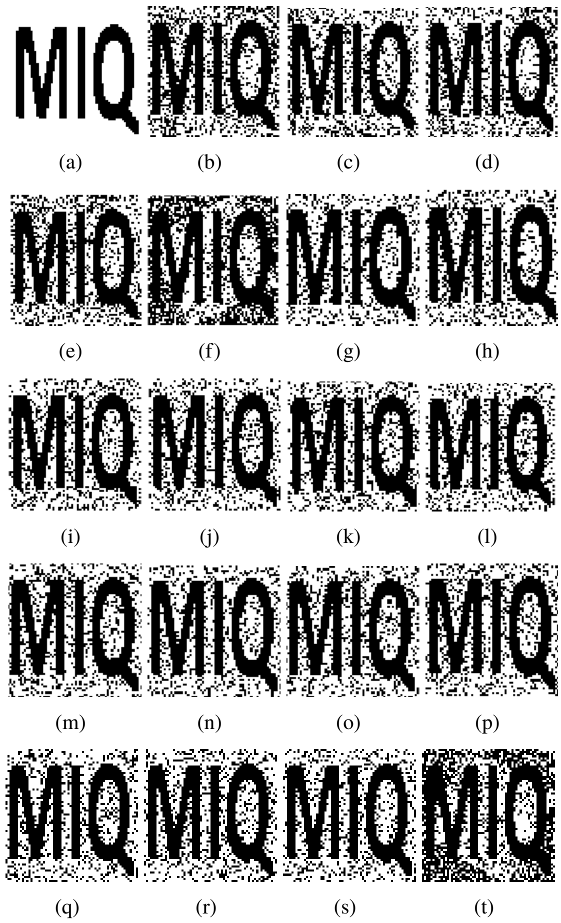


Fig. 4. Extracted watermarks from attacked watermarked images (proposed scheme 1 ($\beta = 0.5$)): (a) Original watermark (b) RO, (c) TR, (d) XSH, (e) YSH, (f) AFT, (g). SC, (h) CR, (i). GN, (j) S&P (k) SN, (l) MB, (m) SB, (n) AF, (o) HE, (p) JQ (q) JQ+AF, (r) JQ+GN, (s) JQ+SC (t) RO+SC.

5.2 Robustness

Robustness refers to the ability of watermarking scheme to withstand against intentional or unintentional attacks, that may be applied on watermarked images either to remove or to destroy the hidden information [7], [21]. Robustness is measured using normalized correlation [6] shown in (24). In order to check the robustness of proposed schemes different attacks like rotation (RO), translation (TR), x-shearing (XSH), y-shearing (YSH), scaling (SC), cropping (CR), affine transformation (AFT), Gaussian noise (GN), salt & pepper noise

Attacks		Constant Scaling Factor (β)				
Attack	**Parameters**	**0.1**	**0.3**	**0.5**	**0.7**	**0.9**
Rotation	$\theta = 45$	0.8031	0.7283	0.8229	0.8211	0.7286
	$\theta = 60$	0.8258	0.8279	0.8103	0.8098	0.8112
	$\theta = 125$	0.8272	0.8064	0.8068	0.8064	0.8066
Translation	displacement 60%	0.8142	0.8135	0.8135	0.8596	0.8117
	displacement 120%	0.8089	0.7444	0.7444	0.8084	0.7441
X-Shearing	Shearing Factor=0.4	0.7998	0.7987	0.8466	0.7982	0.8466
	Shearing Factor=-0.5	0.7989	0.7996	0.8466	0.8488	0.7980
Y-Shearing	Shearing Factor=-0.4	0.8488	0.8322	0.7873	0.7899	0.8455
	Shearing Factor=0.5	0.7715	0.8413	0.8418	0.7722	0.7717
Affine Transformation	Transform Factor=0.5	0.7563	0.7551	0.7558	0.8188	0.7556
Scaling	3times	0.8712	0.8695	0.8693	0.8682	0.8693
	0.5times	0.8792	0.8800	0.8796	0.8787	0.8783
Cropping	10%	0.8676	0.8682	0.8678	0.8676	0.8674
	25%	0.8646	0.8646	0.8648	0.8641	0.8646
Gaussian Noise	$\mu = 0.4, \sigma^2 = .01$	0.8654	0.8635	0.8659	0.8678	0.8643
	$\mu = 0.5, \sigma^2 = 0.5$	0.8641	0.8563	0.8587	0.8663	0.8700
Salt & Pepper Noise	Density=0.1	0.8652	0.8633	0.8704	0.8654	0.8691
	Density=0.5	0.8609	0.8650	0.8704	0.8652	0.8609
Speckle Noise	Density=0.1	0.8725	0.8689	0.8667	0.8689	0.8732
	Density=0.5	0.8695	0.8738	0.8585	0.8567	0.8598
Blurring	Motion Blurring	0.8678	0.8687	0.8689	0.8700	0.8691
	Simple Blurring	0.8719	0.8721	0.8715	0.8706	0.8704
	5×5	0.8836	0.8834	0.8834	0.8830	0.8836
Average Filtering	7×7	0.8757	0.8747	0.8730	0.8727	0.8738
Histogram Equalization		0.8661	0.8667	0.8665	0.8665	0.8663
JPEG Compression	Quality Factor=50	0.8611	0.8624	0.8617	0.8617	0.8600
Combined Watermarking Attacks	JPEG Comp+Filtering(5×5)	0.8745	0.8753	0.8762	0.8751	0.8747
	JPEG Comp + Gaussian Noise (0.5)	0.8643	0.8730	0.8680	0.8723	0.8736
	JPEG Comp + Scaling (Half)	0.8811	0.8813	0.8804	0.8811	0.8800
	Translation+Shearing	0.8429	0.8493	0.8521	0.8623	0.8670
	Rotation($45°$)+ scaling	0.8133	0.8084	0.7479	0.7471	0.8270

Tab. 6. NC For Different Attacks (Proposed Scheme 1).

(S&P), speckle noise (SN), motion blurring (MB), simple blurring (SB), average filtering (AF), histogram equalization (HE) and JPEG compression (JQ) were applied on watermarked image. In addition to conventional watermarking attacks, combined attacks are formed by combining two or more conventional attacks. For instance, watermark is tried to be extracted form a watermarked images that has been subjected to JPEG compression and filtering attack. In this way five additional attacks – JPEG compression plus filtering (JQ+AF), JPEG compression plus Gaussian noise (JQ+GN), JPEG compression plus scaling (JQ+SC), translation plus x and y shearing (TR+SH), and rotation plus scaling (RO+SC) – are also used to check robustness of proposed schemes

$$NC = \frac{\sum_{p=1}^{P}\sum_{q=1}^{Q}\left(W(p,q)\times\hat{W}(p,q)\right)}{\sqrt{\sum_{p=1}^{P}\sum_{q=1}^{Q}W^2(p,q)}\times\sqrt{\sum_{p=1}^{P}\sum_{q=1}^{Q}\hat{W}^2(p,q)}}. \quad (24)$$

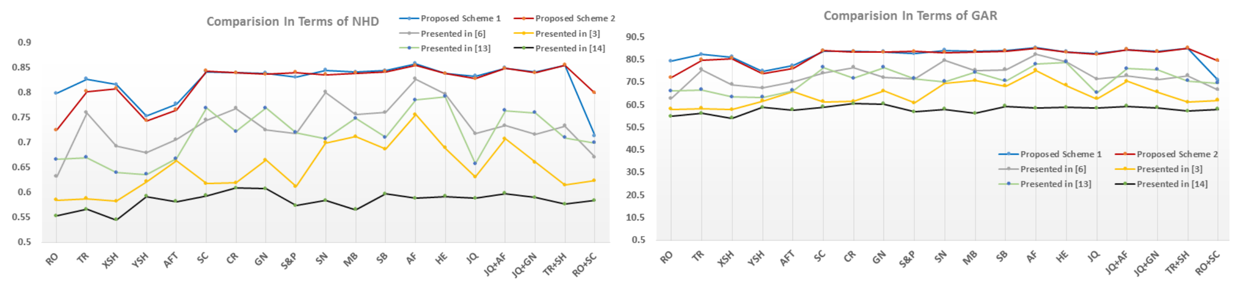
For qualitative assessment of extracted watermarks after applying above mentioned attacks on watermarked image, Fig. 7 can be referred. It can be seen that in all cases the extracted watermarks are clearly visible hence can be used to prove ownership. The performance of proposed scheme 1 in terms of robustness for different scaling factors is shown in Tab. 6. In general with increasing scaling factor the robustness is increased [3], whereas, the change in NC values shown in Tab. 6, is random and that is due to the adaptive scaling factor (α_{ML}).

The comparison of proposed schemes in terms of NC with existing technique [3], [6], [13] and [14] is shown in Tab. 7.

Robustness of watermarking techniques are also measured using Bit Error Rate (BER) [3], shown in (25). The comparision of proposed schemes in terms of BER with [3], [6], [13] and [14] is shown in Tab. 8. From Tab. 7 and Tab. 8, it is clear that the proposed schemes give better results in terms of robustness as well.

$$BER = \frac{\text{Number of wrong bits extracted}}{\text{Total number of bits embedded}}. \quad (25)$$

The extracted watermarks shown in Fig. 4 are for proposed scheme 1, however, the quality of watermarks obtained using proposed scheme 2 is also good. This can be seen from Tab. 7 that there is not significant difference between NC



(a) (b)

Fig. 5. Comparison of proposed schemes with existing techniques (a). Comparison in terms of NHD (b). Comparison in terms of GAR.

Attacks	For Constant Scaling Factor $\beta = 0.5$					
	Proposed Schemes		Presented in			
	1	2	[6]	[3]	[13]	[14]
RO	0.8229	0.8036	0.5894	0.5377	0.6274	0.5218
TR	0.8135	0.8529	0.5946	0.5182	0.6056	0.5593
XSH	0.8466	0.8384	0.6148	0.5002	0.6633	0.5442
YSH	0.8418	0.8453	0.6582	0.4788	0.6779	0.6278
AFT	0.7558	0.8060	0.6376	0.4885	0.7029	0.5385
SC	0.8796	0.8672	0.7664	0.6356	0.7909	0.5386
CR	0.8648	0.8570	0.6825	0.6322	0.7370	0.6216
GN	0.8659	0.8583	0.7438	0.5797	0.7896	0.5823
S&P	0.8704	0.8656	0.7406	0.5270	0.7420	0.5436
SN	0.8667	0.8716	0.7304	0.6247	0.7375	0.5565
MB	0.8689	0.8716	0.7859	0.6355	0.7772	0.5873
SB	0.8715	0.8665	0.7824	0.6555	0.7312	0.5527
AF	0.8834	0.8073	0.7811	0.6577	0.7417	0.5562
HE	0.8665	0.7929	0.7539	0.5576	0.7493	0.5601
JQ	0.8617	0.8639	0.7488	0.5538	0.6861	0.5621
JQ+AF	0.8762	0.8753	0.7568	0.5234	0.7882	0.5343
JQ+GN	0.8680	0.8643	0.7375	0.5769	0.7822	0.5870
JQ+SC	0.8804	0.8813	0.7554	0.5305	0.7316	0.5425
TR+SH	0.8521	0.8475	0.7058	0.5028	0.7238	0.5123
RO+SC	0.7479	0.8308	0.6973	0.5028	0.7276	0.5348

Tab. 7. NC for different techniques.

values of both proposed schemes. The recognizable watermarks can be extracted as long as the distorted watermarked image are visually identifiable.

Besides NC and BER, there are other ways to calculate the credibility of extracted watermarks quantitatively. For instance, Normalized Hamming Distance (NHD) [6] shown in 26, where, w and $\hat{w}$ represent embedded and extracted watermark respectively, can be used to calculate the similarity (or difference) between embedded and extracted watermarks.

$$H_{\mathrm{D}} = \frac{\sum_{1=1}^{m} \sum_{j=1}^{n} h_{w\hat{w}}(i, j)}{m \times n} \tag{26}$$

where

$$h_{w\hat{w}}(i, j) = \begin{cases} 1, & \text{if} \quad w(i, j) = \hat{w}(i, j), \\ 0, & \text{otherwise.} \end{cases}$$

Attacks	For Constant Scaling Factor $\beta = 0.5$					
	Proposed Schemes		Presented in			
	1	2	[6]	[3]	[13]	[14]
RO	0.2107	0.2256	0.2360	0.3679	0.3153	0.3791
TR	0.1792	0.1736	0.1907	0.2933	0.2510	0.2717
XSH	0.1848	0.1892	0.2268	0.2951	0.2225	0.2712
YSH	0.1902	0.1819	0.2965	0.2984	0.2108	0.2276
AFT	0.2798	0.2231	0.2577	0.3570	0.2481	0.3239
SC	0.1477	0.1580	0.1939	0.2738	0.2200	0.3231
CR	0.1611	0.1692	0.1920	0.2799	0.2401	0.2847
GN	0.1672	0.1677	0.1829	0.2801	0.2056	0.2788
S&P	0.1582	0.1597	0.1454	0.2798	0.1987	0.2713
SN	0.1660	0.1531	0.1825	0.2857	0.2420	0.3207
MB	0.1599	0.1531	0.1833	0.2769	0.2264	0.2996
SB	0.1570	0.1587	0.1761	0.2758	0.2472	0.3271
AF	0.1433	0.1477	0.1652	0.2601	0.2306	0.3076
HE	0.1626	0.2517	0.1130	0.2769	0.2061	0.2757
JQ	0.1680	0.1616	0.2064	0.2760	0.2228	0.2719
JQ+AF	0.1516	0.1526	0.1985	0.2864	0.2318	0.2945
JQ+GN	0.1609	0.1650	0.2053	0.2356	0.2514	0.2718
JQ+SC	0.1467	0.1458	0.1856	0.2281	0.2346	0.2815
TR+SH	0.1656	0.1715	0.1983	0.2459	0.2287	0.2568
RO+SC	0.1876	0.2021	0.2598	0.2983	0.2795	0.3143

Tab. 8. BER for different techniques.

Similarly, Global Authentication Rate (GAR) [22] shown in (27) is also used to check the quality of extracted watermark. It should be noted that GAR and NHD are almost same just different form of representations

$$\varrho^{\mathrm{GAR}} = \left(1 - \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(w(i, j) \oplus \hat{w}(i, j)\right)\right) \times 100\,\%. \tag{27}$$

The performance of proposed schemes is examined using both NHD and GAR in terms of robustness and also compared with other watermark techniques.

The comparision of proposed and existing watermarking schemes in terms of NHD is shown in Fig. 5(a) and in terms of GAR in Fig. 5(b). Both figures clearly demonstrate the improvement of proposed scheme over existing watermarking techniques.

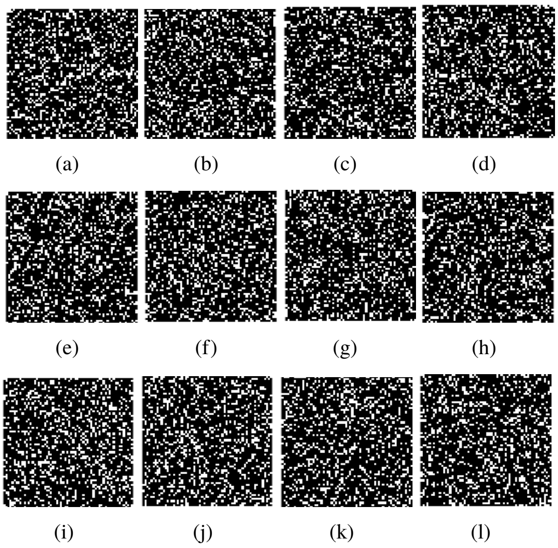


Fig. 6. Extracted watermarks with fake keys (proposed scheme 1).

5.3 Security

Security refers to the resistance against false positive or true negative extraction of watermark [5]. In designing the proposed schemes security is given high importance and it was ensured to nullify the chances of false positive or true negative detection or extraction of hidden information. To test the security ample number of fake keys were used to extract the watermark neither true nor false watermark was extracted. In Fig. 6 the extracted watermarks with false keys are shown. It is evident that no watermark was extracted.

5.4 Capacity

Capacity refers to the amount of data that can be embedded into the host image without degrading the quality of watermarked image. The capacity of proposed schemes is $(64 \times 64 \times 3 = 12288)$, since watermark of size 64×64, and all three components (U, S and V) of SVD decomposition are used. This is considered to be good capacity for a watermarking scheme. The capacities of proposed schemes are 3 times more than the capacities of [3] and [6].

6. Conclusion

In this paper, two watermarking schemes are proposed. In order to achieve four conflicting requirements for a good watermarking scheme, HVS, FIS, PCA and SVD are used together. The perceptual quality is improved by using PCA to decorrelate the three channels of color image, afterwards HVS and FIS are used to find adaptive scaling factor so that the amount of information embedded is subject to the acceptability of host image. For instance, the areas which are less prone to modifications are modified to lesser extent as compared to areas which are open to changes. In this way imperceptibility is further improved, and can be seen from results that the imperceptibility of proposed scheme 1 is much better than proposed scheme 2 (HVS and FIS are not employed in proposed scheme 2, otherwise it is same as proposed scheme 1). To achieve robustness, SVD is used, as changes in singular values does not change the image and vice versa. Whereas to obtain security, based on correlation certain elements from SVD components are selected for modification, and then those locations served as key at the time of watermark extraction. In this way not only security and capacity are achieved but this method also helped to improve the imperceptibility as suggested by results. The proposed schemes are compared with state-of-the-art watermarking techniques and obtained better results.

References

[1] TSUI, K. T., ZHANG, P. X., ANDROUTSOS, D. Color image watermarking using multidimensional Fourier transforms. *IEEE Transactions on Information Forensics and Security*, 2008, vol. 3, no. 1, p. 1556–6013. DOI: 10.1109/TIFS.2007.916275

[2] CHOU, H. C., LIU, C. K. A perceptually tuned watermarking scheme for color images. *IEEE Trans. on Image Processing*, 2010, vol. 19, no. 11, p. 2966–2982. DOI: 10.1109/TIP.2010.2052261

[3] CEDILLO-HERNANDEZ, M. CEDILLO-HERNANDEZ, A. GARCIA-UGALDE, F., et. al. Copyright protection of color imaging using robust-encoded watermarking. *Radioengineering*, 2015, vol. 24, no. 1, p. 240–251. DOI: 10.13164/re.2015.0240

[4] SU, Q., NIU, Y., ZOU, H., et el. A blind dual color image watermarking based on singular value decomposition. *International Journal of Applied Mathematics and Computation*, 2013, vol. 219, no. 16, p. 8455–8466. DOI: 10.1016/j.amc.2013.03.013

[5] MAKBOOL, N. M., KHOO, E. B. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *International Journal of Digital Signal Processing*, 2014, vol. 33, p. 134–147. DOI: 10.1016/j.dsp.2014.06.012

[6] PRATHAP, I., NATARAJAN, V., ANITHA, R. Hybrid robust watermarking for color images. *International Journal of Computers & Electrical Engineering*, 2014, vol. 14, no. 3, p. 920–930. DOI: 10.1016/j.compeleceng.2014.01.006

[7] GHAFOOR, A., IMRAN, M. A non-blind color image watermarking scheme resistant against geometric attacks. *Radioengineering*, 2012, vol. 21, no. 4, p. 1246–1251. ISSN: 1805-9600

[8] BAISA, L., GUNJAL, MALI, N. S. Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces. *International Journal of Computer Theory and Engineering*, 2011, vol. 3, no. 6, p. 714–717.

[9] SUN, X., BO, S. A blind digital watermarking for color medical images based on PCA. In *Proceedings of the IEEE International Conference on Wireless Communications, Networking, and Information Security (WCNIS)*. Beijing (China), 2010, p. 421–427. DOI: 10.1109/WCINS.2010.5541812

[10] LIU, R., TAN, T. An SVD based watermarking scheme for protecting rightful information. *IEEE Transactions on Multimedia*, 2002, vol. 4, no. 1, p. 121–128. DOI: 10.1109/6046.985560

[11] LAI, C. C., TAI, C. C. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 2010, vol. 59, no. 11, p. 3060–3063. DOI: 10.1109/TIM.2010.2066770

[12] LAI, C. C. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *International Journal of Digital Signal Processing*, 2011, vol. 21, no. 4, p. 522–527. DOI: 10.1016/j.dsp.2011.01.017

[13] FAZLI, S., MOEINIi, M. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *International Journal of Optik*, 2016, vol. 127, no. 2, p. 964–972. DOI: 10.1016/j.ijleo.2015.09.205

[14] ROY, A., MAITI, K. A., GHOSH, K. A perception based color image adaptive watermarking scheme in YCbCr space. In *Proceedings of the IEEE International Conference on Signal Processing and Integrated Networks*. 2015, p. 537–543. DOI: 10.1109/SPIN.2015.7095399

[15] QI, H., ZHENG, D., ZHAO, J. Human visual system based adaptive digital image watermarking. *International Journal of Signal Processing*, 2008, vol. 88, no. 1, p. 174–188. DOI: 10.1016/j.sigpro.2007.07.020

[16] GOU, J. M., PRASETYO, H. A novel gray-scale image watermarking using hybrid fuzzy-BPN architecture. *International Journal of Visual Communication and Image Representation*, 2014, vol. 25, no. 5, p. 1149–1163. DOI: 10.1016/j.eij.2015.01.002

[17] WANG, X., L. *A Course in Fuzzy Systems and Control*. 1st ed., USA: Prentice Hall, 1997. ISBN: 978-0135408827

[18] JOLLIFFE, T. I. *Principal Component Analysis*. 2nd ed., USA: Springer, 2002. ISBN: 978-0-387-22440-4

[19] WANG, Z. BOVIK, C. A., SHEIKH, R. H., et al. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 2004, vol. 13, no. 4, p. 600–612. DOI: 10.1109/TIP.2003.819861

[20] SHEIKH, R. H., BOVIK, C. A. T. S. Image information and visual quality. *IEEE Transactions on Image Processing*, 2006, vol. 15, no. 2, p. 430–444. DOI: 10.1109/TIP.2005.859378

[21] LEVICKY. D., FORIS, P. Human visual system models in digital image watermarking. *Radioengineering*, 2004, vol. 13, no. 4, p. 28–43. ISSN: 1805-9600

[22] LIE, N. W., LIN, S. G., CHENG, L. S. Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques. *IEEE Transactions on Information Forensics and Security*, 2006, vol. 1, no. 3, p. 330–341. DOI: 10.1109/TIFS.2006.879297

About the Authors . . .

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 Education Societies.