A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD

by Musrrat Ali, Chang Wook Ahn, Millie Pant, and Patrick Siarry from *Discrete Dynamics in*

Nature and Society is available under a Creative Commons Attribution 4.0 International license. ©

2016, Musrrat Ali et al. UMGC has modified this work and it is available under the original license.

Hindawi Publishing Corporation Discrete Dynamics in Nature and Society Volume 2016, Article ID 3263587, 15 pages http://dx.doi.org/10.1155/2016/3263587



Research Article

A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD

Musrrat Ali, 1 Chang Wook Ahn, 2 Millie Pant, 3 and Patrick Siarry 4

¹Department of Natural and Applied Science, Glocal University, Saharanpur-247122, India

Correspondence should be addressed to Chang Wook Ahn; cwan@skku.edu

Received 23 July 2015; Revised 4 October 2015; Accepted 15 October 2015

Academic Editor: David Arroyo

Copyright © 2016 Musrrat Ali et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Digital image watermarking is the process of concealing secret information in a digital image for protecting its rightful ownership. Most of the existing block based singular value decomposition (SVD) digital watermarking schemes are not robust to geometric distortions, such as rotation in an integer multiple of ninety degree and image flipping, which change the locations of the pixels but don't make any changes to the pixel's intensity of the image. Also, the schemes have used a constant scaling factor to give the same weightage to the coefficients of different magnitudes that results in visible distortion in some regions of the watermarked image. Therefore, to overcome the problems mentioned here, this paper proposes a novel image watermarking scheme by incorporating the concepts of redistributed image normalization and variable scaling factor depending on the coefficient's magnitude to be embedded. Furthermore, to enhance the security and robustness the watermark is shuffled by using the piecewise linear chaotic map before the embedding. To investigate the robustness of the scheme several attacks are applied to seriously distort the watermarked image. Empirical analysis of the results has demonstrated the efficiency of the proposed scheme.

1. Introduction

Digital watermarking [1, 2] is the process of insertion of digital watermark in media content and its extraction, if required, for authentication or ownership verification of media content. A digital watermark is a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer but easily detected by a computer [3]. Different types of digital watermarking methods for digital contents have been developed that are classified into different categories depending upon the use and the requirement of information required for the extraction/detection of watermark. To check the authenticity of a digital content fragile watermarking is used while, for the purpose of copyright protection, robust watermarking is utilized. This classification is application-dependent. Based on the information required for the extraction/detection

process watermarking schemes can be classified into blind, semiblind, and nonblind categories. Also, one more categorization is possible depending upon the domain of embedding of watermark: spatial and frequency. A detailed review of watermarking schemes can be found in [4, 5].

In a robust image watermarking scheme, a trade-off always exists among the two conflicting objectives, imperceptibility (also known as perceptual transparency) and robustness. So, the main goal of a robust image watermarking scheme is to produce the watermarked image with low quality degradation and high robustness. Increasing the amount of embedding information in an image may enhance its robustness to intentional or unintentional distortions applied to the image while simultaneously scarifying its imperceptibility and vice versa. Therefore, in order to improve these objectives, researchers have proposed several watermarking schemes implemented in spatial as well as

²Department of Computer Engineering, Sungkyunkwan University, Suwon-440746, Republic of Korea

³Department of Applied Science and Engineering, IIT Roorkee-247667, India

⁴Laboratoire Images, Signaux et Systèmes Intelligents (LiSSi, EA 3956), Université Paris-Est Créteil Val de Marne, 61 avenue du Général de Gaulle, 94010 Créteil, France

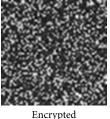
transformed domain that find a compromise between these two objectives. The spatial domain watermarking techniques directly embed the watermark into the host image by altering the pixel values [6-9]. These methods generally are less robust to image and signal processing attacks and required low computational efforts, while frequency domain methods transform the representation of spatial domain into the frequency domain and then modify its frequency coefficients to embed the watermark. There are many transform domain watermarking techniques such as discrete cosine transforms (DCT) [10, 11], discrete Fourier transforms (DFT) [12–14], discrete wavelet transforms (DWT) [15-17], and singular value decomposition (SVD) [2, 18-20]. These methods typically provide higher image imperceptibility and are much more robust to image manipulations, but the computational cost is higher than spatial domain watermarking methods. The performance of watermarking methods was further improved by combining two or more transformations [21-36]. The idea was based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

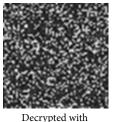
The singular value decomposition (SVD) is extensively used in image watermarking field in recent years due to its features. However, various researchers pointed out the false positive detection problem in most of the SVD-based algorithms [33, 37-40]. To counter this problem, numerous researchers have proposed improved versions of SVD-based image watermarking schemes. A robust image watermarking scheme based on SVD that embeds the entire watermark is given in [19]. There are two versions of this scheme depending on the implementation of SVD, to entire cover image and block-wise. The imperceptibility of an image watermarking scheme using block based SVD proposed in [18] is improved by incorporating compensation operation. According to this scheme, the damage in the quality due to insertion of the watermark in the left singular vector matrix is compensated by modifying the right singular vector matrix. The host image is segmented into nonoverlapping blocks of size 4 × 4; then the embedding blocks are selected at random. The watermark bits are embedded by modifying the coefficients in the first column of the left singular vector matrix of the target blocks. The different regions within an image have different local features, so some visual models such as human visual system (HVS) may be incorporated in finding the suitable embedding regions to improve robustness while maintaining imperceptibility. Based on this concept, a blind SVD-based watermarking scheme is presented in [34]. The host image is segmented into nonoverlapping blocks of size 8 × 8; then the embedding blocks are selected based on the sum of visual and edge entropies. The watermark bits are embedded by modifying the coefficients in the first column of the left singular vector matrix of the target blocks. The above mentioned SVD-based watermarking schemes embed the entire watermark within the cover image. It has improved the reliability of the watermarking but sacrificed the transparency. Also, these schemes are applicable only for the black and white watermark. If the watermark image is grayscale, then encode it to binary before embedding. A watermarking scheme proposed in [41] is based on the

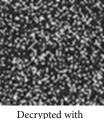
fact that SVD subspace (left and right singular vectors) can preserve a significant amount of information about an image. Therefore, it embeds the principal component, multiplication of left singular vector matrix and the singular value matrix, of watermark into the host image instead of singular values of the watermark. On the same concept, Run et al. [36] introduced an image watermarking scheme embedding the principal component of the watermark in frequency domain (DCT and DWT domains, resp.). Also, an optimization technique is applied to get the optimal scaling factors for embedding. Guo and Prasetyo [33] have extended this principal component concept to the block based watermarking. For convenience, this "false positive free SVD-based watermarking" scheme is abbreviated as "FPF-SVD-W" and used throughout the paper. The low frequency subband of the DWT transformed image is segmented into nonoverlapping blocks equal to the size of the watermark. Then the largest singular value of each block is modified by adding to it a scalar multiple of the corresponding element of the principal component matrix of the watermark. This reliable SVD-based watermarking scheme has solved the false positive detection problem and shown the resistance against some image manipulation attacks. It is not robust against some special distortions, such as image rotation in integer multiple of ninety degrees and image flipping (rows/columns). It is also realized from this scheme that a single scaling factor is not suitable to scale all the elements of the principal component matrix of the watermark. As the largest singular values from each block of the image have a different tolerance limit of modification to embed the watermark, it results in some visible distortions in the watermarked image with single scaling factor.

The focus of this research is on imperceptibility and robustness improvement of the reliable SVD-based image watermarking FPF-SVD-W. This paper proposes a novel and efficient and reliable SVD-based image watermarking scheme by incorporating the redistributed image normalization and variable scaling factor. To make the proposed scheme resilient against the attacks, such as rotation in an integer multiple of ninety degrees and image flipping, which change the locations of the pixels but do not make any changes to the pixel's intensity of the image, redistributed image normalization is utilized. To mitigate the problem of visible distortions in the watermarked image, a variable scaling factor in employed depending on the coefficient's magnitude to be embedded. In the proposed scheme the host image is redistributed and then some normalization operators are applied. Subsequently, the low frequency subband of the DWT transformed image is segmented into nonoverlapping blocks and SVD is applied to each block to get the largest singular value. The watermark is shuffled by using the piecewise linear chaotic map [35, 42] and then the elements of the principal component matrix of the watermark are embedded into the blocks by modifying the largest singular value of the corresponding blocks. The performance of the proposed scheme has been analyzed using several cover and watermark images and fifteen distortion attacks. Experimental results indicate that the proposed scheme not only gives the best results, but also outperforms the other SVD-based scheme FPF-SVD-W.











wrong p

crypted with x_1 Decrypted with x_2 correct values

FIGURE 1: Illustration of PWLCM with different cases.

The rest of the paper is organized as follows. A brief review of the components of the proposed scheme is given in Section 2. The watermarking scheme *FPF-SVD-W* is discussed in detail in Section 3. Section 4 describes the proposed scheme. The experimental results are analyzed in Section 5. Finally, Section 6 draws the conclusions based on this research.

2. Brief Review of Components of the Proposed Scheme

2.1. Piecewise Linear Chaotic Map (PWLCM). To enhance the confidentiality of the watermarking scheme, encryption of the watermark must be done before embedding into cover image. There are several chaotic maps that can be used for encryption; piecewise linear chaotic map (PWLCM) [35, 42] is one of them that recently has gained popularity due to its simplicity in representation and efficiency in implementation, as well as good dynamical behavior. Since the chaotic signal generally has good invariance to disturbance due to the low correlation between the initial parameters, it has been widely utilized for encryption and data hiding applications. The PWLCM, mathematically, is described in

$$x_{i+1} = f_p(x_i) = \begin{cases} \frac{x_i}{p} & \text{if } x_i \in [0, p) \\ \frac{(x_i - p)}{(0.5 - p)} & \text{if } x_i \in [p, 0.5) \\ f_p(1 - x_i) & \text{if } x_i \in [0.5, 1), \end{cases}$$
(1)

where $p \in (0, 0.5)$ is control parameter and considered as secret key. The most attractive features of PWLCM are its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. It is a noninvertible transformation of unit interval onto itself.

The encryption process of an image (I) of size $M \times N$ based on this map is performed by implementing the steps given in Algorithm 1. An illustration of output of Algorithm 1 is given in Figure 1, by considering the different cases.

2.2. Singular Value Decomposition (SVD). The singular value decomposition (SVD) [18–20] is a numerical analysis technique based on a theorem of linear algebra that decomposes a rectangular matrix into the product of three matrices: an orthogonal matrix (*U*), a diagonal matrix (*S*), and the

transpose of an orthogonal matrix (V). It may be considered as a method of transforming correlated data set into uncorrelated one that better explains the various relationships among the original data. Due to the unique features and attractive properties such as stability with little disturbance, SVD has been used in many signal and image processing applications such as image watermarking, image hiding, image compression, and noise reduction. The digital image is also a kind of signal which can be viewed as a matrix. According to the theory, the SVD of a rectangular matrix A of order $m \times n$ is represented mathematically as

$$A = USV^T, (2)$$

where $UU^T = I_m$ and $VV^T = I_n$; the columns of U are orthonormal eigenvectors of AA^T , the columns of V are orthonormal vectors of A^TA , and S is a diagonal matrix containing the square roots of the eigenvalues from U or V in descending order. If r ($r \le n$) is the rank of the matrix A then the elements of the diagonal matrix S satisfy the relation (3) and the matrix A can be written as (4):

$$\lambda_1 \ge \lambda_2 \ge \dots \ge \lambda_r > \lambda_{r+1} = \lambda_{r+2} \dots = \lambda_n = 0,$$
 (3)

$$A = \sum_{k=1}^{r} \lambda_k u_k v_k^T, \tag{4}$$

where u_k and v_k are the kth eigenvector of U and V and λ_k is the kth singular value.

Algorithm 1 (shuffling of an image by PWLCM). Consider the following steps.

Step 1. Iterate the piecewise linear chaotic map $M \times N$ times to get a vector $V = \{x_1, x_2, \dots, x_{MN}\}$ of MN values.

Step 2. Sort the above values in ascending/descending order and record their position indices $IX = \{s_1, s_2, ..., s_{MN}\}$.

Step 3. Perform vectorization operation which converts the image (*I*) into a vector *A*.

Step 4. Copy the pixel values from vector A to another vector B such that B = A(IX).

Step 5. Finally, the encrypted image (EI) is obtained by reshaping *B* back to an $M \times N$ matrix.

2.3. Discrete Wavelet Transform (DWT). The temporal resolution (i.e., it captures both frequency and location or time information) advantage of DWT [15, 21, 28] over more traditional transforms, such as the Fourier transform, makes it a versatile mathematical transform having numerous applications in different areas including image and signal processing. Wavelet transform has recently become an important tool in image processing and watermarking due to its good energy compaction properties. The basic idea of discrete wavelet transform (DWT) is to separate frequency detail and is based on small waves, called wavelets, of varying frequency and limited duration. In DWT, a time scale representation of digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales. Each level of decomposition of DWT decomposes an image into four subbands, namely LL, HL, LH, and HH. The lower resolution approximation subband (LL) that contains a rough description of the image is obtained by passing the digital signal through a low-low filter in both directions. The HL and LH subbands are obtained by passing through a low-pass filter in one direction and through a high-pass filter in another direction. The HH subband is high-pass filtered in both directions and contains the high-frequency components along the diagonals. After the image is processed by the wavelet transform, most of the information contained in the original image is concentrated into the LL image. LH contains mostly the vertical detail information which corresponds to horizontal edges. HL represents the horizontal detail information from the vertical edges. The low-pass subband can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached.

3. The "FPF-SVD-W" Scheme and Its Weakness

This section provides the detail of the scheme proposed by Guo and Prasetyo [33] and then analyzes its weakness.

3.1. The "FPF-SVD-W" Scheme. Let I be a grayscale cover image of size $M \times M$, and let W be the visual grayscale watermark of size $N \times N$. This scheme embeds the principal component of the watermark into the singular value matrix of the cover image composed by the largest singular values of the blocks.

3.1.1. Watermark Embedding. (E1) The SVD is performed on the watermark image W as follows:

$$W \xrightarrow{\text{SVD}} U_w S_w V_w^T. \tag{5}$$

(E2) The watermark principal component is obtained by multiplying the matrices U_m and S_m :

$$W_{US} \longleftarrow U_m S_m.$$
 (6)

Let the value in principal component matrix at location (i, j) be denoted by $W_{US}(i, j)$, where i, j = 1, 2, ..., N.

(E3) One-level DWT is performed on the host image *I* to obtain four subbands each of size $M/2 \times M/2$:

$$I \xrightarrow{\text{DWT}} \{LL, HL, LH, HH\}. \tag{7}$$

(E4) The LL subband is divided into several nonoverlapping blocks of size $m \times m$. Let ll(i, j) denote an image block at position (i, j), where i, j = 1, 2, ..., N. The block size is chosen as m = M/2N.

(E5) The SVD is applied for each image block ll(i, j) to get the largest singular value $\lambda_{max}(i, j)$:

$$ll(i, j) \xrightarrow{\text{SVD}} USV^T,$$
 (8)

where $S = \text{diag}(\lambda_k)$ and k = 1, 2, ..., m. The watermark principal component is embedded into the host image by modifying the largest singular value.

(E6) The watermark principal component is embedded into the largest singular value of host image for each image block (i, j) using the following formula:

$$\lambda_{\max}^{d}(i,j) = \lambda_{\max}(i,j) + \alpha W_{US}(i,j), \qquad (9)$$

where $\lambda_{\max}^d(i,j)$ denotes the distorted largest singular value in image block (i, j).

(E7) Inverse SVD is performed on each image block (i, j)

$$ll^d(i,j) \longleftarrow US^dV^T, \tag{10}$$

where $S^d = \operatorname{diag}(\lambda_{\max}^d, \lambda_k)$ for k = 2, ..., m. (E8) The distorted LL subband image is obtained as

$$LL^{d} \longleftarrow \left\{ ll^{d} \left(i, j \right) \right\}. \tag{11}$$

(E9) The watermarked image is reconstructed by performing 1-level inverse DWT (IDWT) as

$$I_w \stackrel{\text{IDWT}}{\longleftarrow} \left\{ LL^d, HL, LH, HH \right\}.$$
 (12)

The singular vector matrix V_w^T of the watermark and the largest singular value $\lambda_{\max}(i,j)$, where $i,j=1,2,\ldots,N$, of each block of the cover image are kept safe for the watermark extraction.

3.1.2. Watermark Extraction. In the watermark extraction process, the watermark W^* is extracted from the possibly corrupted watermarked image I_w^* by using the side information that is kept safe in embedding process $(V_w^T \text{ and } \lambda_{\max}(i, j))$ by employing the following steps.

(X1) One-level DWT is applied on the possibly corrupted watermarked image as

$$I_{w}^{*} \xrightarrow{\text{DWT}} \{LL^{*}, HL^{*}, LH^{*}, HH^{*}\}. \tag{13}$$

(X2) The LL* subband is divided into several nonoverlapping image blocks of size $m \times m$ which are denoted as $ll^*(i, j)$, where i, j = 1, 2, ..., N.





(a) Cover image

(b) Watermark

FIGURE 2: Cover and watermark images.

(X3) SVD is applied for each image block $ll^*(i, j)$ to get the largest singular value $\lambda_{\max}^*(i, j)$:

$$ll^*(i,j) \xrightarrow{\text{SVD}} U^* S^* V^{*T}.$$
 (14)

(X4) Corrupted principal component is obtained as

$$W_{\text{US}}^{*}\left(i,j\right) = \frac{\left(\lambda_{\text{max}}^{*}\left(i,j\right) - \lambda_{\text{max}}\left(i,j\right)\right)}{\alpha}.$$
 (15)

(X5) The extracted watermark is obtained as

$$W^* \longleftarrow W_{US}^* V_w^T. \tag{16}$$

3.2. Weakness Analysis of the "FPF-SVD-W" Scheme. To analyze the weakness of the scheme grayscale square images of sizes 512 and 64 are considered as cover and watermark images, respectively. These two images are given in Figure 2. This scheme has solved the false positive detection problem that occurred in some previous SVD-based watermarking schemes [22, 27]. It has given the competitive results in comparison to other watermarking schemes in terms of imperceptibility and robustness. It is obvious from the SVD properties that singular values are invariant to the operations of flipping and rotation of the matrix in integer multiple of ninety degrees. In other words, singular values of a matrix, singular values of its rotated version obtained by rotating in integer multiple of ninety degrees, and singular values of row/column flipping matrix are the same. So the watermarking scheme that applies the SVD to entire cover image will be resistant to rotation and flipping attacks. But in the scheme *FPF-SVD-W*, SVD is implemented block-wise, and these blocks are not invariant to these operations. So, this scheme is not resistant to these types of attacks. Watermarked image, distorted watermarked images under these operations, and extracted watermarks from these images are given in Figure 3. From this figure, it is clear that the scheme is not robust to these attacks.

In singular value decomposition (SVD) the singular values are in descending order of the rows from top to bottom. The columns of the singular vector matrix U are

orthonormal vectors. The principal component matrix is obtained by the multiplication of these two matrices. The absolute value of the columns of this matrix decreases from left to right. There is a huge difference in the absolute values of the columns at left and right. This situation is illustrated in Figure 4 by taking a square matrix of order three. Therefore, a single constant scaling factor would not be suitable for the embedding principal component matrix of the watermark. It will introduce the visible distortions on the left side of the image that is shown in Figure 5. To obtain the good imperceptibility this scaling factor must be a variable depending on the columns of the principal component matrix that are being embedded.

4. The Proposed Scheme

This section is devoted to the mathematical formulation of the proposed watermarking scheme and its components.

4.1. Redistributed Image Normalization. The purpose of redistributed image normalization is to obtain the invariant blocks under the rotation and flipping operations. The location of pixel values in a block may vary, but the elements of the blocks remain the same. To achieve it, pixels' locations of the image are redistributed and then some normalization procedures are performed. Mathematically, it is formulated as follows.

Let *A* be the image of size $M \times N$ that is divided into four (2×2) , equal-sized subimages and their respective mean of intensities is calculated and stored in a matrix form as Mean = $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $a, b, c, d \ge 0$.

With the help of these means a normalization matrix (B) is constructed as

$$B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} a+b+c+d & a+b-c-d \\ a-b+c-d & a-b-c+d \end{pmatrix}.$$
(17)

Redistribute the original image (*A*), using the distribution relation given in (18) to obtain the redistributed image (RI):

$$RI(2i-1,2j-1) = I(i,j),$$

$$1 \le i \le \frac{M}{2}, \ 1 \le j \le \frac{N}{2},$$

$$RI(2i-1,2j-N) = I\left(i,\frac{3N}{2}-j+1\right),$$

$$1 \le i \le \frac{M}{2}, \ \frac{N}{2} \le j \le N,$$

$$RI(2i-M,2j-1) = I\left(\frac{3M}{2}-i+1,j\right),$$

$$\frac{M}{2} \le i \le M, \ 1 \le j \le \frac{N}{2},$$

$$RI(2i-M,2j-N) = I\left(\frac{3M}{2}-i+1,\frac{3N}{2}-j+1\right),$$

$$\frac{M}{2} \le i \le M, \ \frac{N}{2} \le j \le N.$$

$$(18)$$

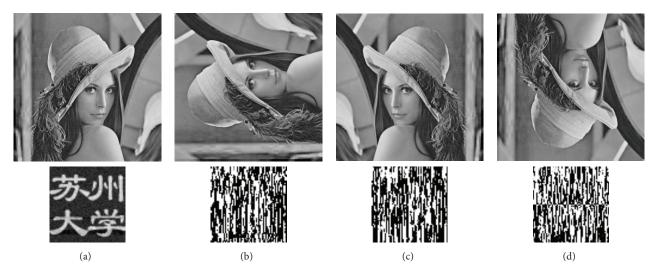


FIGURE 3: Watermarked, distorted watermarked, and extracted watermark images.

$$\begin{bmatrix} 23 & 47 & 32 \\ 13 & 5 & 42 \\ 12 & 43 & 32 \end{bmatrix} = \begin{bmatrix} -0.68 & -0.32 & 0.66 \\ -0.40 & 0.92 & 0.03 \\ -0.61 & -0.24 & -0.75 \end{bmatrix} \times \begin{bmatrix} 88.50 & 0.00 & 0.00 \\ 0.00 & 29.29 & 0.00 \\ 0.00 & 0.00 & 6.85 \end{bmatrix} \times \begin{bmatrix} -0.32 & 0.06 & 0.95 \\ -0.68 & -0.71 & -0.19 \\ -0.66 & 0.71 & -0.27 \end{bmatrix}^T$$

$$\begin{bmatrix} -60.46 & -9.26 & 4.51 \\ -35.16 & 26.86 & 0.19 \\ 54.22 & -7.09 & -5.15 \end{bmatrix}$$
Principal component = $U \times S$

FIGURE 4: Illustration of SVD and its principal component.



FIGURE 5: Illustration of visible distortion caused by embedding the watermark by zooming the portions of watermarked image.

If $|B_{21}| > |B_{12}|$, where the term |*| is the absolute value operator, then transpose the image RI to obtain the redistributed normalized image. To show this visually, we have taken an example of a square matrix of order 4 that is shown in Table 1. The block size is taken 2×2 to show the singular values of the blocks by applying SVD to both original and normalized versions, respectively. From this table it is clear that the singular values of the blocks of redistributed

image are invariant under the operation of rotation and flipping.

4.2. Scaling Factor. The scaling factor in watermarking determines the watermark strength and plays an important role to control the robustness and watermark imperceptibility. A small value of the scaling factor favors the watermark imperceptibility, but the watermarked image is less robust to

Operation	Image an	d its singular value	Normalized image and its singular value			
Operation	Matrix	Singular value of blocks	Matrix	Singular value of blocks		
	1 5 9 13	8.11 0.00 23.37 0.00	1 13 5 9	20.95 0.00 17.71 0.00		
Original	2 6 10 14	0.00 0.49 0.00 0.17	4 16 8 12	0.00 1.72 0.00 0.68		
Original	3 7 11 15	11.74 0.00 27.31 0.00	2 14 6 10	20.82 0.00 17.49 0.00		
	4 8 12 16	0.00 0.34 0.00 0.15	3 15 7 11	0.00 0.58 0.00 0.23		
	13 14 15 16	23.37 0.00 27.31 0.00	13 1 9 5	20.95 0.00 17.71 0.00		
Rotate 90 degrees	9 10 11 12	0.00 0.17 0.00 0.15	16 4 12 8	0.00 1.72 0.00 0.68		
Rotate 70 degrees	5 6 7 8	8.11 0.00 11.74 0.00	14 2 10 6	20.82 0.00 17.49 0.00		
	1 2 3 4	0.00 0.49 0.00 0.34	15 3 11 7	0.00 0.58 0.00 0.23		
	4 8 12 16	11.74 0.00 27.31 0.00	4 16 8 12	20.95 0.00 17.71 0.00		
Flip rows	3 7 11 15	0.00 0.34 0.00 0.15	1 13 5 9	0.00 1.72 0.00 0.68		
Thp Tows	2 6 10 14	8.11 0.00 23.37 0.00	3 15 7 11	20.82 0.00 17.49 0.00		
	1 5 9 13	0.00 0.49 0.00 0.17	2 14 6 10	0.00 0.58 0.00 0.23		
	13 9 5 1	23.37 0.00 8.11 0.00	13 1 9 5	20.95 0.00 17.71 0.00		
Flip column	14 10 6 2	0.00 0.17 0.00 0.49	16 4 12 8	0.00 1.72 0.00 0.68		
rup commi	15 11 7 3	27.31 0.00 11.74 0.00	14 2 10 6	20.82 0.00 17.49 0.00		
	16 12 8 4	0.00 0.15 0.00 0.34	15 3 11 7	0.00 0.58 0.00 0.23		

TABLE 1: Illustration of invariant features of the redistributed normalization.

several common attacks. On the other hand, selecting a high value of scaling factor favors the robustness, but the quality of watermarked image is unacceptably degraded. Proper choice of scaling factor for watermarking is more difficult than expected.

A single constant scaling factor cannot be suitable to modify the coefficients having huge difference in absolute values. To maintain the balance between the imperceptibility and robustness the scaling factor corresponding to the large coefficient values must be small, whereas the scaling factor corresponding to the small coefficient values must be large [23]. From Figure 4, it is clear that the scaling factor must increase from left to right depending on the columns of the watermark being embedded, because the absolute coefficient values in the columns of principal component matrix being embedded decrease from left to right. Therefore, in the proposed watermarking scheme a variable scaling factor in the range $[\alpha_{\min} = 0.25, \alpha_{\max} = 1.0]$ depending on the columns of the watermark of size $N \times N$ is utilized to achieve a better performance:

$$\alpha_j = \alpha_{\min} - (\alpha_{\min} - \alpha_{\max}) \times \frac{j}{N}, \quad j = 1, 2, \dots, N.$$
 (19)

4.3. Embedding Process. (E1) Apply the PWLCM on the watermark image to get the shuffled watermark image W using (1).

(E2) Perform the SVD on the shuffled watermark image *W* as follows:

$$W \xrightarrow{\text{SVD}} U_m S_m V_m^T. \tag{20}$$

(E3) Obtain the watermark principal component by multiplying matrices U_w and S_w :

$$W_{US} \longleftarrow U_w S_w.$$
 (21)

Let $W_{US}(i, j)$ be the principal component in pixel position (i, j), where i, j = 1, 2, ..., N.

(E4) Apply the redistributed image normalization process on the cover image (*I*) to obtain the normalized cover image RI and use the flag to keep the transpose record.

(E5) Perform 1-level DWT on the normalized cover image RI of size $M \times M$ to obtain four subbands each of size $M/2 \times M/2$:

$$RI \xrightarrow{DWT} \{LL, HL, LH, HH\}. \tag{22}$$

(E6) Divide the *LL* subband into several nonoverlapping blocks of size $m \times m$. Let ll(i, j) denote an image block at position (i, j), where i, j = 1, 2, ..., N. The block size is chosen as m = M/2N.

(E7) Apply SVD for each image block ll(i, j) to get the largest singular value $\lambda_{\max}(i, j)$:

$$ll(i, j) \xrightarrow{\text{SVD}} USV^T,$$
 (23)

where $S = \text{diag}(\lambda_k)$ and k = 1, 2, ..., m. The watermark principal component is embedded into the host image by modifying the largest singular value.

(E8) Embed the watermark principal component into the largest singular value of host image for each image block (i, j) using the following formula:

$$\lambda_{\max}^{d}(i,j) = \lambda_{\max}(i,j) + \alpha_{j}W_{US}(i,j), \qquad (24)$$

where $\lambda_{\max}^d(i,j)$ denotes the distorted largest singular value in image block (i,j) and α_j is the scaling factor that is determined by (19).

(E9) Perform inverse SVD on each image block (i, j) as

$$ll^d(i,j) \longleftarrow US^dV^T,$$
 (25)

where $S^d = \text{diag}(\lambda_{\text{max}}^d, \lambda_k)$ for k = 2, ..., m.

(E10) Obtain the distorted LL subband image as

$$LL^{d} \longleftarrow \left\{ ll^{d} \left(i, j \right) \right\}. \tag{26}$$

(E11) Perform 1-level inverse DWT on wavelet subbands replacing LL subband by LL^d as

$$RI_{w} \stackrel{IDWT}{\longleftarrow} \{LL^{d}, HL, LH, HH\}.$$
 (27)

- (E12) Apply the inverse redistributed image normalization process on the image obtained in step (E9) to obtain the watermarked image I_w . Now, we have to decide depending on the flag whether a transpose is required or not. The normalization step is done depending on flag (E4) and fresh calculation of B_{11} , B_{12} , B_{21} , and B_{22} values is not required. Finally, redistribute the modified RI_w to get the watermarked image.
- 4.4. Extraction Process. The watermarked image I_w is subjected to various distortions. If I_w^* is distorted watermarked image, then a possibly corrupted watermark W^* can be extracted by performing the following steps.
- (X1) Apply the redistributed image normalization process on the distorted watermarked image to obtain the normalized image RI_w^* .
- (X2) Apply 1-level DWT on the possibly corrupted watermarked image RI_w^* as

$$RI_{w}^{*} \xrightarrow{DWT} \left\{ LL^{*}, HL^{*}, LH^{*}, HH^{*} \right\}. \tag{28}$$

(X3) Divide the LL^* subband into several nonoverlapping image blocks of size $m \times m$ which are denoted as $ll^*(i, j)$, where i, j = 1, 2, ..., N.

(X4) Apply the SVD for each image block $\mathcal{U}^*(i,j)$ to get the largest singular value $\lambda^*_{\max}(i,j)$:

$$ll^*(i,j) \xrightarrow{\text{SVD}} U^* S^* V^{*T}.$$
 (29)

(X5) Obtain corrupted principal component as

$$W_{US}^{*}(i,j) = \frac{\left(\lambda_{\max}^{*}(i,j) - \lambda_{\max}(i,j)\right)}{\alpha_{j}},$$
 (30)

where α_i is the scaling factor given in (19).

(X6) Obtain the extracted watermark as

$$W^* \longleftarrow W_{US}^* V_w^T. \tag{31}$$

(X7) Apply the PWLCM on extracted watermark to get the embedded watermark.

5. Results and Discussions

This section analyzes the performance of the proposed watermarking scheme under the various experiments. Ten test images of size 512×512 given in Figures 6(a)-6(j) are taken as the cover images, while the grayscale images of size 64×64 given in Figures 6(k)-6(m) are taken as the watermark images. PSNR (peak signal-to-noise ratio) [30] is used to analyze the visual quality of the watermarked image. To investigate the robustness of the proposed scheme fifteen attacks are applied to the watermarked images: (1) median filtering (MF) with window size 5×5 , (2) average filtering (AF) with window size 3×3 , (3) rotation (RO) with 90° anticlockwise, (4) rows flipping (FR), (5) columns flipping (FC), (6) pixilation with window size 4×4 (PI), (7) JPEG compression with quality factor 50, (8) motion blur with (3,3) (MB), (9) resizing (RS) 512 \rightarrow 256 \rightarrow 512, (10) Gaussian low-pass filtering (GF) with window size $5 \times$ 5, (11) Gaussian noise (GN) with mean zero and variance 0.01, (12) salt and pepper noise (SP) with density 0.05, (13) speckle noise (SN) with variance 0.04, (14) gamma correction (GC) with gamma value 0.9, and (15) sharpening (SH). The algorithms are implemented in MATLAB environment on a PC with 4 GB RAM and Core 2 Duo processor. Normalized correlation (NC) [33] coefficient is used as a similarity measure between the original and extracted watermark images. In order to justify the performance of the proposed scheme, results are compared to the false positive free SVD-based watermarking scheme (FPF-SVD-W) [33].

The average of PSNR values of the watermarked images obtained by the proposed scheme is 34.5769 while in case of *FPF-SVD-W* it is 30.8663. Also, the average PSNR over all the test images corresponding to each embedded watermarks is plotted for both the schemes in Figure 7. From this figure, it is clear that the PSNR values obtained by the proposed scheme are quite high in comparison to *FPF-SVD-W* in all the cases.

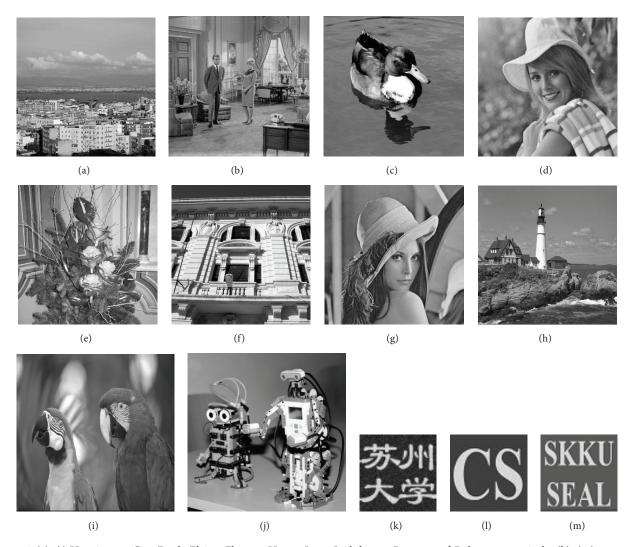


FIGURE 6: (a)–(j) Host images City, Duck, Elaine, Flowers, House, Lena, Lighthouse, Parrots, and Robots, respectively; (k)–(m) watermark images WM1, WM2, and WM3.

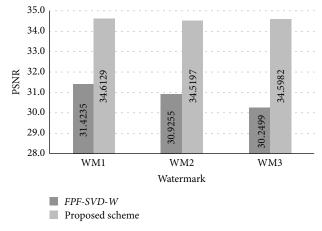


FIGURE 7: Comparison of PSNR values.

A high PSNR value is the indication of better quality of the watermarked image under consideration. It is shown that the

variable scaling factor has increased the imperceptibility to a great extent of the proposed scheme.

For the robustness experiments the distortions are applied on watermarked images that are described above. The normalized correlation values corresponding to each of the watermarks are given in Tables 2-4. These tables show that the performance of the proposed scheme is quite satisfactory in all the cases except gamma correction case, where its performance is poor. It is due to the insertion of watermark data into low frequencies. For the robustness comparison of the proposed scheme with the FPF-SVD-W, the average of normalized correlation (NC) values of extracted watermarks over the test images obtained in each case is given in Table 5. The best results are highlighted in bold for each case. From Table 5 it is clear that the performance of the proposed scheme is quite better in comparison to the FPF-SVD-W scheme. In case of rotation and flipping, especially, the proposed scheme has given best performance, while the performance of FPF-SVD-W scheme is worse. For the visual

Table 2: Correlation values of the extracted watermarks by the proposed scheme corresponding to WM1.

Attack	City	Couple	Duck	Elaine	Flowers	House	Lena	Lighthouse	Parrots	Robots
NO	0.9868	0.9989	0.9978	0.9987	0.9989	0.9991	0.9988	0.9989	0.9985	0.9981
MF	0.6236	0.7570	0.8552	0.8616	0.6288	0.5104	0.8501	0.7267	0.8715	0.7628
AF	0.8529	0.9161	0.9288	0.9260	0.8766	0.8296	0.9195	0.9043	0.9445	0.8926
RO	0.9868	0.9989	0.9978	0.9987	0.9989	0.9991	0.9988	0.9989	0.9985	0.9981
FR	0.9868	0.9989	0.9978	0.9987	0.9989	0.9991	0.9988	0.9989	0.9985	0.9981
FC	0.9868	0.9989	0.9978	0.9987	0.9989	0.9991	0.9988	0.9989	0.9985	0.9981
PI	0.9825	0.9969	0.9967	0.9983	0.9940	0.9769	0.9975	0.9951	0.9962	0.9873
JPEG	0.9731	0.9889	0.9851	0.9886	0.9872	0.9873	0.9880	0.9877	0.9869	0.9845
MB	0.9250	0.9640	0.9686	0.9723	0.9469	0.9542	0.9664	0.9629	0.9728	0.9564
RS	0.9488	0.9791	0.9835	0.9852	0.9697	0.9479	0.9851	0.9737	0.9843	0.9745
GF	0.9710	0.9903	0.9902	0.9903	0.9863	0.9824	0.9903	0.9893	0.9940	0.9876
GN	0.8170	0.8165	0.7984	0.8269	0.8208	0.8064	0.8272	0.8234	0.8225	0.7993
SP	0.7340	0.7559	0.7283	0.7382	0.7189	0.6505	0.7235	0.7265	0.6772	0.7024
SN	0.7600	0.8156	0.8130	0.7976	0.7741	0.7530	0.8121	0.8463	0.8706	0.8004
GC	0.5206	0.4462	0.4118	0.4458	0.4650	0.4739	0.4503	0.4308	0.4302	0.4708
SH	0.8944	0.9140	0.9164	0.9307	0.9016	0.8770	0.9414	0.9263	0.9555	0.9124

Table 3: Correlation values of the extracted watermarks by the proposed scheme corresponding to WM2.

Attack	City	Couple	Duck	Elaine	Flowers	House	Lena	Lighthouse	Parrots	Robots
NO	0.9807	0.9988	0.9978	0.9985	0.9988	0.9989	0.9986	0.9987	0.9984	0.9979
MF	0.5871	0.7304	0.8448	0.8461	0.6105	0.5177	0.8393	0.6925	0.8642	0.7410
AF	0.8342	0.9012	0.9151	0.9101	0.8589	0.8122	0.9067	0.8893	0.9377	0.8761
RO	0.9807	0.9988	0.9978	0.9985	0.9988	0.9989	0.9986	0.9987	0.9984	0.9979
FR	0.9807	0.9988	0.9978	0.9985	0.9988	0.9989	0.9986	0.9987	0.9984	0.9979
FC	0.9807	0.9988	0.9978	0.9985	0.9988	0.9989	0.9986	0.9987	0.9984	0.9979
PI	0.9760	0.9964	0.9966	0.9981	0.9934	0.9748	0.9971	0.9947	0.9959	0.9862
JPEG	0.9658	0.9869	0.9845	0.9869	0.9868	0.9857	0.9868	0.9862	0.9849	0.9843
MB	0.9122	0.9571	0.9620	0.9687	0.9409	0.9476	0.9611	0.9579	0.9693	0.9508
RS	0.9382	0.9769	0.9819	0.9830	0.9656	0.9417	0.9830	0.9701	0.9828	0.9712
GF	0.9638	0.9889	0.9889	0.9886	0.9844	0.9795	0.9887	0.9877	0.9933	0.9853
GN	0.7953	0.7968	0.7897	0.7989	0.7921	0.7884	0.8013	0.8090	0.8035	0.7819
SP	0.7210	0.7092	0.7069	0.7248	0.7350	0.6190	0.7229	0.7208	0.6696	0.6658
SN	0.7454	0.7979	0.7955	0.7658	0.7462	0.7201	0.7894	0.8164	0.8391	0.7838
GC	0.4754	0.3914	0.3607	0.3962	0.4208	0.4302	0.4042	0.3768	0.3675	0.4203
SH	0.9047	0.9363	0.9458	0.9532	0.9192	0.8638	0.9515	0.9336	0.9562	0.9188

Table 4: Correlation values of the extracted watermarks by the proposed scheme corresponding to WM3.

Attack	City	Couple	Duck	Elaine	Flowers	House	Lena	Lighthouse	Parrots	Robots
NO	0.9612	0.9980	0.9966	0.9976	0.9981	0.9983	0.9977	0.9978	0.9973	0.9959
MF	0.4967	0.6655	0.8000	0.8169	0.5339	0.4213	0.7935	0.6075	0.8298	0.6716
AF	0.7613	0.8577	0.8790	0.8757	0.8077	0.7374	0.8664	0.8369	0.9148	0.8267
RO	0.9612	0.9980	0.9966	0.9976	0.9981	0.9983	0.9977	0.9978	0.9973	0.9959
FR	0.9612	0.9980	0.9966	0.9976	0.9981	0.9983	0.9977	0.9978	0.9973	0.9959
FC	0.9612	0.9980	0.9966	0.9976	0.9981	0.9983	0.9977	0.9978	0.9973	0.9959
PI	0.9541	0.9945	0.9947	0.9970	0.9900	0.9624	0.9955	0.9916	0.9931	0.9790
JPEG	0.9377	0.9814	0.9777	0.9830	0.9816	0.9802	0.9815	0.9802	0.9796	0.9769
MB	0.8560	0.9299	0.9403	0.9581	0.9175	0.9174	0.9460	0.9328	0.9569	0.9302
RS	0.8992	0.9681	0.9751	0.9775	0.9523	0.9177	0.9765	0.9573	0.9768	0.9589
GF	0.9337	0.9831	0.9834	0.9821	0.9758	0.9694	0.9825	0.9809	0.9907	0.9773
GN	0.7249	0.7224	0.6962	0.7167	0.7300	0.6892	0.7206	0.7178	0.7253	0.7171
SP	0.6076	0.6267	0.6152	0.6507	0.6232	0.5447	0.6137	0.6211	0.5905	0.5927
SN	0.6476	0.7232	0.7208	0.6909	0.6678	0.6191	0.7036	0.7355	0.7866	0.6992
GC	0.4082	0.3356	0.3049	0.3388	0.3662	0.3655	0.3439	0.3212	0.3211	0.3621
SH	0.8596	0.9095	0.9316	0.9368	0.8809	0.7940	0.9235	0.8979	0.9237	0.8731

Attack		FPF-SVD-W			Proposed scheme	
Attack	WM1	WM2	WM3	WM1	WM2	WM3
NO	0.9959	0.9954	0.9837	0.9974	0.9967	0.9938
MF	0.8208	0.8169	0.7498	0.7448	0.7274	0.6637
AF	0.9196	0.9141	0.8662	0.8991	0.8841	0.8364
RO	0.0016	0.0042	0.0212	0.9974	0.9967	0.9938
FR	0.0277	0.0368	0.0009	0.9974	0.9967	0.9938
FC	0.0296	0.0232	0.0169	0.9974	0.9967	0.9938
PI	0.9523	0.9484	0.9185	0.9921	0.9909	0.9852
JPEG	0.9863	0.9848	0.9685	0.9857	0.9839	0.9760
MB	0.9590	0.9554	0.9235	0.9590	0.9528	0.9285
RS	0.9771	0.9752	0.9529	0.9732	0.9694	0.9559
GF	0.9861	0.9841	0.9665	0.9872	0.9849	0.9759
GN	0.7961	0.7737	0.6802	0.8158	0.7957	0.7160
SP	0.6613	0.6378	0.5371	0.7155	0.6995	0.6086
GC	0.4253	0.4368	0.2843	0.4545	0.4043	0.3468
SH	0.7897	0.7473	0.6788	0.9170	0.9283	0.8931
SN	0.7435	0.7218	0.6371	0.8043	0.7800	0.6994

TABLE 5: The average of correlation values of the extracted watermarks under different attacks.











FIGURE 8: Illustration of the false positive detection. (a) Watermarked image, (b) embedded watermark, (c) extracted watermark with correct information, (d) extracted watermark from (a) by using V_w of watermark (WM2), (e) extracted watermark from (a) by using V_w of watermark (WM3), and (f) extracted watermark from an arbitrary image by using the information of images given in (a) and (b).

quality analysis, the extracted watermarks from "Lena" are given in Tables 6 and 7, respectively. From these tables it is clear that the extracted watermarks are almost similar to the original watermark. The quality of extracted watermarks is good in all the cases except rotation and flipping attack cases. In these two cases we can see a big difference in qualities of the extracted watermarks obtained from both the schemes, where the proposed scheme is performed better in comparison to the *FPF-SVD-W* scheme.

Additionally, the proposed scheme is also checked for false positive detection problem that generally occurs in SVD-based watermarking schemes. False positive detection problem in an image watermarking occurs when a specific watermark is detected in a watermarked image that actually was not embedded in it. An experiment is conducted for testing the reliability of the proposed scheme. Figures 8(a) and 8(b) shows the watermarked image "Lena" and original watermark image WM1. Figure 8(c) shows the watermark extracted by providing the correct side information (V_w^T)

WM1 and $\lambda_{\max}(i,j)$ of Lena image). Figure 8(d) shows the watermark extracted by providing the V_w^T of WM2 as side information. Figure 8(e) shows the watermark extracted by providing the V_w^T of WM3 as side information. However, the extracted watermark given in Figure 8(f) is extracted from an arbitrary image other than "Lena" by providing the side information (V_w^T of WM1 and $\lambda_{\max}(i,j)$ of Lena image). Therefore, it is clear from these figures that the embedded watermark cannot be detected using any arbitrary reference watermark. Furthermore, one more security layer is also there in terms of encryption of watermark image depending on two secret keys (initial value x_1 and probability p). Thus the proposed scheme is able to handle the problem of false positive detection.

6. Conclusions

The proposed scheme has incorporated the concept of redistributed image normalization for finding the invariant blocks

Table 6: Extracted watermarks from the watermarked images that are distorted by various attacks.

Attack	WM1	FPF-SVD-W WM2	WM3	WM1	Proposed scheme WM2	WM3
NO	苏州 大学	CS	SKKU SEAL	苏州 大学	CS	SKKU SEAL
MF	苏州 大学	CS	SKKU SEAL	苏州 大学	CS	SKKU SEAL
AF	苏州 大学	CS	SKKU SEAL	苏.州 大学	CS	SKKU SEAL
RO				苏州 大学	CS	SKKU SEAL
FR				苏州 大学	CS	SKKU SEAL
FC				苏州 大学	CS	SKKU SEAL
PI	苏州 大学	CS	SKKU SEAL	苏州 大学	CS	SKKU SEAL
JPEG	苏州 大学	CS	SKKU SEAL	苏州 大学	CS	SKKU SEAL

that are used for watermarking. The invariance is in the sense that the location of the pixels in a block may vary but the elements are always the same. The SVD operation is then applied to these blocks to get the largest singular value from each block that is invariant to the rotation and flipping attacks. Then the principal component of the watermark image is embedded into these largest singular values by employing a variable scaling factor. The scaling factor varies in a specified range depending on the magnitude of embedding coefficient. To investigate the robustness of the

scheme several attacks are applied to seriously distort the watermarked image. Numerical and pictorial representation of the results has shown the efficiency of the proposed scheme. In most of the cases watermark is extracted with high correlation value. The experimental results compared with the other SVD-based watermarking scheme (*FPF-SVD-W*) have also represented the better performance of the proposed scheme. The imperceptibility of the proposed scheme has increased to a great extent by employing a variable scaling factor in comparison to *FPF-SVD-W* scheme that has used

Table 7: Extracted watermarks from the watermarked images that are distorted by various attacks.

constant scaling factor. Thus, the proposed scheme has satisfied the robustness, and imperceptibility, requirements that are essential for a robust watermarking scheme. The proposed scheme has proven its reliability for grayscale image watermarking; as a future work it can be extended to the video watermarking and color image watermarking. Due to the reliability of the proposed scheme, it may have the application in various areas, such as fingerprinting and medical image watermarking.

Conflict of Interests

GC

SH

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the MISP (Ministry of Science, ICT & Future Planning), Korea, under the SW oriented college support program: ICT/SW Creatieve Research program (IITP-2015-R2215-15-1005) supervised by the IITP (Institute for Information & Communications Technology Promotion).

References

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

- [2] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, 2002.
- [3] M. L. Miller, I. J. Cox, J.-P. M. G. Linnartz, and T. Kalker, "A review of watermarking principles and practices," in *Digital Signal Processing in Multimedia Systems*, K. K. Parhi and and T. Nishitani, Eds., pp. 461–485, Marcell Dekker, 1999.
- [4] E. Hussein and M. A. Belal, "Digital watermarking techniques, applications and attacks applied to digital media: a survey," *International Journal of Engineering Research and Technology*, vol. 1, no. 7, pp. 1–8, 2012.
- [5] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Information Sciences*, vol. 279, pp. 251–272, 2014.
- [6] L.-D. Li and B.-L. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks," *AEU: International Journal of Electronics and Communications*, vol. 63, no. 2, pp. 123–131, 2009.
- [7] Q. Su, Y. Niu, Q. Wang, and G. Sheng, "A blind color image watermarking based on DC component in the spatial domain," *Optik*, vol. 124, no. 23, pp. 6255–6260, 2013.
- [8] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, 2008.
- [9] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1469–1474, 2013.
- [10] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Computer Standards and Interfaces*, vol. 32, no. 1-2, pp. 54–60, 2010.
- [11] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, M. Nakano-Miyatake, H. Perez-Meana, and A. Ramirez-Acosta, "Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT," Signal Processing, vol. 97, pp. 40–54, 2014.
- [12] B. Chen, G. Coatrieux, G. Chen, X. Sun, J. L. Coatrieux, and H. Shu, "Full 4-D quaternion discrete Fourier transform based watermarking for color images," *Digital Signal Processing*, vol. 28, no. 1, pp. 106–119, 2014.
- [13] J. Lang and Z.-G. Zhang, "Blind digital watermarking method in the fractional Fourier transform domain," *Optics and Lasers in Engineering*, vol. 53, pp. 112–121, 2014.
- [14] W. Lu, H. Lu, and F.-L. Chung, "Feature based robust water-marking using image normalization," *Computers and Electrical Engineering*, vol. 36, no. 1, pp. 2–18, 2010.
- [15] E. H. Elshazly, O. S. Faragallah, A. M. Abbas et al., "Robust and secure fractional wavelet image watermarking," Signal, Image and Video Processing, 2014.
- [16] L. Li, H.-H. Xu, C.-C. Chang, and Y.-Y. Ma, "A novel image watermarking in redistributed invariant wavelet domain," *Jour*nal of Systems and Software, vol. 84, no. 6, pp. 923–929, 2011.
- [17] N. Liu, H. Li, H. Dai, D. Guo, and D. Chen, "Robust blind image watermarking based on chaotic mixtures," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1329–1355, 2015.
- [18] M.-Q. Fan, H.-X. Wang, and S.-K. Li, "Restudy on SVD-based watermarking scheme," *Applied Mathematics and Computation*, vol. 203, no. 2, pp. 926–930, 2008.
- [19] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," *Signal Processing*, vol. 88, no. 9, pp. 2158–2180, 2008.

- [20] Q. Su, Y. Niu, H. Zou, and X. Liu, "A blind dual color images watermarking based on singular value decomposition," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8455–8466, 2013
- [21] H.-T. Hu and L.-Y. Hsu, "Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression," *Computers and Electrical Engineering*, vol. 41, pp. 52–63, 2015.
- [22] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," AEU—International Journal of Electronics and Communications, vol. 67, no. 2, pp. 102–112, 2013
- [23] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," *Digital Signal Processing*, vol. 33, pp. 134–147, 2014.
- [24] X.-Y. Wang, Y.-P. Yang, and H.-Y. Yang, "Invariant image watermarking using multi-scale Harris detector and wavelet moments," *Computers & Electrical Engineering*, vol. 36, no. 1, pp. 31–44, 2010.
- [25] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," Applied Soft Computing Journal, vol. 13, no. 2, pp. 1170–1182, 2013.
- [26] P.-P. Zheng, J. Feng, Z. Li, and M.-Q. Zhou, "A novel SVD and LS-SVM combination algorithm for blind watermarking," Neurocomputing, vol. 142, pp. 520–528, 2014.
- [27] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, 2014.
- [28] M. Ali and C. W. Ahn, "An optimized watermarking technique based on self-adaptive de in DWT-SVD transform domain," *Signal Processing*, vol. 94, no. 1, pp. 545–556, 2014.
- [29] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik*, vol. 125, no. 1, pp. 428–434, 2014.
- [30] M. Ali, C. W. Ahn, M. Pant, and P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony," *Information Sciences*, vol. 301, pp. 44–60, 2015.
- [31] M. Ali, C. W. Ahn, and P. Siarry, "Differential evolution algorithm for the selection of optimal scaling factors in image watermarking," *Engineering Applications of Artificial Intelligence*, vol. 31, pp. 15–26, 2014.
- [32] S. H. Amiri and M. Jamzad, "Robust watermarking against print and scan attack through efficient modeling algorithm," Signal Processing: Image Communication, vol. 29, no. 10, pp. 1181–1196, 2014.
- [33] J.-M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1149–1163, 2014.
- [34] C.-C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Optics Communications*, vol. 284, no. 4, pp. 938–944, 2011.
- [35] B. Lei, D. Ni, S. Chen, T. Wang, and F. Zhou, "Optimal image watermarking scheme based on chaotic map and quaternion wavelet transform," *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2897–2907, 2014.
- [36] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright

- protection," Expert Systems with Applications, vol. 39, no. 1, pp. 673-689, 2012.
- [37] M. Ali and C. W. Ahn, "Comments on 'optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2392–2394, 2015.
- [38] J.-M. Guo and H. Prasetyo, "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," AEU—International Journal of Electronics and Communications, vol. 68, no. 9, pp. 816–834, 2014.
- [39] G. C.-W. Ting, "Ambiguity attacks on the Ganic-Eskicioglu robust DWT-SVD Image watermarking scheme," in *Information Security and Cryptology—ICISC 2005*, D. H. Won and S. Kim, Eds., vol. 3935 of *Lecture Notes in Computer Science*, pp. 378–388, Springer, Berlin, Germany, 2006.
- [40] X.-P. Zhang and K. Li, "Comments on 'an SVD-based water-marking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 7, no. 3, pp. 593–594, 2005.
- [41] C. Jain, S. Arora, and P. K. Panigrahi, "A reliable SVD based watermarking schem," http://arxiv.org/abs/0808.0309.
- [42] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Optics and Lasers in Engineering*, vol. 51, no. 6, pp. 665–673, 2013.