CHAPTER 3

Intelligent Watermarking Scheme Employing the Concepts of Block Based Singular Value Decomposition and Firefly Algorithm

Musrrat Ali, Chang Wook Ahn and Millie Pant

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, even if for some special distortions, such as multiples of 90° rotation of integers and image flipping, which change the location of pixels but have no effect on the value of the image. Therefore, to overcome the problems mentioned here, this chapter proposes a novel image watermarking scheme by redistributing the image and applying some normalization operators. Subsequently, this image is segmented into non-overlapping blocks and SVD is applied to each block to get the largest singular
value. The watermark is scrambled by using the Arnold cat map and then the bits are embedded in the blocks by quantizing the largest singular value of each block. In addition, the firefly algorithm (FA) is applied to obtain the quantization step (QS) optimally to improve the fidelity and the perceptual quality of the watermarked image. 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.

3.1 Introduction

Digital image watermarking [12, 34] is the process of authenticating a digital image by embedding a secret information into it and thereby protecting the image from copyright infringement. This information should be embedded imperceptibly in a way that allows it to be extracted/detected at a later stage for authentication/ownership verification. Different types of digital watermarking methods for digital contents have been developed that are classified into different categories depending upon the use 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, semi-blind and non-blind categories. Also, one more categorization is possible depending upon the domain of embedding the watermark; spatial and frequency. A detailed review of watermarking schemes can be found in [21, 22].

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 the embedded 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 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 [33, 43]. 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) [6, 29, 57], discrete Fourier transforms (DFT) [11, 25, 36, 47, 53], discrete wavelet transforms (DWT) [8, 13, 15, 17, 26, 28, 39, 40, 48, 49, 50], and singular value decomposition (SVD) [34, 42]. 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
Intelligent Watermarking Scheme Employing the Concepts ... 39

transformations [15 20 39 40 45 47 54 55 57 62]. The idea was based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

In an alternate way, some researchers have considered the watermarking problem as an optimization problem with these objectives and have taken the advantage of intelligent optimization techniques to obtain the optimal solution. Applications of genetic algorithm (GA) in image watermarking can be found in [23 37 38 44], particle swarm optimization (PSO) [48 53 56], and differential evolution (DE) [3 5 11 27]. Recently, Mishra et al. [41] implemented Firefly algorithm (FA) and Ali et al. [4] implemented artificial bee colony (ABC) algorithm to find the optimal parameters values for watermark embedding. Ali et al. [2] pointed out that the algorithm [41] implementing firefly algorithm is fundamentally flawed, which leads to false positive detection problem. Therefore, it has no practical value even though having high robustness against several image manipulation attacks under the consideration. Actually, it was due to improper algorithm design.

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 [2 17 16 30 31 32 35 52 60 61]. To count 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 [42]. Run et al. [48] introduced an image watermarking scheme employing SVD and embedding the principal component of the watermark. Particle swarm optimization is applied to get the optimal scaling factors for embedding. It is based on the fact that SVD subspace (left and right singular vectors) can preserve a significant amount of information about an image. Because different regions of an image have different local features, so some visual models 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 [10]. The host image is segmented into non-overlapping blocks of size 8 × 8, then the embedding blocks (most textured) are selected depending upon the number of non-zero singular values. The watermark bits are embedded by modifying the coefficients in the first column of the left singular vector matrix of the target blocks. Lai [24] has introduced an image watermarking scheme based on human visual system (HVS) and SVD. The embedding process of the scheme is the same as of [10], while the embedding blocks are selected based on the sum of visual and edge entropies. The scheme of Fan et al. [14] is an advanced version of the scheme proposed by Chang et al. [10], that promoted the transparency of the scheme by incorporating compensation operation. According to their 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. However, though these SVD based watermarking schemes have solved the false positive detection problem, they are not robust against some special distortions, such as multiples of 90° rotation of integers and image flipping. It is also observed from these studies that larger quantization step (QS) leads to higher robustness while simultaneously, it degrade the quality of the watermarked image and vice versa. Each image has a different tolerance limit of modification to embed the watermark. To
mitigate this problem, intelligent optimization techniques could be the best option to choose the quantization step to maintain a balance between imperceptibility and robustness.

This chapter proposes a novel and efficient watermarking scheme based on redistributed block SVD and firefly optimization algorithm. For convenience the proposed scheme is abbreviated as RSVD. The firefly algorithm, an intelligent optimization technique, has been successfully applied in solving many real life application problems with promising results [9, 19, 18, 41, 58, 59]. Also, this emerging optimization technique has been applied to image watermarking problem [41] but due to the false positive detection problem it has no practical value. Here, it is used in a different manner. In the proposed scheme the host image is redistributed and then applied some normalization operators. Subsequently, this image is segmented into non-overlapping blocks of size $8 \times 8$ and SVD is applied to each block to get the largest singular values. The watermark is scrambled by using the Arnold cat map [46] and then the bits are embedded into the blocks by quantizing the largest singular value of each block. Furthermore, the firefly algorithm (FA) is applied to obtain the quantization step (QS) optimally to improve the fidelity and the perceptual quality of the watermarked image. The challenge to withstand against the attacks of ninety degree multiple of rotation and flipping in block based SVD watermarking schemes has been solved in this work. The performance of the proposed scheme has been analyzed using several host and watermark images and twelve distortion attacks. Experimental results indicate that the proposed method is not only highly competitive, but also outperforms the scheme based on SVD without implementation of redistribution and firefly.

The rest of the chapter is organized as follows. The preliminaries are briefly described in Section 3.2. Section 3.3 describes the proposed scheme. The experimental results are analyzed in Sections 3.4. Finally, Section 3.5 draws the conclusions based on this research.

### 3.2 Preliminaries

#### 3.2.1 Singular Value Decomposition (SVD)

The singular value decomposition (SVD) [24, 34, 51] 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:

$$ A = USV^T $$

(3.1)
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 $r (r \leq n)$ is the rank of the matrix $A$ then the elements of the diagonal matrix $S$ satisfy the relation Eq.(3.2) and the matrix $A$ can be written as Eq.(3.3).

\[ \sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r > \sigma_{r+1} = \sigma_{r+2}... = \sigma_n = 0 \]  \hspace{1cm} \text{(3.2)}

\[ A = \sum_{k=1}^{r} \sigma_k u_k v_k^T \]  \hspace{1cm} \text{(3.3)}

where $u_k$ and $v_k$ are the $k$-th eigenvector of $U$ and $V$ and $\sigma_k$ is the $k$-th singular value.

### 3.2.2 Arnold cat map

To enhance the confidentiality of the watermarking scheme, scrambling must be done of the watermark before embedding into cover image. There are several chaotic maps that can be used for scrambling and Arnold cat map [5, 46] is one of them that is used in this study. 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 Arnold cat map is a two-dimensional invertible map which simply illustrates the principles of chaos. The generalized two-dimensional (2D) Arnold cat map applied to a square image $I$ of size $n \times n$ changes the locations of the pixels using the following relation:

\[
\begin{bmatrix}
  p_i (x+1) \\
  p_i (y+1)
\end{bmatrix} = \begin{bmatrix}
  1 & a \\
  b & ab + 1
\end{bmatrix} \begin{bmatrix}
  p_i (x) \\
  p_i (y)
\end{bmatrix} \mod (n)
\]  \hspace{1cm} \text{(3.4)}

where $0 \leq i \leq n^2 - 1$, $p_i(x)$ and $p_i(y)$ denote the coordinates $(x, y)$ of the pixel $p_i$, $\mod$ is the modulo operator, $a$ and $b$ are two positive integers such that the determinant of the matrix must be one. The Arnold cat map is periodic in nature due to the restriction imposed to the parameters $a$ and $b$. If the pixel $p_i$ at location $(x, y)$ undergoes the operation given in Eq.(3.4) several times, then it returns to its original location after $T$ iterations. This $T$ is called the period of the Arnold cat map. It is worth to point out that the period of the map depends on the parameters $a$, $b$, and the size of the image. These parameters can be used as secret keys. To get back the original image, periodicity is required. Suppose the scrambling is done performing $k$ iterations, so one can get back the original image by performing $(T - k)$ iterations. A graphical illustration of Arnold cat map by taking a binary square image of size 64 (i.e. $n = 64$) for different iterations $(k)$ with parameters $a = 1$ and $b = 1$ is shown in Fig.(3.1). It is obvious from the Fig.(3.1) that the period of a square image of size 64 is 48.
3.2.3 Firefly Algorithm

The firefly algorithm (FA) is inspired by the social behavior of fireflies that is developed by Yang [58, 59] at Cambridge University in 2008. The fireflies produce short and rhythmic flashes to attract a mate. It can also be used to send information between fireflies. The idea of this attractiveness and information passing is what led to the inspiration for the FA. In the firefly algorithm, there are three idealized rules:

1. All fireflies are unisexual, so that one firefly will be attracted to other fireflies regardless of their sex.
2. Attractiveness is proportional to their brightness, thus a less bright firefly will move towards a brighter firefly.
3. The brightness of a firefly is determined by the value of the objective function. For a maximization problem, the brightness of each firefly is proportional to the value of the objective function. In case of a minimization problem, the brightness of each firefly is inversely proportional to the value of the objective function. In general, firefly algorithm incorporates three important strategies which are given as follows.

3.2.3.1 Attractiveness

In the firefly algorithm, the main form of attractiveness function $\beta(r)$ can be any monotonically decreasing functions such as the following generalized form:

$$\beta = \beta_0 e^{-\gamma r^m}, \quad m \geq 1$$

(3.5)
Algorithm 3.1 Pseudo-code of Firefly Algorithm

Generate a uniformly distributed random population of \( NP \) fireflies \( X_i, i = 1, 2 \ldots NP \).
Define the objective function \( f(X) \) Initialize the values to the parameters \( \alpha, \beta_0, \) and \( \gamma \)

Begin
while (termination condition not met)
for \( i = 1 \) to \( NP \)
for \( j = 1 \) to \( NP \)
if ( \( f(X_i) < f(X_j) \))
    Move firefly ‘\( i \)’ towards firefly ‘\( j \)’
end if
Evaluate new solutions and update objective function
end for \( j \)
end for \( i \)
Rank the fireflies and find the current global best
end while
Post process results and visualization
End

where \( r \) is the distance between two fireflies, \( \beta_0 \) is the initial attractiveness of firefly and \( \gamma \) is a absorption coefficient.

3.2.3.2 Distance between fireflies

The distance between any two fireflies ‘\( i' \) and ‘\( j' \)’ at positions \( X_i \) and \( X_j \) respectively, can be defined as a Cartesian or Euclidean distance as follows:

\[
    r_{ij} = \|X_i - X_j\| = \sqrt{\sum_{k=1}^{d} (x_{i,k} - x_{j,k})^2} \tag{3.6}
\]

where \( x_{i,k} \) is the \( k \)-th component of the spatial coordinate of the \( i \)-th firefly and \( d \) is the total number of dimensions. Also ‘\( j' \) another firefly that must be distinct from firefly ‘\( i' \).

3.2.3.3 Movement of firefly

The movement of a firefly ‘\( i' \)’, when attracted to another more attractive (brighter) firefly ‘\( j' \)’, is determined by

\[
    X_i = X_i + \beta_0 e^{-\gamma r_{ij}} (X_j - X_i) + \alpha (rand - 0.5) \tag{3.7}
\]

The second term in Eq. (3.7) is due to attraction. The third term introduces randomization with ‘\( \alpha \)’ being the randomization parameter and ‘\( rand \)’ is a uniformly distributed random number between 0 and 1. In addition, if the scales of the problem
to be solved vary significantly in different dimensions, then the randomization parameter can be multiplied with the scale of the dimension to produce a vector of scaling values. The pseudo-code of the algorithm is given in Algorithm 3.1.

3.3 Proposed scheme

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

3.3.1 Redistributed block based SVD (RSVD)

A robust image watermarking used for ownership protection must be resistant to a variety of intentional and unintentional attacks. Singular value decomposition (SVD), is a powerful multimedia tool having numerous applications in image processing including digital image watermarking. Although most existing watermarking schemes based on block SVD have been survived against some common image processing attacks, but still not robust to the geometric distortions such as multiples of $90^\circ$ rotation and image flipping. To overcome this challenging problem redistributed block based SVD (RSVD) is introduced here. It is based on the fact [28] that a multiple of $90^\circ$ rotation and image flipping change only locations of the pixels in the image and their intensities leave unchanged. According to it, pixels’ locations of the image are redistributed and then some normalization procedures are performed. Subsequently, this image is segmented into blocks and SVD is applied to each block to collect the largest singular values for embedding. The watermark embedded to these locations is robust to the distortions mentioned above. Mathematically, it is formulated as:

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

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

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

Redistribute the original image ($A$), using the distribution relation given in Eq.(3.8) to obtain the redistributed image ($RI$).

$$RI (2i - 1, 2j - 1) = I(i, j), \quad 1 \leq i \leq M/2, 1 \leq j \leq N/2$$
$$RI (2i - 1, 2j - N) = I(i, 3N/2 - j + 1), \quad 1 \leq i \leq M/2, N/2 \leq j \leq N$$
$$RI (2i - M, 2j - 1) = I(3M/2 - i + 1, j), \quad M/2 \leq i \leq M/2, 1 \leq j \leq N/2$$
$$RI (2i - M, 2j - N) = I(3M/2 - i + 1, 3N/2 - j + 1), \quad M/2 \leq i \leq M/2, N/2 \leq j \leq N$$ (3.8)

If $|B_{21}| > |B_{12}|$, where the term $|*|$ is the absolute value operator, then transpose the image $RI$. Finally, the redistributed image ($RI$) is segmented into blocks and SVD is applied to get singular values that are invariant to multiples of $90^\circ$ rotation and row or column flipping. Therefore, the original image and its rotated and flipped versions have the same singular values obtained by RSVD.
3.3.2 Embedding Process

A watermark image \( W \) of size \( n \times n \) is embedded in to host image \( H \) of size \( m \times m \) by implementing the following steps:

**Step 1:** Watermark should be preprocessed first in order to improve the robustness and enhance the confidentiality. The binary watermark image is chaotically scrambled before embedding to increase the safety of the proposed watermarking scheme. The binary image as watermark data is scrambled by implementing the Arnold cat map up to a specified number of iterations, which is considered as a secret key.

**Step 2:** Apply redistributed block based SVD (RSVD) on host image by segmenting it into blocks of size \( 8 \times 8 \) to get the largest singular values.

**Step 3:** The watermark bit \( W_{ij} \) of the scrambled watermark is embedded by quantizing the largest singular value \( S_{ij} \) of \( ij \)-th block obtained in Step 2 utilizing an optimal quantization step \( Q \), which is obtained by firefly optimization algorithm. The largest singular values are quantized depending upon the watermark bits. Mathematically, the embedding process is given by:

\[
\begin{align*}
S^*_{ij} &= S_{ij} - (S_{ij} \mod Q) + 0.75 \times Q & \text{if } W_{ij} = 1 \\
S^*_{ij} &= S_{ij} - (S_{ij} \mod Q) + 0.25 \times Q & \text{if } W_{ij} = 0
\end{align*}
\]

(3.9)

**Step 4:** Replace the original blocks of the transformed host image by modified blocks respectively, and then apply the inverse process to get the watermarked image \( I_W \).

3.3.3 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:

**Step 1:** Apply Step 2 of the embedding process to the distorted watermarked image to get the singular values where the watermark bits were embedded.

**Step 2:** The watermark bits are extracted from these largest singular values using the relation given in Eq.(3.10). It is evident that this procedure does not need the cover image and hence our scheme is a blind one. If \( S^*_{ij} \) is the largest singular value where the watermark bit \( W^*_{ij} \) was embedded then it is extracted as follows:

\[
\begin{align*}
W^*_{ij} &= 1 & \text{if } (S^*_{ij} \mod Q) > Q/2 \\
W^*_{ij} &= 0 & \text{if } (S^*_{ij} \mod Q) < Q/2
\end{align*}
\]

(3.10)

**Step 3:** Apply the Arnold cat map on extracted watermark to get the embedded watermark.

3.3.4 Application of the Firefly algorithm in Finding Optimal Quantization step \( Q \)

Numerous researchers have dealt with solving the problem of image watermarking as an optimization problem. The objective function, in image watermarking, may
include various requirements (like, imperceptibility, robustness, capacity, etc.) that should be fulfilled by the given watermarking scheme. Here we have considered the objective function based on imperceptibility and robustness. Now the aim of firefly algorithm is to find the optimal quantization step that optimizes this objective function. Quantization step in the proposed watermarking scheme determines the watermark strength that controls the imperceptibility and robustness. Use of small quantization step favors the invisibility of the watermark, but the watermarked image is less robust to several common attacks. On the other hand, high quantization step favors the robustness, but the quality of watermarked image is unacceptable. Proper choice of quantization step for watermarking is more difficult than expected. Therefore, here we apply firefly algorithm to automatically determine quantization value to achieve a better performance. To start the algorithm, the fireflies are placed in random locations in the solution space of the problem. The location of a firefly corresponds to the values of the parameters of optimization problem to be solved. Then from each firefly’s newly acquired position, the objective function is evaluated, and the firefly’s brightness is set as the inverse of objective function value. The inverse has been used since the goal is to minimize the objective function. Thus a lower objective function value will result in a higher brightness. To evaluate the objective function a series of operations is done. The watermark is embedded into the host image by quantizing the singular values with the help of quantization step obtained by firefly algorithm. Then the watermarked image is distorted by implementing the three attacks; pixilation, JPEG compression and Gaussian low pass filtering. From these distorted watermarked images, watermarks are extracted using the extraction process. Peak signal to noise ratio (PSNR) and normalized correlation (NC) measures are used for imperceptibility and robustness respectively. Then the objective function Eq. (3.11) is computed for each firefly.

\[
\text{Minimize } f = 10 \times |\text{PSNR} - \text{PSNR}_{\text{target}}| + \left( 1 - \frac{1}{3} \sum_{i=1}^{3} \text{NC}_i \right)
\]  

(3.11)

where \(\text{NC}_i\) is the normalized correlation of extracted watermark corresponding to the \(i\)-th attack, and \(\text{PSNR}_{\text{target}}\) is a desired PSNR value equal to 40. The incorporation of the target PSNR transforms the optimization to a constrained procedure in order to ensure a minimum of image quality that must be acquired. After initialization, each firefly is compared to all the remaining fireflies, and will move towards every brighter firefly encountered. If a firefly finds the brighter firefly then the distance between these is calculated. With the distance between two fireflies the attractiveness is calculated to produce new solution. Subsequently, evaluate the objective function value at new solution. Continue the process till the termination criterion is not satisfied. At the end of the algorithm, we will obtain the near optimum quantization step. The simplest method for deciding when to stop the algorithm is to run it for a specified number of generations.
3.4 Results and Discussions

This section analyzes the performance of the proposed watermarking scheme under the various experiments. Ten test images of size $512 \times 512$ given in Fig. (3.2a - 3.2j) are taken as the host images. While the binary images of size $64 \times 64$ given in Fig. (3.2k - 3.2m) are taken as the watermark images. PSNR (peak signal-to-noise ratio) is used to analyze the visual quality of the watermarked image. To investigate the robustness of the proposed scheme twelve attacks are applied to the watermarked images: (1) average filtering (AF) with window size $3 \times 3$, (2) columns flipping (CF), (3) corner cropping (CR) 20%, (4) Gaussian low pass filtering (GF) with window size $3 \times 3$, (5) JPEG compression with quality factor 50, (6) motion blur with $(3,3)$ (MB), (7) median filtering (MF) with window size $3 \times 3$, (8) pixilation with window size $4 \times 4$ (PI), (9) rows flipping (RF), (10) rows and columns deletion (RCD), (11) rotation (RO) with $90^\circ$ anticlockwise, (12) resizing (RS)$512 \rightarrow 256 \rightarrow 512$. The algorithms are implemented in MATLAB environment on a PC with 4 GB RAM and Core 2 Duo processor. Normalized correlation (NC) coefficient is used as a similarity measure between the original and extracted watermark images. The optimal parameters setting of $\alpha$, $\beta_0 = 1.0, \gamma = 1.0$, population (number of fireflies) size $NP = 10$, and maximum generations 10 is considered as suggested in [41]. In order to justify the proposed approach RSVD, results are compared to the scheme based on SVD without implementation of redistribution and firefly. For the convenience we will call this scheme SVD. The quantization step ($Q$) used in SVD scheme is selected based on trial and error method. It can be observed from the Fig. (3.3), imperceptibility decrease with the increase of quantization step while the watermark extracted without error. Therefore, quantization step $Q = 50$ is selected for SVD here that have the acceptable quality of watermarked image with the extraction of watermark without error.

The PSNR values of the watermarked images obtained by the schemes SVD and RSVD are given in Table 3.1. In proposed scheme RSVD our aim is to achieve a target value 40db of PSNR. From the Table 3.1 it is clear that the obtained PSNR values are equivalent to the target PSNR value. Also, the results obtained by both the schemes are quite close to each other. A high PSNR value is the indication of better quality of the watermarked image under consideration. It shows that the good imperceptibility is obtained by the proposed scheme.

For the robustness experiments the distortions are applied on watermarked images and a sample of distorted images is shown in Fig. (3.4). For the visual quality analysis, the extracted watermarks are given in Table 3.3 and Table 3.4 respectively. From Table 3.3 and Table 3.4 it is clear that the extracted watermarks are almost similar to the original watermark. The quality of extracting watermarks is good in all the cases, but the quality of the extracted watermark in the case of rotation, flipping attacks are very poor obtained by the SVD scheme. The average of normalized correlation (NC) values of extracted watermarks over the test images obtained in each case are given in Table 3.2. Also, the results obtained by the algorithm based on SVD are given in the same table for the comparison. The best results are highlighted in bold for each case. From the Table 3.2 it is clear that the each scheme has extracted the watermark with high correlation values in all the cases except rotation and flipping.
Figure 3.2: (a) - (j) Host images Baboon, Cameraman, Clown, Couple, Elaine, Kiel, Lena, Lighthouse, Man, and Zelda respectively, (k) - (m) watermark images Butterfly, Horse, and CS.

Figure 3.3: Effect of employing different quantization step \( (Q) \) in SVD watermarking.
Table 3.1: PSNR values of the watermarked images with different watermark insertion by the different schemes.

<table>
<thead>
<tr>
<th>Image</th>
<th>SVD</th>
<th></th>
<th></th>
<th>RSVD</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
</tr>
<tr>
<td>Baboon</td>
<td>40.4631</td>
<td>40.4804</td>
<td>40.4736</td>
<td>39.9497</td>
<td>40.0375</td>
<td>40.1644</td>
</tr>
<tr>
<td>Cameraman</td>
<td>40.3301</td>
<td>40.3634</td>
<td>40.4247</td>
<td>40.1036</td>
<td>40.0745</td>
<td>39.9786</td>
</tr>
<tr>
<td>Clown</td>
<td>40.7295</td>
<td>40.6729</td>
<td>40.7545</td>
<td>40.0140</td>
<td>39.9714</td>
<td>40.0611</td>
</tr>
<tr>
<td>Couple</td>
<td>40.5359</td>
<td>40.3461</td>
<td>40.5178</td>
<td>39.9698</td>
<td>40.0591</td>
<td>39.9828</td>
</tr>
<tr>
<td>Kiel</td>
<td>40.3396</td>
<td>40.4775</td>
<td>40.4597</td>
<td>39.9206</td>
<td>40.0247</td>
<td>40.0973</td>
</tr>
<tr>
<td>Lena</td>
<td>40.4929</td>
<td>40.4463</td>
<td>40.4399</td>
<td>39.9633</td>
<td>39.9660</td>
<td>40.0313</td>
</tr>
<tr>
<td>Lighthouse</td>
<td>40.4738</td>
<td>40.6146</td>
<td>40.5714</td>
<td>39.9139</td>
<td>39.9288</td>
<td>39.9668</td>
</tr>
<tr>
<td>Man</td>
<td>40.5501</td>
<td>40.5577</td>
<td>40.4503</td>
<td>39.9866</td>
<td>39.9245</td>
<td>39.9486</td>
</tr>
<tr>
<td>Zelda</td>
<td>40.5158</td>
<td>40.3824</td>
<td>40.5180</td>
<td>39.9759</td>
<td>39.9785</td>
<td>39.9514</td>
</tr>
<tr>
<td>Average</td>
<td>40.4982</td>
<td>40.4932</td>
<td>40.5154</td>
<td>39.9779</td>
<td>39.9942</td>
<td>40.0073</td>
</tr>
</tbody>
</table>

Table 3.2: The average correlation values of the extracted watermark under different attacks and different schemes.

<table>
<thead>
<tr>
<th>Attack</th>
<th>SVD</th>
<th></th>
<th></th>
<th>RSVD</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
</tr>
<tr>
<td>NO</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>AF</td>
<td>0.8568</td>
<td>0.8587</td>
<td>0.8591</td>
<td>0.7967</td>
<td>0.8016</td>
<td>0.8093</td>
</tr>
<tr>
<td>CF</td>
<td>0.5059</td>
<td>0.5498</td>
<td>0.6455</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>CR</td>
<td>0.9022</td>
<td>0.9168</td>
<td>0.9373</td>
<td>0.9084</td>
<td>0.9256</td>
<td>0.9477</td>
</tr>
<tr>
<td>GF</td>
<td>0.9468</td>
<td>0.9468</td>
<td>0.9472</td>
<td>0.9613</td>
<td>0.9622</td>
<td>0.9620</td>
</tr>
<tr>
<td>JPEG</td>
<td>0.9994</td>
<td>0.9994</td>
<td>0.9996</td>
<td>0.9952</td>
<td>0.9954</td>
<td>0.9953</td>
</tr>
<tr>
<td>MB</td>
<td>0.9256</td>
<td>0.9266</td>
<td>0.9258</td>
<td>0.9207</td>
<td>0.9229</td>
<td>0.9243</td>
</tr>
<tr>
<td>MF</td>
<td>0.8877</td>
<td>0.8897</td>
<td>0.8895</td>
<td>0.8567</td>
<td>0.8625</td>
<td>0.8642</td>
</tr>
<tr>
<td>PI</td>
<td>0.8959</td>
<td>0.8970</td>
<td>0.8973</td>
<td>0.9440</td>
<td>0.9441</td>
<td>0.9446</td>
</tr>
<tr>
<td>RF</td>
<td>0.5137</td>
<td>0.5518</td>
<td>0.6621</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>RCD</td>
<td>0.7719</td>
<td>0.7719</td>
<td>0.7705</td>
<td>0.7717</td>
<td>0.7724</td>
<td>0.7717</td>
</tr>
<tr>
<td>RO</td>
<td>0.5146</td>
<td>0.5420</td>
<td>0.6489</td>
<td>1.0000</td>
<td>1.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>RS</td>
<td>0.9411</td>
<td>0.9416</td>
<td>0.9414</td>
<td>0.9355</td>
<td>0.9376</td>
<td>0.9393</td>
</tr>
</tbody>
</table>
cases where the performance of SVD is very poor in comparison to the RSVD. In addition, the advantage of the proposed scheme is that it automatically chooses the optimal quantization step depending on the image and watermark. It gives the freedom to the user not bothering about this parameter. The overall performance of the proposed algorithm is better than the SVD scheme.

Additionally, when coping with common image processing operations, both of the schemes show a similar perceptual quality and robustness; however, once the watermarked image is attacked by geometric transform, such as 90° multiples of integer rotation and image flipping, the SVD scheme fails completely, but the proposed scheme RSVD still works well. For a secure image watermarking scheme, robustness against attacks is an important issue. Actually, the security of information system depends on keys rather than the privacy of the scheme. In our proposed image watermarking scheme, we use the number of iterations for scrambling of watermark as the secret key to generate a chaotic version of the watermark for enhancing the security of the proposed scheme. Thus, without knowing the correct information about embedding it is impossible to detect the embedded watermark from the watermarked image.
Table 3.3: Extracted watermarks from the watermarked images that are distorted by various attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>SVD</th>
<th></th>
<th></th>
<th>RSVD</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
</tr>
<tr>
<td>NO</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>AF</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>CF</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>CR</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>GF</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>JPEG</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
<tr>
<td>MB</td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
<td><img src="image1" alt="Butterfly" /></td>
<td><img src="image2" alt="Horse" /></td>
<td><img src="image3" alt="CS" /></td>
</tr>
</tbody>
</table>
Table 3.4: Extracted watermarks from the watermarked images that are distorted by various attacks.

<table>
<thead>
<tr>
<th>Attack</th>
<th>SVD</th>
<th></th>
<th></th>
<th></th>
<th>RSVD</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
<td>Butterfly</td>
<td>Horse</td>
<td>CS</td>
<td></td>
</tr>
<tr>
<td>MF</td>
<td></td>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
<td><img src="image6" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>PI</td>
<td></td>
<td><img src="image7" alt="Image" /></td>
<td><img src="image8" alt="Image" /></td>
<td><img src="image9" alt="Image" /></td>
<td><img src="image10" alt="Image" /></td>
<td><img src="image11" alt="Image" /></td>
<td><img src="image12" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>RF</td>
<td></td>
<td><img src="image13" alt="Image" /></td>
<td><img src="image14" alt="Image" /></td>
<td><img src="image15" alt="Image" /></td>
<td><img src="image16" alt="Image" /></td>
<td><img src="image17" alt="Image" /></td>
<td><img src="image18" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>RCD</td>
<td></td>
<td><img src="image19" alt="Image" /></td>
<td><img src="image20" alt="Image" /></td>
<td><img src="image21" alt="Image" /></td>
<td><img src="image22" alt="Image" /></td>
<td><img src="image23" alt="Image" /></td>
<td><img src="image24" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td></td>
<td><img src="image25" alt="Image" /></td>
<td><img src="image26" alt="Image" /></td>
<td><img src="image27" alt="Image" /></td>
<td><img src="image28" alt="Image" /></td>
<td><img src="image29" alt="Image" /></td>
<td><img src="image30" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td></td>
<td><img src="image31" alt="Image" /></td>
<td><img src="image32" alt="Image" /></td>
<td><img src="image33" alt="Image" /></td>
<td><img src="image34" alt="Image" /></td>
<td><img src="image35" alt="Image" /></td>
<td><img src="image36" alt="Image" /></td>
<td></td>
</tr>
</tbody>
</table>
3.5 Conclusions

The proposed technique (RSVD) in this chapter has taken the advantage of an evolutionary technique called firefly algorithm for finding the suitable quantization step that is used in image watermarking. The watermark image is embedded into the host image in the redistributed SVD domain that is invariant to the rotation and flipping. The advantage of the proposed technique is that it automatically chooses the optimal quantization step depending on the image and watermark, while for the ordinary methods it is constant and needs the fine tuning for all the types of images. To investigate the robustness of the scheme several attacks are applied to seriously distort the watermarked image. Numerical and pictorial representation of the results have shown the efficiency of the proposed technique. In most of the cases watermark is extracted with high correlation value. The experimental results comparison with the other algorithm based on SVD has also shown the efficiency of the proposed scheme. Thus, our proposed scheme has satisfied the robustness, and imperceptibility, requirements that are essential for a robust watermarking scheme.

Acknowledgements

This work was supported under the framework of international cooperation program managed by NRF of Korea (NRF-2013K2A1B9066056).

References


[40] 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 decompo-


