

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

Musrrat Ali, Chang Wook Ahn, Millie Pant
Department of Computer Engineering, Sungkyunkwan University
Suwon-440746, Republic of Korea
e-mail: musrrat.iitr@gmail.com, cwan@skku.edu

Millie Pant
Department of Applied Science and Engineering, IIT
Roorkee-247667, India
e-mail: millifpt@iitr.ac.in

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 sacrificing 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

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, 1, 7, 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 degrades 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 8×8 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:

$$A = USV^T \quad (3.1)$$

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 $A^T A$ 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).

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \sigma_{r+2} \dots = \sigma_n = 0 \quad (3.2)$$

$$A = \sum_{k=1}^r \sigma_k u_k v_k^T \quad (3.3)$$

where u_k and v_k are the k -th eigenvector of U and V and σ_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:

$$\begin{bmatrix} p_i(x+1) \\ p_i(y+1) \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} p_i(x) \\ p_i(y) \end{bmatrix} \text{mod}(n) \quad (3.4)$$

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.

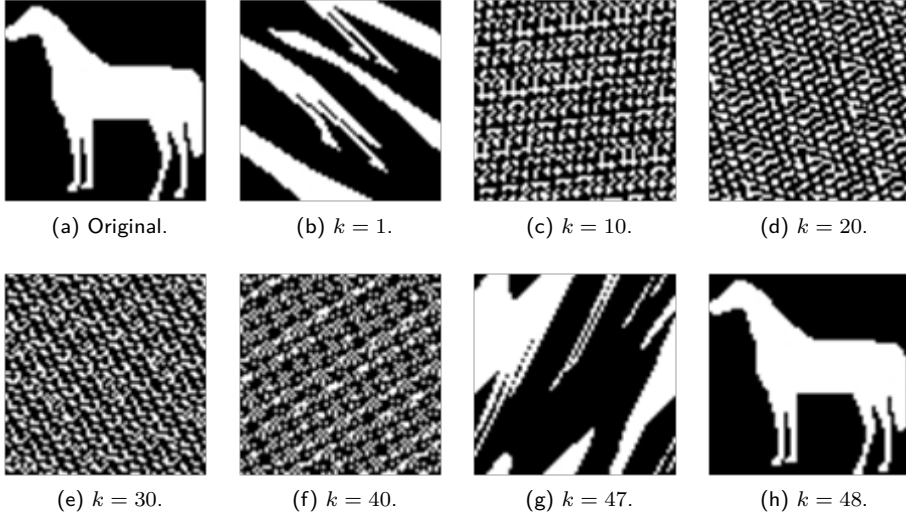


Figure 3.1: Illustration of Arnold cat map with different number of iterations.

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:

$$\beta = \beta_0 e^{-\gamma r^m}, m \geq 1 \quad (3.5)$$

Algorithm 3.1 Pseudo-code of Firefly Algorithm

```

Generate a uniformly distributed random population of  $NP$  fireflies
 $X_i, i = 1, 2, \dots, NP$ .
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, β_0 is the initial attractiveness of firefly and γ 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:

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

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

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

The second term in Eq.(3.7) is due to attraction. The third term introduces randomization with ' α ' 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° 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° 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 (2×2) , 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).

$$\begin{cases} RI(2i-1, 2j-1) = I(i, j), & 1 \leq i \leq M/2, 1 \leq j \leq N/2 \\ RI(2i-1, 2j-N) = I(i, 3N/2-j+1), & 1 \leq i \leq M/2, N/2 \leq j \leq N \\ RI(2i-M, 2j-1) = I(3M/2-i+1, j), & M/2 \leq i \leq M/2, 1 \leq j \leq N/2 \\ RI(2i-M, 2j-N) = I(3M/2-i+1, 3N/2-j+1), & M/2 \leq i \leq M/2, N/2 \leq j \leq N \end{cases} \quad (3.8)$$

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° 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 8×8 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:

$$\begin{cases} S_{ij}^* = S_{ij} - (S_{ij} \bmod Q) + 0.75 \times Q & \text{if } W_{ij} = 1 \\ S_{ij}^* = S_{ij} - (S_{ij} \bmod Q) + 0.25 \times Q & \text{if } W_{ij} = 0 \end{cases} \quad (3.9)$$

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:

$$\begin{cases} W_{ij}^* = 1 & \text{if } (S_{ij}^* \bmod Q) > Q/2 \\ W_{ij}^* = 0 & \text{if } (S_{ij}^* \bmod Q) < Q/2 \end{cases} \quad (3.10)$$

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.

$$\text{Minimize } f = 10 \times |PSNR - PSNR_{target}| + \left(1 - \frac{1}{3} \sum_{i=1}^3 NC_i \right) \quad (3.11)$$

where NC_i is the normalized correlation of extracted watermark corresponding to the i -th attack, and $PSNR_{target}$ 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 512×512 given in Fig.(3.2a - 3.2j) are taken as the host images. While the binary images of size 64×64 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 3×3 , (2) columns flipping (CF), (3) corner cropping (CR) 20%, (4) Gaussian low pass filtering (GF) with window size 3×3 , (5) JPEG compression with quality factor 50, (6) motion blur with (3,3) (MB), (7) median filtering (MF) with window size 3×3 , (8) pixilation with window size 4×4 (PI), (9) rows flipping (RF), (10) rows and columns deletion (RCD), (11) rotation (RO) with 90° 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 FA, $\alpha = 0.01$, $\beta_0 = 1.0$, $\gamma = 1.0$, 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

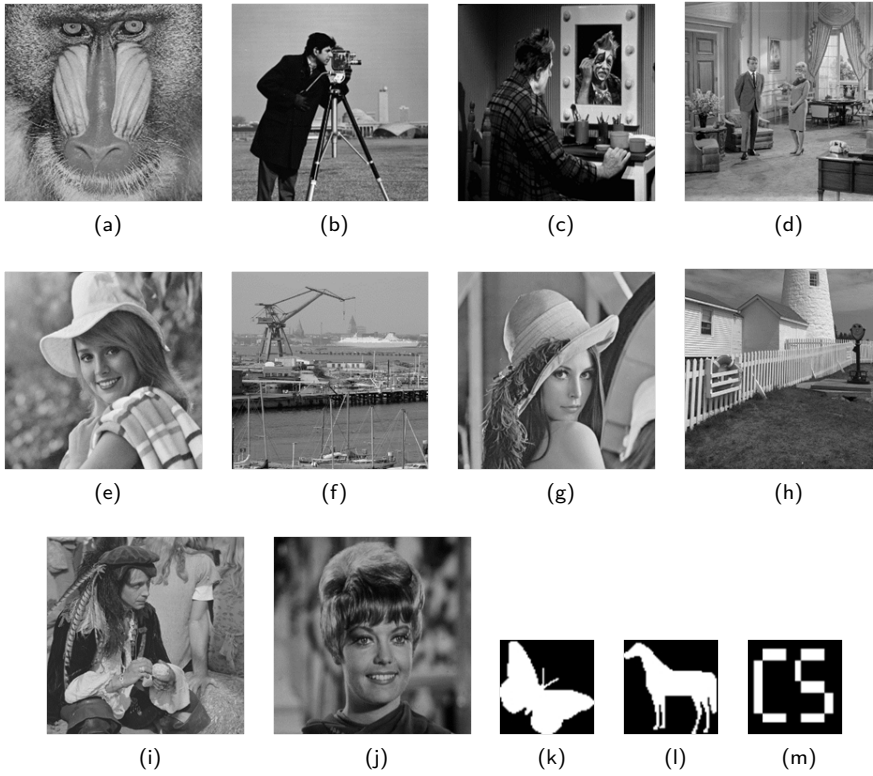


Figure 3.2: (a) - (j) Host images Baboon, Cameraman, Clown, Couple, Elaine, Kiel, Lena, Lighthouse, Man, and Zelda respectively, (k) - (m) watermark images Butterfly, Horse, and CS.

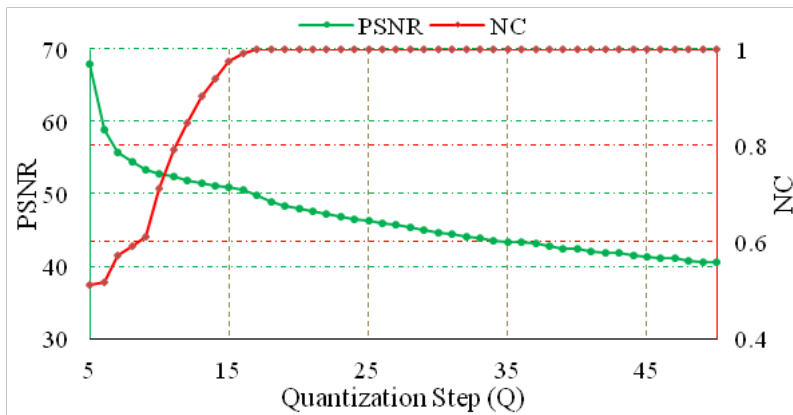


Figure 3.3: Effect of employing different quantization step (Q) in SVD watermarking.

Table 3.1: PSNR values of the watermarked images with different watermark insertion by the different schemes.

Image	SVD			RSVD		
	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>
Baboon	40.4631	40.4804	40.4736	39.9497	40.0375	40.1644
Cameraman	40.3301	40.3634	40.4247	40.1036	40.0745	39.9786
Clown	40.7295	40.6729	40.7545	40.0140	39.9714	40.0611
Couple	40.5359	40.3461	40.5178	39.9698	40.0591	39.9828
Elaine	40.5509	40.5907	40.5446	39.9815	39.9770	39.8910
Kiel	40.3396	40.4775	40.4597	39.9206	40.0247	40.0973
Lena	40.4929	40.4463	40.4399	39.9633	39.9660	40.0313
Lighthouse	40.4738	40.6146	40.5714	39.9139	39.9288	39.9668
Man	40.5501	40.5577	40.4503	39.9866	39.9245	39.9486
Zelda	40.5158	40.3824	40.5180	39.9759	39.9785	39.9514
Average	40.4982	40.4932	40.5154	39.9779	39.9942	40.0073

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

Attack	SVD			RSVD		
	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>
NO	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
AF	0.8568	0.8587	0.8591	0.7967	0.8016	0.8093
CF	0.5059	0.5498	0.6455	1.0000	1.0000	1.0000
CR	0.9022	0.9168	0.9373	0.9084	0.9256	0.9477
GF	0.9468	0.9468	0.9472	0.9613	0.9622	0.9620
JPEG	0.9994	0.9994	0.9996	0.9952	0.9954	0.9953
MB	0.9256	0.9266	0.9258	0.9207	0.9229	0.9243
MF	0.8877	0.8897	0.8895	0.8567	0.8625	0.8642
PI	0.8959	0.8970	0.8973	0.9440	0.9441	0.9446
RF	0.5137	0.5518	0.6621	1.0000	1.0000	1.0000
RCD	0.7719	0.7719	0.7705	0.7717	0.7724	0.7717
RO	0.5146	0.5420	0.6489	1.0000	1.0000	1.0000
RS	0.9411	0.9416	0.9414	0.9355	0.9376	0.9393

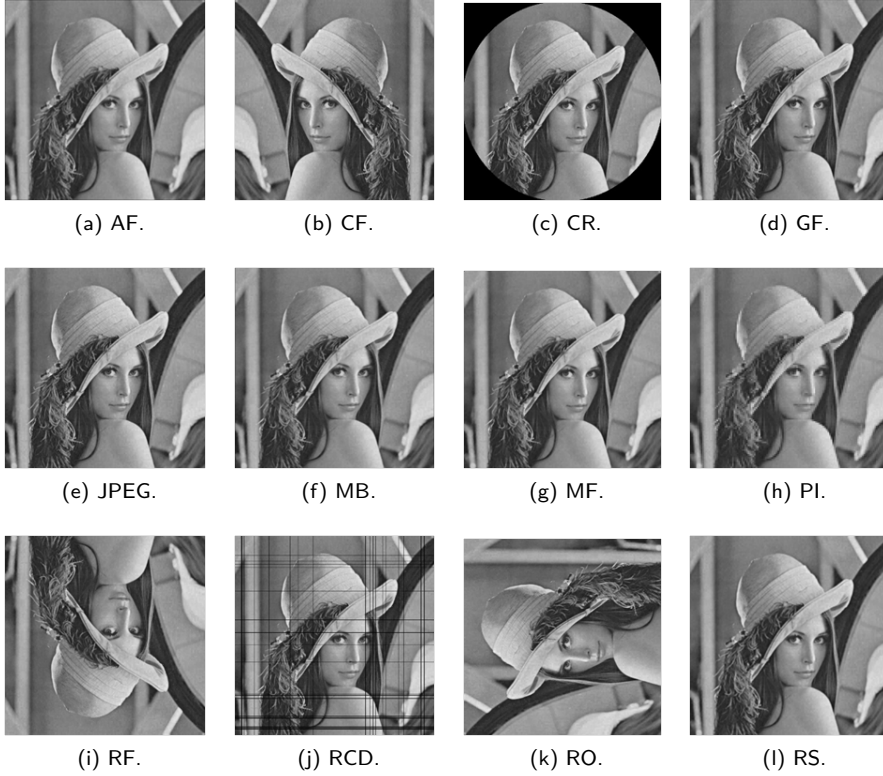


Figure 3.4: . (a) - (l) Watermarked images under different distortion attacks.

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.

























































































































Attack	SVD			RSVD		
	Butterfly	Horse	CS	Butterfly	Horse	CS
NO						
						
AF						
						
CF						
						
CR						
						
GF						
						
JPEG						
						
MB						

Table 3.4: Extracted watermarks from the watermarked images that are distorted by various attacks.

Attack	SVD			RSVD		
	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>	<i>Butterfly</i>	<i>Horse</i>	<i>CS</i>
MF						
						
PI						
RF						
RCD						
						
RO						
RS						

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

- [1] M. Ali and C.W. Ahn. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Processing*, 94:545–556, 2014.
- [2] M. Ali and C.W. Ahn. Comments on 'Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm'. *Expert Systems with Applications*, 42(5):2392–2394, 2015.
- [3] M. Ali, C.W. Ahn, and M. Pant. A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik - International Journal for Light and Electron Optics*, 125(1):428–434, 2014.
- [4] 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*, 301:44–60, 2015.
- [5] 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*, 31:15–26, 2014.
- [6] S.H. Amiri and M. Jamzad. Robust watermarking against print and scan attack through efficient modeling algorithm. *Signal Processing: Image Communication*, 29(10):1181–1196, 2014.
- [7] V. Aslantas. An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5):769–777, 2009.

- [8] G. Bhatnagar and Q.M. Jonathan Wu. A new logo watermarking based on redundant fractional wavelet transform. *Mathematical and Computer Modelling*, 58(1-2):204–218, 2013.
- [9] K. Chandrasekaran and S.P. Simon. Network and reliability constrained unit commitment problem using binary real coded firefly algorithm. *International Journal of Electrical Power & Energy Systems*, 43(1):921–932, 2012.
- [10] C.-C. Chang, P. Tsai, and C.-C. Lin. SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10):1577–1586, 2005.
- [11] 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*, 28:106–119, 2014.
- [12] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.
- [13] E.H. Elshazly, O.S. Faragallah, A.M. Abbas, M.A. Ashour, E.-S.M. El-Rabaie, H. Kazemian, S.A. Alshebeili, F.E. Abd El-Samie, and H.S.El-sayed. Robust and secure fractional wavelet image watermarking. *Signal, Image and Video Processing*, 2014. in press.
- [14] M.-Q. Fan, H.-X. Wang, and S.-K. Li. Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2):926–930, 2008.
- [15] E. Ganic and A.M. Eskicioglu. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *Journal of Electronic Imaging*, 14(4):043004–9, 2005.
- [16] J.-M. Guo and H. Prasetyo. False-positive-free SVD-based image watermarking. *Journal of Visual Communication and Image Representation*, 25(5):1149–1163, 2014.
- [17] 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*, 68(9):816–834, 2014.
- [18] M.-H. Horng. Vector quantization using the firefly algorithm for image compression. *Expert Systems with Applications*, 39(1):1078–1091, 2012.
- [19] M.-H. Horng and R.-J. Liou. Multilevel minimum cross entropy threshold selection based on the firefly algorithm. *Expert Systems with Applications*, 38(12):14805–14811, 2011.
- [20] H.-T. Hu and L.-Y. Hsu. Exploring DWT“cSVD”cDCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. *Computers & Electrical Engineering*, 41:52–63, 2015.
- [21] E. Hussein and M.A. Belal. Digital watermarking techniques, applications and attacks applied to digital media: a survey. *International Journal of Engineering Research & Technology*, 1(7):1–8, 2012.
- [22] A. Khan, A. Siddiq, S. Munib, and S. A. Malik. A recent survey of reversible watermarking techniques. *Information Sciences*, 279:251–272, 2014.
- [23] C.-C. Lai. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, 21(4):522–527, 2011.
- [24] C.-C. Lai. An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4):938–944, 2011.

- [25] J. Lang and Z.-G. Zhang. Blind digital watermarking method in the fractional Fourier transform domain. *Optics and Lasers in Engineering*, 53:112–121, 2014.
- [26] S.-H. Lee. DWT based coding DNA watermarking for DNA copyright protection. *Information Sciences*, 273:263–286, 2014.
- [27] B. Lei, E.-L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei. Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, 41(7):3178–3188, 2014.
- [28] L. Li, H.-H. Xu, C.-C. Chang, and Y.-Y. Ma. A novel image watermarking in redistributed invariant wavelet domain. *Journal of Systems and Software*, 84(6):923–929, 2011.
- [29] S.D. Lin, S.-C. Shie, and J.Y. Guo. Improving the robustness of DCT-based image watermarking against JPEG compression. *Computer Standards & Interfaces*, 32(1-2):54–60, 2010.
- [30] H.-C. Ling, R.C.-W. Phan, and S.-H. Heng. On an optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5):769–777, 2009.
- [31] H.-C. Ling, R.C.-W. Phan, and S.-H. Heng. On the security of a hybrid watermarking algorithm based on singular value decomposition and Radon transform. *AEU - International Journal of Electronics and Communications*, 65(11):958–960, 2011.
- [32] H.-C. Ling, R.C.-W. Phan, and S.-H. Heng. Comment on 'Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition'. *AEU - International Journal of Electronics and Communications*, 67(10):894–897, 2013.
- [33] J.-C. Liu and S.-Y. Chen. Fast two-layer image watermarking without referring to the original image and watermark. *Image and Vision Computing*, 19(14):1083–1097, 2001.
- [34] R. Liu and T. Tan. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 4(1):121–128, 2002.
- [35] K. Loukhaoukha. Comments on 'A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm'. *Digital Signal Processing*, 23(4):1334, 2013.
- [36] W. Lu, H. Lu, and F.-L. Chung. Feature based robust watermarking using image normalization. *Computers & Electrical Engineering*, 36(1):2–18, 2010.
- [37] S.P. Maity, S. Maity, J. Sil, and C. Delpha. Collusion resilient spread spectrum watermarking in M-band wavelets using GA-fuzzy hybridization. *Journal of Systems and Software*, 86(1):47–59, 2013.
- [38] S.P. Maity, S. Maity, J. Sil, and C. Delpha. Perceptually adaptive MC-SS image watermarking using GA-NN hybridization in fading gain. *Engineering Applications of Artificial Intelligence*, 31:3–14, 2014.
- [39] 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*, 67(2):102–112, 2013.
- [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-

- sition. *Digital Signal Processing*, 33:134–147, 2014.
- [41] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi. Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. *Expert Systems with Applications*, 41(17):7858–7867, 2014.
 - [42] A.A. Mohammad, A. Alhaj, and S. Shaltaf. An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing*, 88(9):2158–2180, 2008.
 - [43] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing*, 66(3):385–403, 1998.
 - [44] G.A. Papakostas, E.D. Tsougenis, and D.E. Koulouriotis. Moment-based local image watermarking via genetic optimization. *Applied Mathematics and Computation*, 227:222–236, 2014.
 - [45] S. Rastegar, F. Namazi, K. Yaghmaie, and A. Aliabadian. Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform. *AEU - International Journal of Electronics and Communications*, 65(7):658–663, 2011.
 - [46] S. Rawat and B. Raman. A chaotic system based fragile watermarking scheme for image tamper detection. *AEU - International Journal of Electronics and Communications*, 65(10):840–847, 2011.
 - [47] S. Rawat and B. Raman. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Processing*, 92(6):1480–1491, 2012.
 - [48] 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*, 39(1):673–689, 2012.
 - [49] M.J. Sahraee and S. Ghofrani. A robust blind watermarking method using quantization of distance between wavelet coefficients. *Signal, Image and Video Processing*, 7(4):799–807, 2013.
 - [50] S. Tedmori and N. Al-Najdawi. Image cryptographic algorithm based on the Haar wavelet transform. *Information Sciences*, 269:21–34, 2014.
 - [51] Y. Tian, T. Tan, Y. Wang, and Y. Fang. Do singular values contain adequate information for face recognition? *Pattern Recognition*, 36(3):649–655, 2003.
 - [52] G.C.-W. Ting. Ambiguity attacks on the Ganic-Eskicioglu robust DWT-SVD image watermarking scheme. In *Information Security and Cryptology (ICISC)*, volume 3935, pages 378–388, 2006.
 - [53] H.-H. Tsai, Y.-S. Lai, and S.-C. Lo. A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection. *Journal of Systems and Software*, 86(2):335–348, 2013.
 - [54] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai. Robust lossless image watermarking based on α -trimmed mean algorithm and support vector machine. *Journal of Systems and Software*, 83(6):1015–1028, 2010.
 - [55] X.-Y. Wang, Y.-P. Yang, and H.-Y. Yang. Invariant image watermarking using multi-scale Harris detector and wavelet moments. *Computers & Electrical Engineering*, 36(1):31–44, 2010.
 - [56] Y.-R. Wang, W.-H. Lin, and L. Yang. An intelligent watermarking method based on particle swarm optimization. *Expert Systems with Applications*, 38(7):8024–8029, 2011.

- [57] X. Wu and Wei Sun. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing*, 13(2):1170–1182, 2013.
- [58] X.-S. Yang. *Nature-inspired Metaheuristic Algorithms*. Luniver Press, 2008.
- [59] X.-S. Yang. *Stochastic Algorithms: Foundations and Applications*, volume 5792 of *LNCIS*, chapter Firefly Algorithms for Multimodal Optimization, pages 169–178. Springer Berlin Heidelberg, 2009.
- [60] E. Yavuz and Z. Telatar. Comments on 'A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm'. *Digital Signal Processing*, 23(4):1335–1336, 2013.
- [61] X.-P. Zhang and K. Li. Comments on 'An SVD-based watermarking scheme for protecting rightful Ownership'. *IEEE Transactions on Multimedia*, 7(3):593–594, 2005.
- [62] P.-P. Zheng, J. Feng, Z. Li, and M. Zhou. A novel SVD and LS-SVM combination algorithm for blind watermarking. *Neurocomputing*, 142:520–528, 2014.