

## Research Article

# Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm

Xiaoyi Zhou <sup>1</sup>, Chunjie Cao <sup>1</sup>, Jixin Ma,<sup>2</sup> and Longjuan Wang <sup>1</sup>

<sup>1</sup>*School of Computer Science and Technology, Hainan University, Haikou, China*

<sup>2</sup>*School of Computing and Mathematical Sciences, University of Greenwich, London, UK*

Correspondence should be addressed to Xiaoyi Zhou; [esther\\_z@qq.com](mailto:esther_z@qq.com) and Longjuan Wang; [40552382@qq.com](mailto:40552382@qq.com)

Received 24 May 2017; Revised 8 January 2018; Accepted 21 January 2018; Published 26 March 2018

Academic Editor: Mohamed F. Feteiha

Copyright © 2018 Xiaoyi Zhou 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 watermarking is an effective solution to the problem of copyright protection, thus maintaining the security of digital products in the network. An improved scheme to increase the robustness of embedded information on the basis of discrete cosine transform (DCT) domain is proposed in this study. The embedding process consisted of two main procedures. Firstly, the embedding intensity with support vector machines (SVMs) was adaptively strengthened by training 1600 image blocks which are of different texture and luminance. Secondly, the embedding position with the optimized genetic algorithm (GA) was selected. To optimize GA, the best individual in the first place of each generation directly went into the next generation, and the best individual in the second position participated in the crossover and the mutation process. The transparency reaches 40.5 when GA's generation number is 200. A case study was conducted on a  $256 \times 256$  standard Lena image with the proposed method. After various attacks (such as cropping, JPEG compression, Gaussian low-pass filtering (3, 0.5), histogram equalization, and contrast increasing (0.5, 0.6)) on the watermarked image, the extracted watermark was compared with the original one. Results demonstrate that the watermark can be effectively recovered after these attacks. Even though the algorithm is weak against rotation attacks, it provides high quality in imperceptibility and robustness and hence it is a successful candidate for implementing novel image watermarking scheme meeting real timelines.

## 1. Introduction

Digital watermarking technology is a significant research field of information hiding technology. It is also an important copyright enforcement scheme to protect copyright ownership as well as authentication source and integrity in the open network environment [1]. The concept of digital watermarking first appeared in the 1994 meeting, where van Schyndel et al. [2] made a speech entitled "A digital watermark," and it was first published in the international conference on digital watermark. Since then, the research of digital watermarking technology has been paid more attention and developed [3]. A digital watermark is a visible, or preferably invisible, identification code that is embedded in a digital multimedia product (text, audio, video, graphics, images, etc.). It is hidden in host information (images, audio, video, text, etc.) and becomes an inalienable part of it. Thus the watermark at least remains a recognizable state even if the host media are attacked through direct image processing.

With the purpose of effectiveness, a watermark shall have two characteristics [4]:

(1) Transparency: a watermark shall be perceptually invisible or its presence does not affect the work being protected.

(2) Robustness: a watermark must be at least difficult to remove without effective knowledge (e.g., the embedding location or the embedding intensity of a watermark in an image).

In order to get a trade-off between transparency and robustness, some scholars have introduced adaptive watermark algorithms [5, 6]. The basic principle is to take into account the local features of the host image and then to determine the watermark embedding position with the intensity change of the local features. One method is to determine whether the watermark will be embedded by means of the block variance of the image [6]. Another method is to analyze image block contents by fractal dimension to select images for

reflecting the blocks' texture characteristics and then adaptively embed a watermark with various intensity [5]. Recently, however, more scholars incline to the idea of statistical learning and machine learning for digital watermarking, such as SVM, neural network, GA, and fuzzy clustering [7], to find out the best position and to adjust the intensity with adaptive method. While these methods have attained good results, there are flaws lying in them. For instance, [5, 6] need to set threshold to differentiate image blocks from various images, which makes the algorithm complex to use. Neural network based method has an over-study problem and slow learning speed. GA is a highly parallel, random, and adaptive search algorithm but the generalization ability of primitive genetic algorithm is not very optimistic; thus it is easy to fall into the local optimal solution. SVM regression estimation can approximate any nonlinear function with arbitrary precision and has good generalization ability as well as other superior performances.

In view of the above analysis, based on the DCT domain, an improved scheme is proposed in this study by strengthening the embedding intensity with SVM and improving the embedding position with optimized GA, thus to increase the robustness and transparency of embedded information. In the case of JPEG compression, filtering, histogram equalization, rotation, cropping, and noise attacks, the watermark is extracted and is compared with the original watermark.

## 2. State of the Art

The embedding intensity and embedding position are the main factors that determine the two characteristics mentioned in the first section, and the intrinsic features of the image largely determine these main factors. Digital watermarking based on image features has attracted a large number of researchers for its robustness [5]. In this section, state of the art for digital watermarking schemes on the basis of SVM and GA, as well as their merits and flaws, will be presented and analyzed.

Genetic algorithm was first proposed by Professor Holland in the 1960s; his *Adaptation in Natural and Artificial Systems* published in 1975 marks the birth of genetic algorithm [8]. Since the international genetic algorithm conference was held in 1985, there has been genetic algorithm group meetings in some international conference on machine learning, artificial intelligence, and neural network, and genetic algorithm theory and its application of monographs have been published, in which Goldber's publication *Genetic Algorithms in Search, Optimization, and Machine Learning* [9] is one of the most influential monographs. In recent years, genetic algorithm has become an important branch of many scholars' research, and it has been widely used in different fields.

Baoming et al. [10] introduce a digital watermarking based on optimized tiny genetic algorithm and SVD method. In their scheme, watermark is embedded into the diagonal matrix according to an embedding intensity. After different attacks, a fitness function is employed to determine if the extracted watermark has reached the expectation. However, a small number of populations are not capable of maintaining multiple generations of variation. Chen and Huang [11]

presented a coevolutionary genetic watermarking scheme based on wavelet packet transform. Coevolutionary genetic algorithm is utilized to select an appropriate basis from permissible bases of wavelet packet transform and select proper subbands for watermark embedding. Nevertheless, the watermark is embedded in SVD domain, which causes large information transmission because of the left/right orthogonal matrices. Mohananthini and Yamuna [12] presented an optimization of multiple watermarking scheme with genetic algorithms. The embedding and extracting process uses the combination of discrete wavelet transform (DWT) and singular value decomposition (SVD). However, this algorithm adds the watermark information to the singular values of the diagonal matrix—this drawback is the same as Chen and Huang's algorithm. Lai [13] proposed a robust digital image watermarking technique based on a tiny genetic algorithm (Tiny-GA) and SVD. Lai uses the Tiny-GA to search the proper values with the intention of improving the transparency and robustness of the watermarked image. Experimental results show that Lai's algorithm is able to resist a variety of image processing attacks. However, this algorithm is fundamentally defective because the singular vectors matrices  $U$  and  $V$  of the watermark  $W$  will cause the false positive detection even if the embedded watermark is different or nonexistent.

Support vector machines (SVMs) are proposed by Cortes and Vapnik in 1995. They are supervised learning models which have shown many unique advantages in solving nonlinear and high dimensional pattern recognition with small samples. Vapnik proposed the VC-dimension (VC stands for Chervonenkis Vapnik) concept to ensure the minimum expected risk and to solve the problem of neural network overlearning [14]. Moreover, even with small samples, SVMs have the advantages of good training effect, strong generalization ability, computation complexity, and dimension increasing linearly.

Fuxin et al. [15] introduce a robust watermarking algorithm based on SVM regression. Because the images have many features, such as mean value, variance, skewness, and kurtosis, therefore, in this paper, SVM is trained by features made up of four shapes. The other part is to embed watermarks: use the trained SVM to predict the test patterns. Simulation results indicate that the proposed algorithm can obtain good perceptual invisibility and robustness against many attacks. However, this algorithm is vulnerable to JPEG compression. Wang et al. propose a novel image watermarking by extracting the significant bitplane from host image, then performing DWT on the extracted bitplane image [16]. After that, the corresponding low-pass subband is divided into small blocks. Finally, the processed watermark is embedded into host image by adaptively modulating the selected wavelet coefficients in the low-pass subband blocks. One of the advantages of this algorithm is that pseudo-Zernike moments of the significant bitplane image are calculated and taken as the effective feature vectors, which improves reasonable resistance toward geometric distortions. Nevertheless, flaws of the scheme are the computation of pseudo-Zernike moments. Zheng et al. present a new scheme for blind watermarking embedding and detection by applying SVD and LS-SVM (least squares support vector machine) [17]. In coding

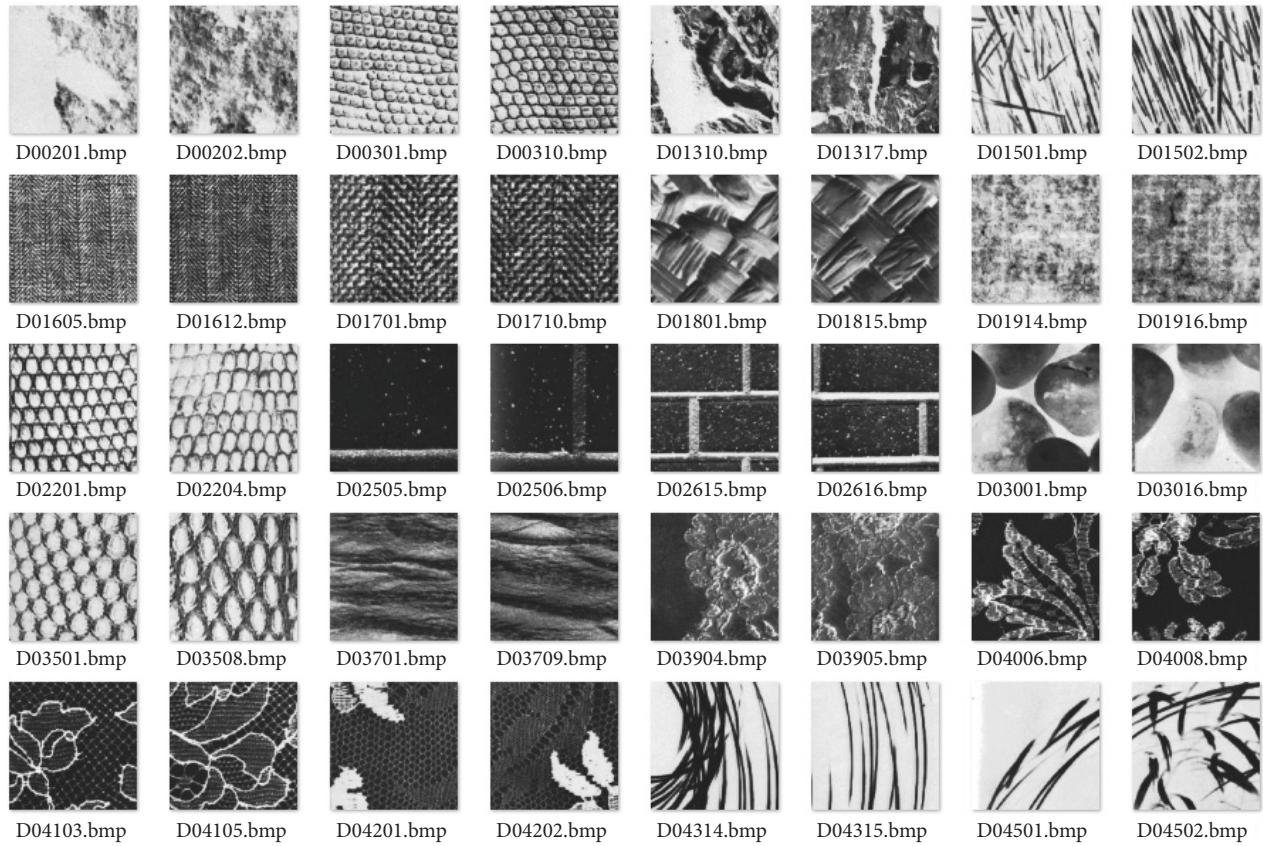


FIGURE 1: Images with different textures and brightness.

process, SVD is performed on coefficient blocks to obtain singular values after host image is transformed into IWT (integer wavelet transform) domain. Afterwards, watermark image is embedded by performing the corresponding numerical operation on the second value of the diagonal matrix. In decoding process, the trained LS-SVM is employed to extract the watermark image without the host image by classifying samples derived from watermarked image. However, the imperfection that lies in this algorithm is the use of SVD, which as discussed above will cause the false positive detection.

Different from the above SVM-based watermarking schemes, the proposed algorithm used SVM to classify textures, then the watermarking embedding intensity was determined according to the classifications. Compared with the texture-based classification method, the deformation model such as shape prior segmentation can deal with the objects of low contrast boundary; it is currently one of the most studied and the most widely used methods; even it can be considered the key to computer vision success in the past few years [18]. The deformation models provide an efficient image analysis method, which combines geometry, physics, and approximation theory. By using the constraints information (bottom-up) from image data and prior knowledge (top-down) from the objects' locations, sizes, and shapes, deformation model can effectively perform segmentation, matching, and tracking analysis to the objects. The main advantage of the deformation model is that it can directly produce closed parametric

curves or surfaces and has strong robustness against noise and pseudoboundary. Some deformation models utilize the prior knowledge such as shape prior knowledge and marking point set [19–21], which can make segmentation results more robust and accurate. However, prior knowledge is required to carry out sample training in advance. Moreover, human interaction is needed in training, and the change information of the shape of specific objects is calculated.

The remainder of this study is organized as follows. Section 3 introduces the procedure for embedding intensity and selecting position and establishes the mechanical model and proposes the algorithm. Section 4 discusses the experimental results by comparing other algorithms. Section 5 summarizes the conclusions and the suggested future work is presented.

### 3. Methodology

This section mainly describes the design idea of watermark embedding and the watermark embedding/extracting procedures.

*3.1. Embedding Intensity with SVM.* Adaptive embedding intensity is used in the proposed scheme. Therefore, the samples were trained by SVM to determine the intensity in each position. As to the sample selection, 50 pairs of images were selected from 2700 images in the texture library according to texture similarity and luminance contrast. Parts of the selected images are shown in Figure 1. As can be seen,

TABLE 1: Types of the image blocks.

| Texture | Brightness  |           |                |
|---------|-------------|-----------|----------------|
|         | Insensitive | Sensitive | More sensitive |
| Smooth  | $T_1$       | $T_2$     | $T_3$          |
| Edge    | $T_4$       | $T_5$     | $T_6$          |
| Texture | $T_7$       | $T_8$     | $T_9$          |

the selected image pairs are roughly the same, except a little change in the texture and brightness.

A certain number of 8-by-8 image blocks with different features were selected from these images. In this experiment, a total of 1600 image blocks were selected, and the different features of these image blocks were used as training set to feed SVM. Because the human eyes are sensitive variously to distinct textures and brightness, they can be used as two attributes for the features of image blocks.

Brightness can be determined by the image intensity; the calculation method is as follows:

$$b = \sum_{m=1}^8 \sum_{n=1}^8 \frac{(A(m, n) - 128)^2}{\beta}. \quad (1)$$

Here  $A(m, n)$  is the pixel value of position  $(m, n)$  in an  $8 \times 8$  block and  $\beta$  is a scale factor to balance the size of  $b$ .

Texture can be determined by entropy and variance of the images. The calculation method is as follows:

$$e = - \sum_{i=0}^{255} P(Z_i) \log_2 P(Z_i),$$

$$v = \sum_{i=0}^{255} (Z_i - u)^2 P(Z_i), \quad (2)$$

$$u = \sum_{i=0}^{255} Z_i P(Z_i).$$

Here,  $Z_i$  represents grey scale of an image, while  $P(Z_i)$  represents the grey level probability of a subblock.

For the difference of the brightness and the textures, so the image blocks were categorized into 9 types in accordance with the rules of Table 1.

In the experiment,  $T_1 \sim T_9$  were replaced by 1~9, respectively.

From the above steps, we can determine the sample matrix of the sample training set and the corresponding sample attribute matrix. Sample matrix contained  $(b, e, v)$  value of 1600 image blocks. The sample attribute matrix contained the corresponding categories of each image block.

By classification of each position from the original image, the mapping relation between the location and the corresponding embedding intensity can be obtained. Therefore, adaptive embedding intensity can be realized.

**3.2. Embedding Position with Optimized GA.** In this section, genetic algorithm has made a certain improvement. Specific changes are as follows:

(1) *Encoding.* The host image was divided into  $8 \times 8$  blocks; each block was embedded by only one watermark component. Let the number of the subblock be  $m \times n$  and let the size of the population be  $G$ ; then the encoding of the  $i$ th chromosome  $P^i$  is

$$P^i = \{p_1^i, p_2^i, \dots, p_{m \times n}^i\}, \quad p_k^i = [2, 3, \dots, 64]. \quad (3)$$

(2) *Selection.* Among many types of selection, roulette wheel is the most common type used in the population selection of each generation. Although this method is widely used and is easy to implement,  $t$  has some disadvantages. In roulette wheel selection, the probabilistic sequence is generated randomly for the next generation. Although it can ensure the randomness, it cannot guarantee that the best individual of the offspring will be able to participate in inheritance; thus it may produce the phenomenon of degeneration.

Hence the selection must be improved. The best individual of each generation is assigned to the population in the first position and the second position. Each generation of the best individual is mandatorily required to participate in inheritance.

In this optimized method, the best individual in the first place of each generation did not participate in any crossover and mutation procedure; it directly went into the next generation, until it was replaced by the better individuals. The best individual in the second position participated in the crossover and the mutation procedure, to ensure that the good part of the best individual is to take part in inheritance.

(3) *Crossover.* After the selection, offspring needed to be produced. The most common solution is called crossover, and while there are many different kinds of crossover, the most common type is single point crossover. In the single point crossover, a locus was chosen to exchange the remaining alleles from on parent to the other. But in practice, the experiment result is not very satisfying. Specifically for a length of 1024 watermarks, single point crossover has a major influence on an individual. It results in the concentration of crossover parts and the lacking stability for the individual fitness value, thus affecting inheritance stability.

Therefore, the crossover operation was carried out by adopting the combination of single point and multipoint crossover. At the beginning of crossover of two randomly selected individuals, the number of crossover points was determined by random number. After that, random number was again used in the selection of crossover probability for the selected crossover points. Finally, whether crossover was operated at each point was determined by comparing with the predefined crossover probability in the genetic process.

The method is rather similar to the multipoint crossover, but there is slight difference. In this method, the crossover position could be one or more, namely, uncertain. Moreover, the crossover probability of each position varied. Whether crossover needs to be carried out still requires further judgment. Through experiments, this method shows good results.

At the same time, as in the selection process, the best individual in the first position of each generation did not participate in the above crossover operation.

(4) *Mutation*. Genetic mutation exists in the process of biological evolution; the significance of mutation is to produce favorable genetic variation, to increase the fitness of individuals, and to pass on to the next generation. In our experiment, because of the particularity of individuals, it is impossible to generate a new numerical value as the conventional mutation operator. Only if the individuals met the conditions of mutation, one of the first two elements was randomly chosen from each individual sequence to swap one element from the latter two. Only note that the element of the best individual in the first position must not participate in the mutation process.

3.3. *Algorithm SOGA: Watermarking Based on SVM and Optimized GA*. This section mainly describes the procedure of watermark embedding and extracting.

3.3.1. *Communication Procedure*. Communication procedure consists of three main parts: watermark encryption (refer to [22]), watermark embedding, and extracting. The specific steps were as follows:

- (1) Key agreements: Alice and Bob agreed on a session key  $Q_{ab}$ .
- (2) Alice encrypted the watermark to enhance the security.
- (3) Alice embedded the watermark into a carrier image.
- (4) Alice sent Bob the watermarked image.
- (5) Bob extracted the watermark from the watermarked image and used the session key to decrypt the extracted watermark.
- (6) Bob verified whether the image was from Alice.

3.3.2. *Embedding Procedure*. Variable embedding intensity of the watermark embedding is used in the experiment. From Section 3.2, the mapping relation between a subblock of the host image and the corresponding embedding intensity has been obtained by SVM. As a result, the specific procedure was as follows:

(1) For a binary watermark image with the size  $M' \times N'$ , after  $W$  was encrypted, it was reduced to one-dimensional sequence. Denote it as

$$W = \{w_1, w_2, \dots, w_{m \times n}\}. \quad (4)$$

(2) Perform DCT on each subblock, then get a series of one-dimensional sequence according to the zigzag sequence. Denote it as

$$Y = \left\{ Y_k(i) \mid 1 \leq i \leq 64, 1 \leq k \leq \left\lfloor \frac{M}{8} \times \frac{N}{8} \right\rfloor \right\}. \quad (5)$$

(3) Calculate the corresponding value of DCT coefficient according to  $Y$ :

$$R(i) = \frac{8 \times 8}{M \times N} \sum_{k=1}^{(M \times 8) / (N \times 8)} \frac{Y_k(i)}{Y_k(1)}, \quad 2 \leq i \leq 64. \quad (6)$$

(4) Choose  $M' \times N'$  coefficients of various subblocks from  $Y$  for watermark embedding. It should be noted that the coefficient sequence of each subblock was only embedded by one bit of watermark. The selected subblock coefficient sequence was denoted as

$$B = \{B(i) \mid 1 \leq i \leq M' \times N'\}, \quad (7)$$

where  $i$  represented the serial number of the chosen subblock and  $B(i)$  represented the watermark embedding position in the subblock.

(5) Define

$$C = \{C(i) \mid 1 \leq i \leq M' \times N'\} \quad (8)$$

$$C(i) = Y_k(1) \times R(i), \quad 2 \leq i \leq 64,$$

where  $i$  was the same as it was in  $B$ .

(6) The embedding of the  $k$ th watermark was according to the relation between  $B(i)$  and  $C(i)$ , and the embedding rule was as follows:

$$B(k) = \begin{cases} C(k) - \alpha_k & \text{if } C(k) - B(k) < \alpha_k, w_k = 0 \\ C(k) + \alpha_k & \text{if } B(k) - C(k) < \alpha_k, w_k = 1 \\ B(k) & \text{else,} \end{cases} \quad (9)$$

where  $\alpha_k > 0$  was embedding intensity corresponding to the  $k$ th coefficient sequence of the selected subblock and  $B'(k)$  was the coefficient sequence of embedded watermark.

(7) After the watermark is totally embedded, recover  $B'$ , perform inverse zigzag and inverse DCT on the coefficient sequence of the subblocks, and then combine each subblock to get the final embedded watermark image.

The extracting procedure was the reverse of the embedding technique.

## 4. Result Analysis and Discussion

On the basis of the watermark embedding method narrated in Section 3, the experimental results will be discussed and analyzed in this section. All of the experiments of information hiding are tested on grey images of size 256-by-256 (as the cover image) and of size 32-by-32 (as the watermark).

4.1. *Transparency with the Number of GA's Generations*. Two important evaluation criteria of digital watermarking are transparency and robustness. The peak signal to noise ratio (PSNR) was applied to evaluate the transparency, which shows the quality of the watermarked image. PSNR is calculated by the following equation [23, 24].

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{I_h \times I_w \sum_{x=1}^{I_h} \sum_{y=1}^{I_w} (f(x, y) - g(x, y))^2} \text{dB}. \quad (10)$$

Here  $I_h$  and  $I_w$  are the height and width of an image  $I$ , respectively,  $f(x, y)$  is the pixel value of  $I$ , and  $g(x, y)$  is the

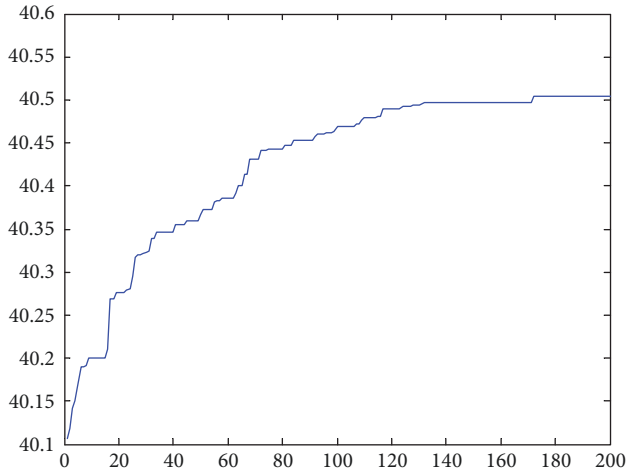


FIGURE 2: PSNR of the watermarked image with the increase of generation number.

pixel value of the other image  $I'$ . The higher value of PSNR, the less difference between  $I$  and  $I'$ .

The other evaluation method is the normalized cross-correlation (NC) between the original watermark and the watermark extracted from the watermarked image. NC is calculated by the following equation:

$$NC = \frac{1}{W_h \times W_w} \sum_{x=1}^{W_h} \sum_{y=1}^{W_w} W(i, j) \times W'(i, j). \quad (11)$$

Here  $W_h$  and  $W_w$  are the height and width of the watermark, respectively,  $W$  is the original watermark, and  $W'$  is the extracted watermark. The higher value of NC indicates the better quality of the extracted watermark.

The abscissa of Figure 2 represents the generation number, and the ordinate represents PSNR value of the watermarked image. As can be seen from the figure, transparency is gradually optimized along with the generations.

**4.2. Robustness against Various Attacks.** Considering both running time and transparency, to analyze how our scheme resists diverse attacks, we utilized the watermarked image optimized by 100 generations.

As can be seen from Figure 3, the proposed algorithm can effectively resist certain attacks with given parameters.

The following are some of the better counterattack ability comparing with other algorithms. It can be found that our algorithm has advantages in many aspects.

Figure 4 shows the proposed algorithm can effectively resist some attacks, such as rotation and histogram equalization. When the quality factor of JPEG attack rises to 90, the quality of the extracted watermark is the same as the algorithms proposed by Lin and HJizadeh. The experimental results of Enping et al., Lin et al., and HJizadeh et al. can be found in [25–27], respectively.

Next, the resistance ability against cropping attack is analyzed. As shown in Figures 5 and 6, after the standard Lena image is embedded, a watermark, except the extracted

watermark cropped by 3/4, can vaguely be recovered, and the rest are recognizable. Even if the watermarked image was cropped by 1/2, the restored watermark can be recognized in the rough outline.

It can be found that, even if the watermarked image is cropped by large area, the NC value of the extracted watermark image of our scheme is better than that obtained in [28–30]. So it is concluded that our algorithm has better cropping resistance. In particular, when the cropping range of the image is larger, the watermark recovery has advantages compared with other algorithms.

By comparing with other algorithms, it can be seen from Figure 7 that the proposed scheme has certain advantages in robustness. For the following kinds of attacks, JPEG, cropping, Gaussian low-pass filtering (3,0.5), histogram equalization, Image Darken, contrast increasing (0.5,0.6), contrast decreasing, Gaussian Noise (0.003), Salt-Pepper Noise (0.01), Product Noise (0.2), and Rotation and Speckle Noise, our algorithm can effectively recover the watermark.

**4.3. Time Complexity.** As illustrated in Section 3, the primary time-consuming operations of watermark embedding in this paper include four parts: DCT, IDCT, genetic algorithm, and SVM. The 2D DCT as well as its IDCT has complexity  $O(M \log M)$  [31], where  $M$  denotes the size of host image. SVM has complexity between  $O(Nsv^3 + Lt \times Nsv^2 + D \times Lt \times Nsv)$  and  $O(D \times Lt^2)$  [32], where  $Nsv$  denotes the number of support vectors,  $Lt$  is the number of training samples, and  $D$  is the dimension of each sample. The time-costing of genetic algorithm mainly lies in the operations of mutation, crossover, selection, and the calculation of the individual fitness value. According to [33], each of them has complexity of  $O(Sp \times Lc \times Ng)$ , where  $Sp$  denotes the population size,  $Lc$  denotes the length of the code, and  $Ng$  denotes the generation number.

Therefore, the total time complexity of the proposed algorithm is

$$O(M \log M + Nsv^3 + Lt \times Nsv^2 + D \times Lt \times Nsv + D \times Lt^2 + 4 \times Sp \times Lc \times Ng). \quad (12)$$

By running the experiment on Intel Core i7-6700 HQ CPU at 2.60 GHz and 2.59 GHz, the CPU time of DCT/IDCT is between 0.1 and 0.2, SVM is nearly 1, and genetic algorithm is between 180 and 190. This shows that the complexity of time depends mainly on the genetic algorithm. Therefore, (11) can be simplified to  $O(Sp \times Lc \times Ng)$ .

The watermark extracting procedure is the reverse of the embedding one, except that it does not need the SVM and the GA algorithms. That is to say, most of the time overhead is focused on the DCT and IDCT transform. Therefore, the time complexity is  $O(M \log M)$ .

## 5. Conclusion and Future Work

To enhance the robustness of watermarked image while considering the trade-off between transparency and robustness, a hybrid digital watermarking scheme based on DCT

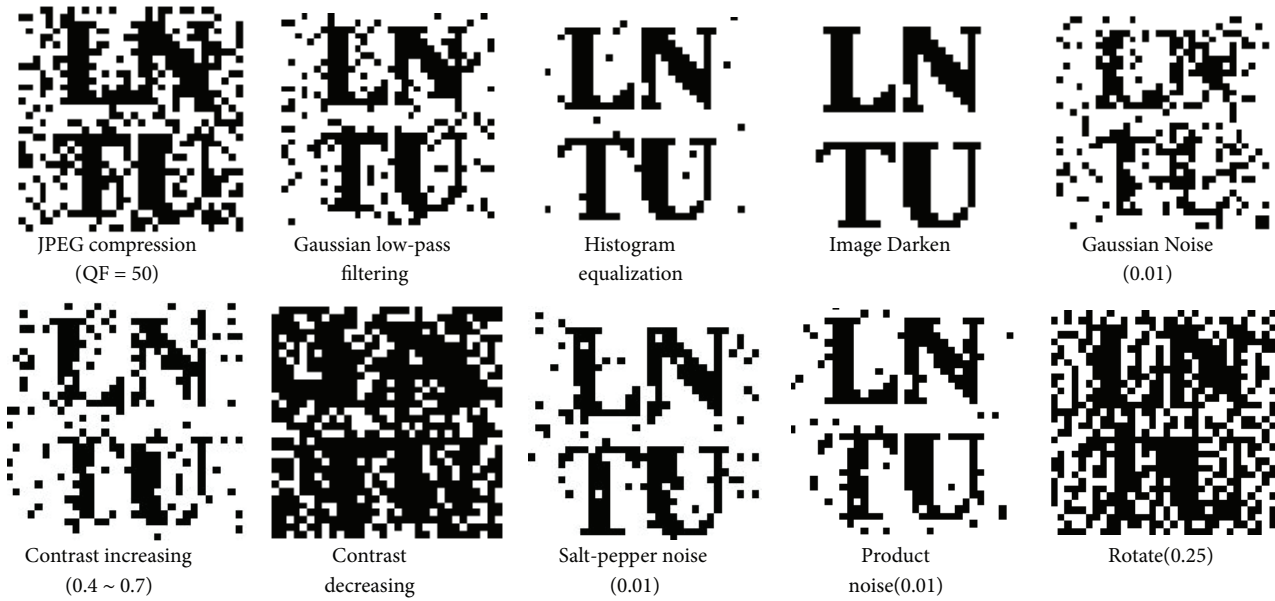


FIGURE 3: Extracted watermark under various attacks.

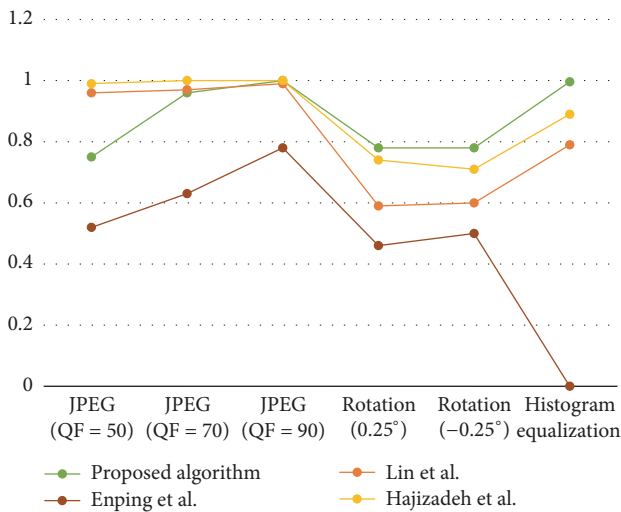


FIGURE 4: Comparison of the proposed algorithm with others under various attacks.

was proposed. The embedding intensity of the watermark was determined according to the texture types obtained by SVM, and the position of the watermark was embedded on the basis of the optimized GA. The result of extracted watermarks under various attack (e.g., JPEG compression, filtering, histogram equalization, rotation, cropping, and noise) and the comparison between the proposed scheme and other schemes were presented. The following conclusions could be drawn:

(1) The proposed scheme has shown both the significant improvement in perceptibility and the robustness under various types (filtering, rotation, cropping, noise, etc.) of image processing attacks.

(2) The proposed algorithm can effectively resist certain attacks such as JPEG compression, filtering, histogram equalization, rotation, cropping, and noise.

(3) Even though this algorithm is weak against rotation attacks, it extracts watermarks of higher quality than other algorithms under attacks such as JPEG compression, filtering, histogram equalization, rotation, cropping, and noise.

Therefore, the proposed method is a useful tool for ownership identification and copyright protection. However, there are still some limitations that lie in the methodology, as follows:

(1) the adaptive genetic operators are unrelated to the fitness function value, which may not ensure the convergence of the genetic algorithm.

(2) the sample classification using SVM is only by calculating the correlation value artificially, which may lead to inaccurate classification and make the “adaptive” algorithm less adaptive.

(3) DCT transform does not utilize spatial frequency characteristics of the image, and these characteristics coincide with some of the visual characteristics of the human eye. In addition, the use of block DCT causes the mosaic phenomenon to the reconstructed images.

Aiming at reducing the limitations, more work shall be considered in future studies, such as to relate the adaptive genetic operators to the fitness function value and ensure the convergence of the genetic algorithm; or to introduce other machine learning methods, such as neural network, to automatically calculate the embedding intensity; or to replace DCT with DWT, for the reason that DWT has the advantages of good spatial frequency characteristics and multiresolution representation and DWT has strong ability to resist noise and compression.

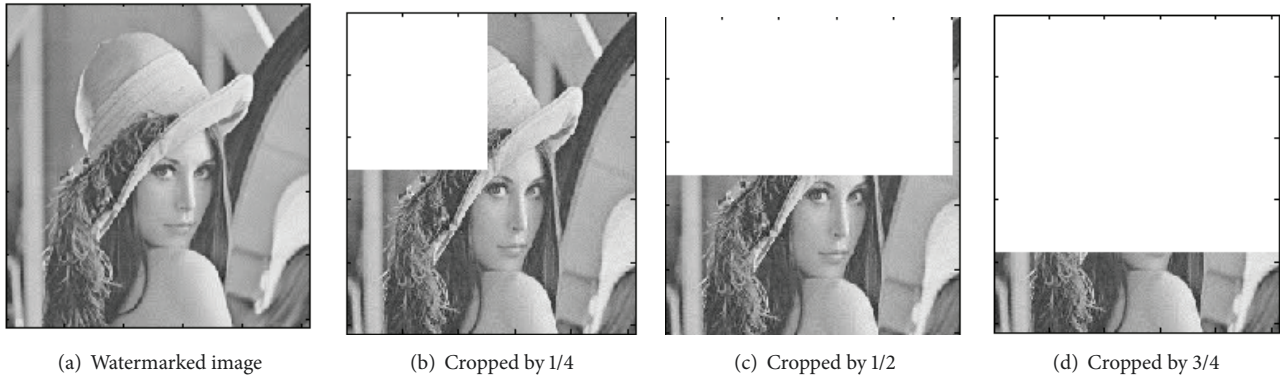


FIGURE 5: Watermarked image and the cropped ones.

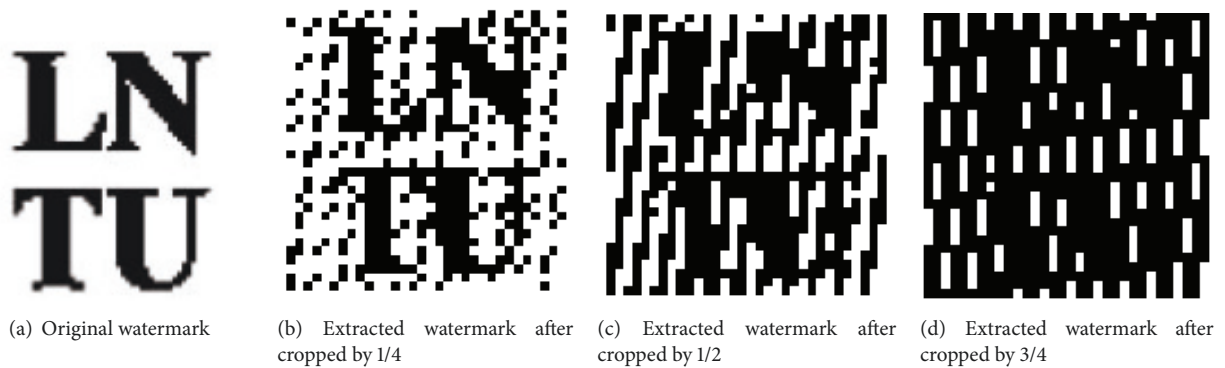


FIGURE 6: Extracted watermark after the watermarked image is attacked by cropping.

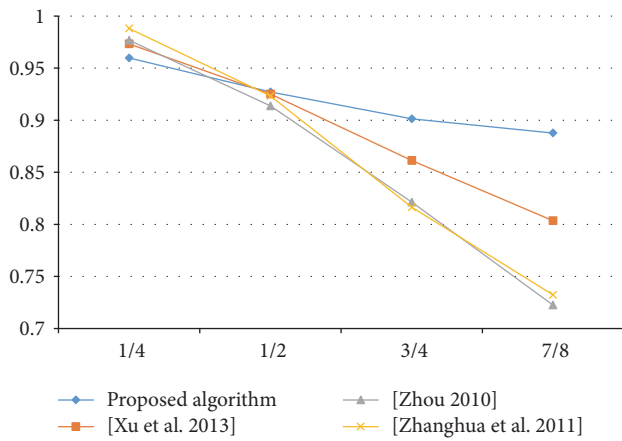


FIGURE 7: Comparison of the proposed algorithm with others under cropping attack.

### Conflicts of Interest

The authors declare that they have no conflicts of interest.

### Acknowledgments

The research was supported by Hainan Provincial Technology Project (Key Research and Development Project,

Grant no. ZDYF2017171), Hainan Provincial Natural Science Foundation (Grant no. 117063), Funding Scheme to Outstanding Scientific and Technological Programs by Chinese Students Abroad (Grant no. Human Society Notice [2015]192 and [2016]176-2), 2016 Hainan University Doctoral Science Research Foundation (Grant no. kyqd1648), and State Key Laboratory of Marine Resource Utilization in South China Sea.

### References

- [1] X. Y. Wang, Q. L. Shi, S. M. Wang, and H. Y. Yang, "A blind robust digital watermarking using invariant exponent moments," *AEU-International Journal of Electronics and Communications*, vol. 70, no. 4, pp. 416–426, 2015.
- [2] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the IEEE International Conference Image Processing (ICIP '94)*, vol. 2, pp. 86–90, Austin, Tex, USA, November 1994.
- [3] P. Chen, L. Yuan, Y. He, and S. Luo, "An improved SVM classifier based on double chains quantum genetic algorithm and its application in analogue circuit diagnosis," *Neurocomputing*, vol. 211, pp. 202–211, 2016.
- [4] A. Nikolaidis and I. Pitas, "Region-based image watermarking," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1726–1740, 2001.



- [5] F. Yang and L. Li, "An adaptive, SVM -based watermarking in frequency domain," in *Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition, ICWAPR*, pp. 465–469, China, August 2008.
- [6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.
- [7] J. Wang, L. Yaojin, and Y. Wang, "Blind watermarking scheme based on support vector machine and singular value decomposition," *Computer Science*, pp. 212–215, 2014.
- [8] J. H. Holland, *Adaptation in Natural and Artificial Systems*, MIT Press, Cambridge, Mass, USA, 1992.
- [9] D. E. Goldberg, *Genetic Algorithms in Search, Optimization And Machine Learning*, vol. 7, 1989.
- [10] S. Baoming, L. Hengjie, H. Yuanxiang, X. Yujuan, and S. Liang, "A robust digital watermarking scheme based on SVD and tiny genetic algorithm," *Journal of Lanzhou University of Arts and Science (Natural Sciences)*, vol. 28, no. 6, pp. 45–49, 2014.
- [11] Y.-H. Chen and H.-C. Huang, "Coevolutionary genetic watermarking for owner identification," *Neural Computing and Applications*, vol. 26, no. 2, pp. 291–298, 2014.
- [12] N. Mohananthini and G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," *Journal of Electrical Systems and Information Technology*, vol. 3, no. 1, pp. 68–80, 2016.
- [13] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Digital Signal Processing*, vol. 21, no. 4, pp. 522–527, 2011.
- [14] Y. X. Wang, N. Zhang, and Y. Y. Wang, "Robust watermarking scheme based on SVM and feature extraction," *Journal of Qingdao Technological University*, 2010.
- [15] W. Fuxin, S. Wei, and H. Jianjun, "Regression of SVM based robust watermarking algorithm," in *Proceedings of the 2008 9th International Conference on Signal Processing, ICSP 2008*, pp. 2197–2200, China, October 2008.
- [16] X.-Y. Wang, C.-P. Wang, A.-L. Wang, and H.-Y. Yang, "SVM correction based geometrically invariant digital watermarking algorithm," *Multimedia Tools and Applications*, vol. 72, no. 2, pp. 1933–1960, 2014.
- [17] 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.
- [18] T. McInerney and D. Terzopoulos, "Deformable models in medical image analysis: a survey," *Medical Image Analysis*, vol. 1, no. 2, pp. 91–108, 1996.
- [19] N. Duta, M. Sonka, and A. K. Jain, "Learning shape models from examples using automatic shape clustering and procrustes analysis," in *Proceedings of the Information Processing in Medical Imaging (IPMI'99)*, pp. 370–375, 1999.
- [20] C. Irapuato, "Unsupervised cardiac image segmentation via multiswarm active contours with a shape prior," *Computational and Mathematical Methods in Medicine*, vol. 3, 2013.
- [21] A. Afifi, T. Nakaguchi, and N. Tsumura, "Segmentation of deformable organs from medical images using particle swarm optimization and nonlinear shape priors," in *Proceedings of the Medical Imaging 2010: Image Processing*, USA, February 2010.
- [22] X. Zhou, J. Ma, W. Du, and Y. Zhao, "A Hybrid-key Based Image Encryption and Authentication Scheme with the Use of Ergodic Matrix," in *Proceedings of the 2nd International Symposium on Computer Network and Multimedia Technology (CNMT2010)*, pp. 212–217, Wuhan, China, 2010.
- [23] X. Zhou, J. Ma, W. Du, and Y. Li, "A dynamic multiple digital watermarking model based on temporal series," in *Proceedings of the 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2014*, pp. 367–371, China, November 2014.
- [24] X. Zhou, J. Ma, and W. Du, "SoW: A hybrid DWT-SVD based secured image watermarking," in *Proceedings of the 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, SNS and PCS 2013*, pp. 197–200, China, March 2013.
- [25] L. Enping, L. Huaqing, and N. Xinxin, "Blind image watermarking scheme based on wavelet tree quantization robust to geometric attacks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation, WCICA 2006*, pp. 10256–10260, China, June 2006.
- [26] W.-H. Lin, Y.-R. Wang, S.-J. Horng, T.-W. Kao, and Y. Pan, "A blind watermarking method using maximum wavelet coefficient quantization," *Expert Systems with Applications*, vol. 36, no. 9, pp. 11509–11516, 2009.
- [27] M. Hajizadeh, M. S. Helfroush, M. J. Dehghani, and A. Tashk, "A robust blind image watermarking method using local maximum amplitude wavelet coefficient quantization," *Advances in Electrical and Computer Engineering*, vol. 10, no. 3, pp. 96–101, 2010.
- [28] G. Xu, Y. Li, and X. Zhang, "Cropped-resistant spread spectrum watermarking algorithm based on magic-square transformation," *Qinghua Daxue Xuebao/Journal of Tsinghua University*, vol. 53, no. 8, pp. 1087–1090, 2013.
- [29] Y. Zhou, "A new color digital image blind watermarking algorithm protecting from shear transformation attack based on chaotic sequences and LWT," *Journal of Engineering Graphics*, vol. 31, no. 4, pp. 82–86, 2010.
- [30] Z. Zhanghua, S. Tan, and T. Lin, "Digital watermarking algorithm in DCT Based on chaotic scrambling and chaotic encryption," *Microelectronics & Computer*, vol. 5, pp. 58–62, 2011.
- [31] Z. Zhang, *Research on Digital Watermarking And Digital Fingerprinting Algorithm for Important Electronic File Protection*, Hangzhou University of Science and Technology, China, 2009.
- [32] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining & Knowledge Discovery*, vol. 2, no. 2, pp. 121–167, 1998.
- [33] Q. Cai, *Research and Application of Quantum Genetic algorithm in Blind Detection*, Nanjing University of Posts and Telecommunications, China, 2013.

