

RESEARCH

Open Access

# On the pinned field image binarization for signature generation in image ownership verification method

Mn-Ta Lee<sup>1</sup> and Hsuan Ting Chang<sup>2\*</sup>

## Abstract

The issue of pinned field image binarization for signature generation in the ownership verification of the protected image is investigated. The pinned field explores the texture information of the protected image and can be employed to enhance the watermark robustness. In the proposed method, four optimization schemes are utilized to determine the threshold values for transforming the pinned field into a binary feature image, which is then utilized to generate an effective signature image. Experimental results show that the utilization of optimization schemes can significantly improve the signature robustness from the previous method (Lee and Chang, *Opt. Eng.* **49**(9), 097005, 2010). While considering both the watermark retrieval rate and the computation speed, the genetic algorithm is strongly recommended. In addition, compared with Chang and Lin's scheme (*J. Syst. Softw.* **81**(7), 1118-1129, 2008), the proposed scheme also has better performance.

**Keywords:** Ownership verification, Image pinned field, Optimization, Content authentication, Genetic algorithm

## 1. Introduction

The advance of computer technology and the popularization of the Internet have resulted in convenient and fast exchange of multimedia contents. How to provide suitable techniques for protecting digital multimedia contents from malicious attacks has become an important and emergent issue. Digital watermarking techniques [1-4] have been massively proposed to protect digital rights. By embedding owner's watermarks such as logos, trademarks, seals, or copyright information into the digital content, an owner can claim one's ownership. According to the embedded domain of watermarks, digital watermarking techniques can be classified into two categories: the spatial and frequency domains. Embedding watermarks in the spatial domain is a straightforward method and has the advantages of low complexity and easy implementation [5-9]. However, there are disadvantages that image processing operations may easily destroy the watermarks. On the other hand, watermarks can be embedded in the frequency domain using

mathematical transforms such as the discrete Fourier transform (DFT), the discrete cosine transform (DCT), and the discrete wavelet transform (DWT) [10-13]. Watermarks embedded in the frequency domain are more robust but time-consuming because all the pixel values of the cover image are involved in the transform operation.

Embedding owner's watermarks into the digital multimedia contents usually results in a slight degradation, which is not suitable for valuable and sensitive digital multimedia contents such as artistic, medical, and military images. Therefore, how to conquer this problem is a major challenge in most of the digital watermarking techniques. Different from conventional watermarking schemes, some novel schemes combining the signature with digital watermarking-like techniques were proposed [1,14-17]. There are four advantages in these schemes. First, these methods are lossless because they do not modify the content of the protected image. Second, these methods do not need the original image during the authentication procedure, so they can satisfy the blind properties of digital watermarking. Third, embedding multiple watermarks is possible. Finally, they can resist counterfeit and copy attacks. The general model

\* Correspondence: htchang@yuntech.edu.tw

<sup>2</sup>Department of Electrical Engineering, National Yunlin University of Science and Technology, Yunlin, Taiwan, ROC

Full list of author information is available at the end of the article

for these combinational schemes is reviewed in this article.

Based on the general model mentioned above, we proposed a new scheme for image ownership verification using the pinned field of the cover image [18], according to the observation that the watermark robustness could be enhanced by using the feature of the cover image. The pinned field reflects the texture information by evaluating the average pixel values at block boundaries of the images and can be used as the feature of the cover image to enhance the watermark robustness. The reasons of choosing the pinned field as the image feature are given as follows:

1. The pinned field reflects the main edges and texture information in an image, which are important features robust to most of the attacks.

2. According to the definition in Ref. [18], to determine the pinned image, the pixel averaging operation is applied on the boundary pixels. Therefore, the pinned field image would be robust to the random noise and compression operations.

3. The pinned field image is determined in the spatial domain rather than being determined in the frequency domain. Instead of taking account of all pixels in an image, furthermore, the computations are only required on block boundaries. Therefore, the computation complexity is much less than that in the features determined in the frequency domain.

By using the average value of the pinned field as a threshold value, the pinned field is transformed into a binary feature image. Then, the binary feature image is combined with a scrambled watermark using exclusive-or (XOR) operation to form a signature image. Finally, by using a general signature generation system with owner's private key, the signature image is obtained. Experimental results show that the proposed scheme is robust to different signal-processing and geometric transformation attacks, and also outperforms a related scheme in the literature with respect to the retrieval rate of the embedded watermark.

In the previous scheme, the threshold values are used when transforming the pinned field of the cover image into a binary feature image. An intuitive scheme utilizes the average value of the block pixel values in the pinned field as the threshold value [18]. This scheme is simple, but may reduce the watermark robustness. If the threshold value is determined according to some criteria, the signature could be more robust although more time will be consumed. When the binary feature image is more similar to the global feature of the cover image, the watermark robustness can be enhanced, because most of the attacks cannot massively alternate the cover image. Otherwise, their malicious purpose will not be sustained anymore. Based on this observation, in this article four

optimization schemes, including the genetic algorithm (GA), simulated annealing (SA), shuffled complex evolution (SCE) and particle swarm optimization (PSO), are employed to determine the threshold values while transforming the pinned field of the cover image into a binary feature image. Experimental results show that the optimization schemes indeed achieve better performances in the watermark retrieval rate than our previous averaging scheme, and also outperform another related scheme. Consider simultaneously the computation speed and the performance of watermark robustness. The GA is superior to other optimization schemes in the proposed image verification method.

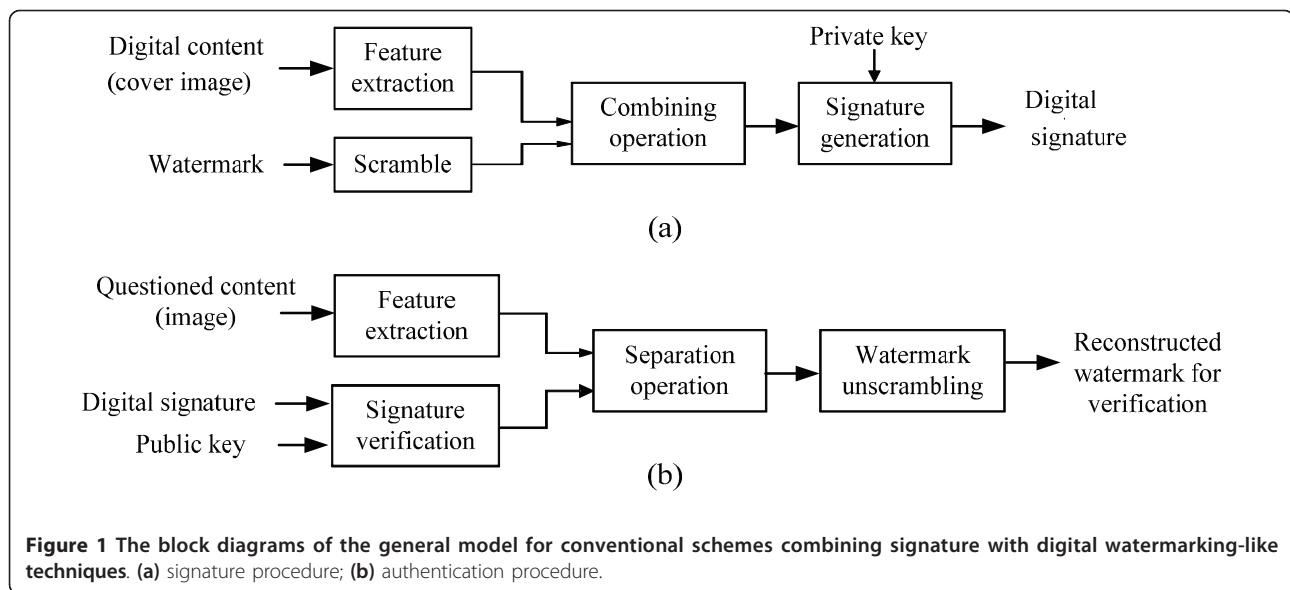
The rest of this article is organized as follows: In Section 2, the general model of the schemes which combine signature with digital watermarking-like techniques, our previous image ownership verification scheme, and the four optimization algorithms, are briefly described. The feature image binarization using the four optimization schemes in the proposed ownership verification are shown in Section 3. Experimental results for different types of image attacks and the comparison to another related scheme and our previous scheme are presented in Section 4. Finally, Section 5 concludes this study.

## 2. Background

In this section, we briefly introduce the background of the ownership verification system and the related techniques. First, the general model of the system, which combines the signature with digital watermarking-like techniques, is briefly described. Second, our previous image ownership verification scheme is presented. Finally, the GA and other optimization schemes are described.

### 2.1. The general model

Figure 1 shows the block diagram of a general model for the conventional data verification systems, which utilize the signature and digital watermarking-like techniques. There are two main parts in the general model: (1) the signature and the authentication procedures for generating an encrypted digital signature and (2) verifying the ownership of the digital content. In the signature procedure shown in Figure 1a, the features of digital content are extracted to increase the robustness and reduce the dimensionality. First, some of the features extracted in the methods including image-edge information [1], DCT [2], or DWT [17] are used. By using the features of digital content, the watermark robustness could be enhanced. Second, the watermark is scrambled to survive under geometric attacks. Third, the features of digital content are combined with the scrambled watermark by using a specific function to form the content with verification attributes. Finally, using the normal



signature generation system with the owner's private key to sign the content with verification attributes, a digital signature can be generated. Two main groups of normal signature generation systems, direct and arbitrated, can be employed to generate a digital signature. The main difference between the direct and the arbitrated signatures is that the latter needs an arbitrator. The scrambled watermark is combined with the features of digital content to form the content with verification attributes, which is required in the authentication procedure to extract the watermark. Thus, the protected digital content is not disturbed because none of the protected digital content is modified. Therefore, it can be applied to artistic and medical digital contents and does not need the original digital content during the authentication process.

In the authentication procedure shown in Figure 1b, it is basically an inverse of the signature procedure. First, given the questioned digital content, the same features are extracted. Second, the normal signature verification system and the owner's public key are employed to verify the digital signature. If the verification result is correct, the content with verification attributes is validated. Third, the reverse combination operation is applied to the extracted features of the questioned digital content with verification attributes, so a scrambled watermark is obtained. Finally, using the unscrambling process, the extracted watermark is obtained to demonstrate the copyright of the questioned digital content.

## 2.2. Our Previous Research

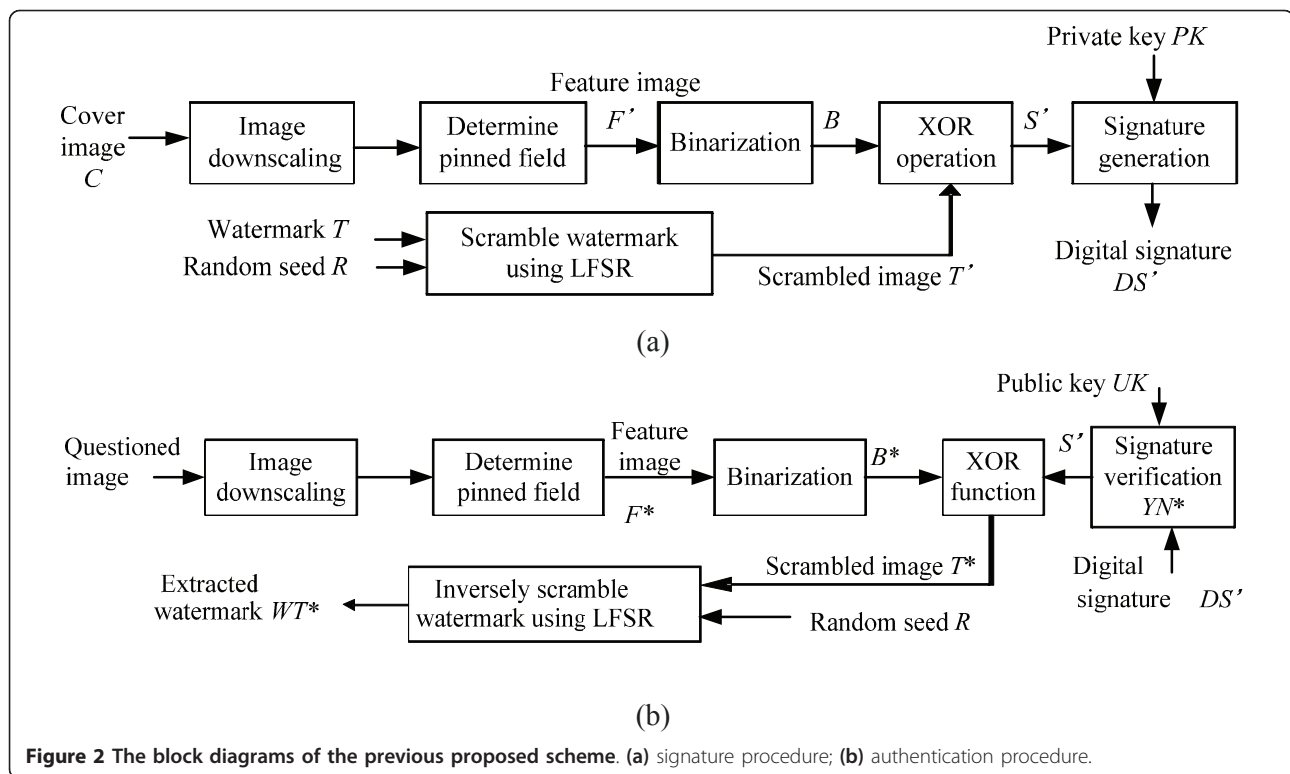
Based on the general model mentioned above, we had proposed a scheme for image ownership verification by using the pinned field of the cover image [18], according

to the observation that the robustness of watermarks could be enhanced using the robust features of the cover image. The pinned field [19-22] reflects the texture information of the cover image by evaluating the average pixel values at block boundaries of the image and is used as the feature of the cover image to enhance the watermark robustness.

The signature and authentication procedures are used in our previous scheme. In the signature procedure, the pinned field of the cover image is extracted as the feature. In the authentication procedure, the pinned field of the questioned image is also extracted for further watermark verification. Assume that the cover image  $C$  and the watermark  $T$  are grayscale images of size  $W_c \times H_c$  and  $W_t \times H_t$  pixels, respectively. The pinned field  $F$  of the cover image is first determined, and the final objective is to generate a digital signature. Figure 2a and 2b show the block diagrams of the signature generation procedure and the authentication procedure, respectively. The detailed descriptions of the previous method can be found in Ref. [18].

## 2.3. Genetic Algorithm and Other Schemes

GA [23] solves optimization problems via simulating the behaviors of biological evolution to obtain optimal solutions. GA is widely used in various fields such as pattern recognition, decision support systems, and the nearest optimization problem. There are mainly five components in GA: the random number generator, fitness evaluation, reproduction operation, crossover operation, and mutation operation. In general, GA starts at an initial population, called the first generation which was generated with some randomly selected genes. Each individual in the population corresponding



to a solution in the problem domain being addressed is called the chromosome. Associated with each chromosome is a fitness value computed by the fitness function. The fitness value is employed to evaluate the quality of each chromosome. The chromosomes with high quality will have greater probabilities to survive and form the population of the next generation. Through the operation of reproduction, crossover, and mutation, a new generation is regenerated from the chromosomes with high fitness values to find the best solution. The new generation will repeatedly apply the evaluation, reproduction, crossover, and mutation operations. After a constant number of iterations are reached or a predefined condition is satisfied, the overall process will be terminated and the approached optimal solution can be obtained.

The pseudo code for implementing the GA is described as follows:

**Method GA**

*Randomly generate an initial population with  $N$  chromosomes*

*Do*

*For each chromosome in the population*

*Evaluate fitness value using fitness function*

*End For*

*Select chromosomes with higher fitness value for reproduction*

*Cross parts of the selected chromosomes with the crossover rate*

*Mutate the gene values in the selected chromosomes with the mutation rate*

*Replace the current population with the new generated chromosomes*

*While the predefined condition is not satisfied*

**End Method**

In addition to the GA, there are many other global optimization techniques that can be applied to the pinned field image binarization in the proposed image signature method. In this article, three other well-known techniques, the SA [24], PSO [25], and SCE [26] schemes, are employed to make the comparison of the system performance with the GA scheme. In this article, these three techniques are briefly introduced as follows [27]:

(1) The algorithms of SA employ a stochastic generation of solution vectors. The concept is originated from the physical annealing process. During the cooling process, transitions are accepted to occur from a low to a high energy level through a Boltzmann probability distribution. SA has been proved that it is possible to converge toward the best solution. However, it may take more time than an exhaustive search.

(2) The PSO is a population-based stochastic optimization technique inspired by the social behavior of bird flocking or fish schooling. The underlying idea of PSO is the following: a swarm of particles moves around in the search space, and the movements of the individual particles are influenced by the improvements discovered by the others in the swarm. As the optimization progresses, the optimum will be discovered.

(3) In the SCE optimization algorithm, the initial population points are sampled randomly from the search space. The population is then partitioned into several complexes, each containing a fixed number of points. During the optimization, each complex evolves based on a statistical reproduction process that uses the simplex geometric shape to direct the search in the correct direction. After a defined number of iteration, the complexes are merged, shuffled, and the points are reassigned to a new set of complexes to ensure information sharing. As the optimization progresses, the entire population would converge toward the neighborhood of the global optimum when the initial population size and the number of complexes are sufficiently large.

### 3. Feature Image Binarization

As shown in Section 2.2, the image pinned field can partially represent the texture information of the cover image. By transforming the pinned field of the cover image into a binary feature image, the robustness of watermark can be enhanced. But how to determine the threshold values for the pinned field of the cover image while transforming it into a binary feature image is an important issue. There are various optimization schemes that can be employed to solve this problem.

Most of the attacks cannot massively alternate the cover image. Otherwise, their malicious purpose will not be sustained anymore. If the binary feature image can be more similar to the global feature of the cover image, the robustness of the generated watermark could be further enhanced. Based on this observation, various optimization schemes are employed to search for the optimal threshold values so that the generated binary feature image can lead to better signatures. The detail procedures are described as follows.

After the image pinned field has been extracted, the optimal threshold values for each non-overlapping block of the image pinned field are required for the following binarization process. Because the down-scaled cover image of size  $W_t \times H_t$  pixels is divided into non-overlapping blocks of size  $k \times r$  pixels while determining the image pinned field, there are totally  $(W_t \times H_t)/(k \times r)$  non-overlapping blocks. For each non-overlapping

block, an optimal threshold value must be determined while transforming the grayscale pinned field image  $F'$  into a binary feature image  $B$ . Therefore, there are totally  $(W_t \times H_t)/(k \times r)$  optimal threshold values needed to be resolved by using the optimization schemes.

While searching for the optimal threshold values for each non-overlapping block of the image pinned field, two values, i.e., the correlation and fitness values, must be calculated. The correlation value  $\text{corr}_{BD}$ , defined as in Equation 1, represents the similarity between the binary feature image  $B$  and the down-scaled cover image  $D$ . Both the images  $B$  and  $D$  are of size  $W_b \times H_b$  pixels. The correlation value is then employed to calculate the fitness value  $f_{\text{val}}$  of a solution in the optimization schemes. The fitness function to be minimized is defined as in Equation 2.

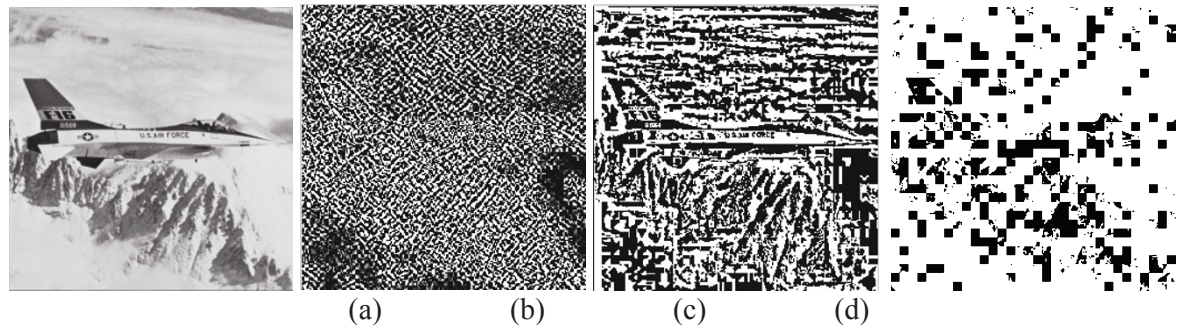
$$\text{corr}_{BD} = \frac{\sum_{j=1}^{H_b} \sum_{i=1}^{W_b} B(j, i)D(j, i)}{\sum_{j=1}^{H_b} \sum_{i=1}^{W_b} D(j, i)^2} \quad (1)$$

$$f_{\text{val}} = 1/\text{corr}_{BD} \quad (2)$$

After the optimal threshold, value  $P'(j, i)$  for each non-overlapping block in the pinned field has been determined using the GA, an optimal binary feature image  $B$  can be determined. For example, Figure 3a shows a cover image F16 of size  $256 \times 256$ , Figure 3b shows the pinned field image of Figure 3a with the block size  $8 \times 8$  and is of the same size  $256 \times 256$ , Figure 3c shows the binary feature image of Figure 3b using the average values of the pinned field as the threshold values, and Figure 3d shows the binary feature image of Figure 3b using the threshold values determined using the GA.

As shown in the block of XOR operation in Figure 2a, the determined binary feature image  $B$  are then combined with a scrambled watermark  $T'$  to create the signature image  $S'$ . Finally, the signature image  $S'$  are signed by using the normal signature generation system with the owner's private key  $PK$  to obtain the digital signature  $DS'$ .

In addition to the GA, three other optimization algorithms: the SA [24], PSO [25], and SCE [26], are used for pinned field image binarization for the comparison purpose. The initial array is of size  $1 \times (W_b \times H_b)/(k \times r)$ , in which each value is a random number within the range  $[0, 255]$  and is the initial threshold value of each block. The same fitness function shown in Equations 1 and 2 are employed in these optimization schemes. The parameters used in each optimization schemes are given as follows: In the SA scheme, the initial temperature is set as 100. The temperature function is set as



**Figure 3** The pinned field decomposition of the F16 image. (a) the source F-16 image; (b) the corresponding image field pinned; (c) binarized image after using the average value as the threshold values; (d) after using the GA to determine the threshold values.

temperature times  $0.95^i$ , where  $i$  denotes the iteration number. The maximum number of iterations is set as 50,000. In the PSO scheme, the number of particles in the swarm for each variable to be optimized is 60. The maximum number of iterations is 500. The cognitive acceleration coefficient and the social acceleration coefficient are 2.4 and 1.3, respectively. Finally, in the SCE scheme, the number of complexes is 5. The numbers of iterations in the inner loop and the maximum number of iterations are 20 and 60, respectively. Figure 4a-c show the binary pinned field images determined using the SA, PSO, and SCE schemes, respectively. It is to be noted that the image shown in Figure 4b is more similar to that in Figure 3d than the other two images shown in Figure 4a, c.

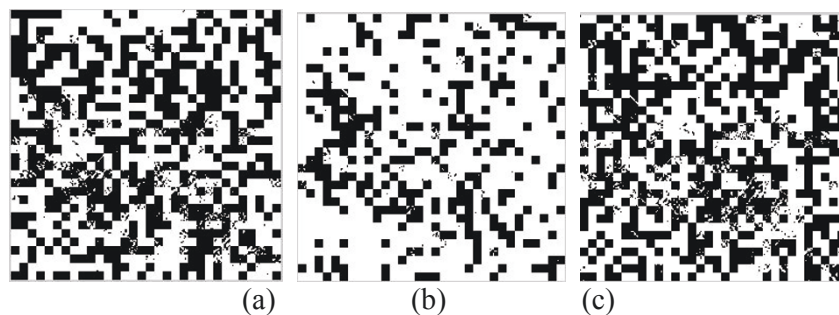
#### 4. Experimental Results

To demonstrate and analyze the watermark robustness of the proposed method, the experimental results obtained by applying external attacks, including signal processing attacks and geometric transformation attacks, are shown in this section. Five sets of the cover and watermark images are used in our experiments to study the performances of the proposed method. Figure 5a-e show the cover and

corresponding watermark images as Set 1 to Set 5. All the cover and the watermark images are grayscale with the sizes  $512 \times 512$  and  $64 \times 64$  pixels, respectively. The comparisons with another related scheme in the literature and our previous scheme are also given in this section.

##### 4.1. Generation of optimal threshold values using GA

In the proposed signature procedure, the cover image is down-scaled at first. Then, the pinned field of the down-scaled image is determined and employed to generate a feature signature using the GA with the fitness function defined in Equation 2. While searching for the optimal threshold values using the GA, each individual in a population consists of 256 variables because the down-scaled cover image is divided into 256 non-overlapping blocks of size  $4 \times 4$  pixels. Every variable represents a possible threshold value for each block of the pinned field image. The ten individuals with the highest fitness value are reserved for the new population of the next generation. The number of generations for each experiment is set to 300. The functions for fitness scaling, selection, mutation, and crossover are rank, roulette, uniform, and single-point functions in MATLAB, respectively.



**Figure 4** The determined binary pinned field images of the F16 image, which are obtained from using the three optimization schemes. (a) SA; (b) PSO; (c) SCE.



**Figure 5** Five sets of the test cover and watermark images. (a) Set 1; (b) Set 2; (c) Set 3; (d) Set 4; (e) Set 5.

While using the GA to solve optimization problems, the choice for values of GA's parameters is very important. The parameters used in the GA include the crossover rate, mutation rate, and population size. Initial values for each observed parameter are empirically chosen. Then, while one parameter is varied, the others are fixed to decide the proper value for this parameter. The GA runs 20 times for each different setting to obtain the average  $f_{val}$  which is employed to determine the proper value of the current observed parameter. For example, Tables 1, 2 and 3 summarize the experimental results for the Hill image in Set 1. The standard deviation is also computed, representing the variation of the  $f_{val}$  values with respect to the average  $f_{val}$  values. As shown in Tables 1, 2 and 3, all the standard deviations are less than 0.1, which indicates that the algorithm is running similarly in each round and is independent on the initial population.

Table 1 shows the results of average  $f_{val}$  value by varying the mutation rate. The best value of the mutation rate is 0.02 due to the lowest average  $f_{val}$  value. The results of average  $f_{val}$  value by varying the crossover rate are shown in Table 2. The best value of the crossover rate is 0.5. In the same manner, the results of average  $f_{val}$  value by varying the population size are shown in

**Table 1** Average results for different mutation rates of the Hill image

Mutation rate	Average $f_{val}$	Standard deviation
0.02	1.0958	0.0045
0.03	1.1033	0.0057
0.04	1.1108	0.0087
0.05	1.1117	0.0075

Crossover rate = 0.7 and population size = 80.

**Table 2 Average results for different crossover rates of the Hill image**

Crossover Rate	Average $f_{val}$ value	Standard deviation
0.5	1.095	0.005
0.6	1.097	0.006
0.7	1.096	0.005
0.8	1.101	0.006

Mutation rate = 0.02 and population size = 80.

Table 3. The best value of the population size is 140. Thus, the parameter values of the GA finally used for mutation rate, crossover rate, and population size are 0.02, 0.5, and 140 for the Hill cover image, respectively.

By using the GA, the optimal threshold values are obtained and then employed to transform the pinned field of the down-scaled Hill image into a binary feature image. Finally, a signature image is generated for the authentication purpose. For example, Figure 6a shows the pinned field of the down-scaled Hill image, Figure 6b shows the binary feature image of Figure 6a after applying the GA, and Figure 6c shows the final signature image.

#### 4.2. Results under attacks

The peak signal-to-noise ratio (PSNR) is employed to evaluate the quality between the cover and the attacked images. For the cover image  $C$  of size  $W_c \times H_c$  pixels, the PSNR is defined as the follow:

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{H_c W_c} \sum_{j=1}^{H_c} \sum_{i=1}^{W_c} |C(j, i) - A(j, i)|^2} \text{ dB}, \quad (3)$$

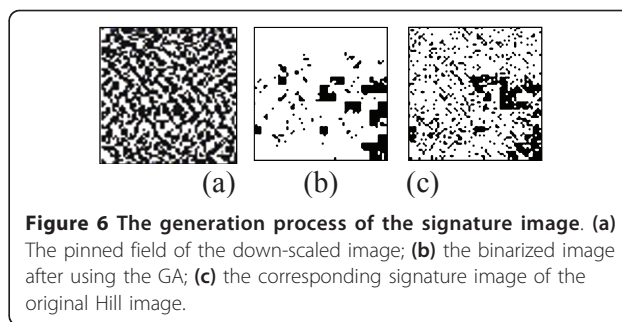
where  $C(j, i)$  and  $A(j, i)$  denote the grayscale values of the cover image  $C$  and the attacked image  $A$  at the pixel coordinate  $(j, i)$ , respectively.

In addition, the similarity between the original watermark  $T$  and extracted watermark  $T'$  is evaluated to estimate the robustness of the proposed copyright protection scheme under different attacks. The similarity is evaluated by the use of the watermark retrieval rate (RR), which is the percentage of the correct pixels recovered and defined as

**Table 3 Average results for different population sizes of the Hill image**

Population size	Average $f_{val}$ value	Standard deviation
80	1.096	0.005
100	1.090	0.004
120	1.089	0.003
140	1.086	0.002

Mutation rate = 0.02 and crossover rate = 0.5.



**Figure 6 The generation process of the signature image. (a)** The pinned field of the down-scaled image; **(b)** the binarized image after using the GA; **(c)** the corresponding signature image of the original Hill image.

$$RR = \frac{\sum_{j=1}^{H_t} \sum_{i=1}^{W_t} T(j, i) \text{ XOR } T'(j, i)}{H_t \times W_t} \times 100\%, \quad (4)$$

where  $T(j, i)$  denotes the grayscale value of the  $(j, i)$ th pixel in the original watermark  $T$ . It is obvious that the higher RR is, the higher similarity between the original and the extracted watermarks can be obtained. Furthermore, the average retrieval rate (ARR) is employed to evaluate the practicability of a copyright protection scheme for common attacks and is defined as

$$ARR = \left( \sum_{i=1}^{NA} RR \right) / NA, \quad (5)$$

where NA is the number of the examined attacks.

For Set 1 images, Table 4 shows the experimental results of the watermarks extracted from the proposed scheme under different attacks. These attacks include applying signal processing schemes and geometric transformations on the cover image. From these results, the retrieved watermark is still recognizable even though the PSNR value of the attacked image is low. Here the various attacks used in the experiments are summarized as follows:

Attack (1) Image Blurring: A Gaussian filter with  $9 \times 9$  kernel coefficients is applied to the cover image, and thus, a blurring image is obtained.

Attack (2) Surround Cropping: A surround cropping is applied to the cover image and only 74% of original size is left.

Attack (3) Quarter Cropping: A quarter cropping is applied to the cover image and only 75% of original size is left.

Attack (4) Noising: While digital images are transmitted on the Internet, they may be interfered with Gaussian noise. Here, the additive Gaussian noise with a zero mean value and the variance value 0.01 is applied to the cover image.

Attack (5) JPEG lossy compression: Images are usually compressed before transmission or storage, so the watermark should be robust to any compression



**Table 4 The attacked images, the corresponding PSNR values, the retrieved watermark images, and the corresponding RR values**

	Image blurring	Surround cropping	Quarter cropping	Nosing
Attacked image				
PSNR(dB)	38.71	11.24	11.77	11.38
Retrieved watermark				
RR	98.27%	96.48%	97.17%	95%
	JPEG	Scaling	Sharpening	Median filtering
Attacked Image				
PSNR (dB)	30.37	25.36	18.45	26.15
Retrieved watermark				
RR	98.29%	98.22%	98.29%	97.46%
	Average filtering	Gamma correction	Histogram equalization	Pixel shifting
Attacked Image				
PSNR (dB)	24.43	12.80	11.53	2.69
Retrieved watermark				
RR	97.02%	97.9%	96.78%	89.6%

schemes. The JPEG is one of the most efficient compression techniques. A JPEG lossy compression with quality factor 95 is applied to the cover image to generate a compressed image.

Attack (6) Scaling: The cover image is resized to 256 × 256 pixels at first and then is enlarged to 512 × 512 pixels.

Attack (7) Sharpening: A linear mapping is applied to the cover image to generate a sharpening image.

Attack (8) Median filtering: Median filtering is a non-linear operation and is often employed to reduce “salt

and pepper” noise in images. A median filter with 9 × 9 kernel coefficients is applied to the cover image to generate a filtered image.

Attack (9) Average filtering: Average filtering blurs an image, especially in the edge part. An average filter with 9 × 9 kernel coefficients is applied to the cover image to generate a blurred image.

Attack (10) Gamma correction: A gamma value 0.7 is applied to the cover image to generate a brighter image.

Attack (11) Histogram equalization: Histogram equalization enhances the contrast of images by manipulating

the pixel values such that the histogram of the output image approximately matches a specified histogram. Uniform histogram equalization is applied to the cover image to generate a histogram equalization image.

Attack (12) Pixel shifting: A  $60 \times 60$  pixels shifting is employed to the cover image to generate a pixel-shifting image.

As shown in Table 4, all the RR values are greater than 89.5%, which means that the recovered watermarks are highly correlated with the original one. Therefore, embedding the watermark into the pinned field of the cover image and optimizing the similarity between the pinned field and the cover image through GA is an efficient way and is robust to different types of attacks.

### 4.3. Comparison results

The proposed scheme is compared with Chang and Lin's adaptive scheme [1] and our previous scheme [18]. The key idea of Chang and Lin's adaptive scheme is to use Sobel operator to extract the edge information of the copyright image. The edge information is employed to represent the feature of the copyright image.

Sobel operator [28,29] is an edge detection approach, which utilizes the kernels to detect the edge directions: horizontal, vertical, and diagonal. In Chang and Lin's article, let  $a, b, c, d, e, f, g,$  and  $h$  be the eight neighboring pixels of an input pixel  $y$  of an image. The corresponding positions of pixels  $a, b, c, d, e, f, g,$  and  $h$  are on the upper left, top, upper right, left, right, lower left, bottom, lower right of the pixel  $y$ , respectively. The four Sobel kernels of the input pixel  $y$  are defined as follows:

Horizontal kernel

$$K(H) = (a + 2b + c) - (f + 2g + h)$$

Vertical kernel

$$K(V) = (c + 2e + h) - (a + 2d + f)$$

Left diagonal kernel

$$K(LD) = (d + 2f + g) - (b + 2c + e)$$

Right diagonal kernel

$$K(RD) = (b + 2a + d) - (e + 2h + g)$$

For the above equations,  $K(H)$  represents the variance of pixel  $y$  in the horizontal direction,  $K(V)$  denotes the variance of input pixel  $y$  in the vertical direction,  $K(LD)$

indicates the variance of pixel  $y$  in the left diagonal direction, and  $K(RD)$  is the variance of pixel  $y$  in the right diagonal direction. These four variances are then employed to evaluate the gradient  $\nabla g(y)$  of the input pixel  $y$ , which is defined as

$$\nabla g(y) = \sqrt{K(H)^2 + K(V)^2 + K(LD)^2 + K(RD)^2} \quad (6)$$

The input pixel  $y$  is considered to be an edge point, if  $\nabla g(y) > t$ . Otherwise, the input pixel  $y$  is considered to be a non-edge point. The parameter  $t$  is a threshold value decided by the user.

In Chang and Lin's article, the extracted edge information is employed to represent the feature of the copyright image. The image owner can use the parameter  $t$  to adjust the watermark robustness to fit personal requirement. Tables 5 and 6 show the RR comparison results with Chang and Lin's and our previous schemes on Sets 1 and 2-5 images, respectively. In both tables, the proposed method significantly improves the RR values under the attacks of the cropping, histogram equalization, and pixel-shifting operations from Chang and Lin's scheme. On the other hand, our scheme has better ARR than Chang and Lin's scheme with different parameter  $t$ . While comparing with our previous scheme, which uses the average value of the pinned field as a threshold value, the GA scheme significantly improves the RR values under the attacks of the cropping, additional noise, and especially the pixel-shifting operations from our previous scheme and has better ARRs.

Finally, the comparisons of the GA, PSO, SA, and SCE schemes mentioned in Section 2.3 are performed for the same image sets (Sets 1-5). In the experiments, the MATLAB implementations of these three schemes are modified from the versions shown in Donckels' website [27]. It is to be noted that the used SA scheme contains an algorithm that was described in Cardoso et al. [30] and is based on the combination of the non-linear simplex and SA algorithms (denoted as the SIMPSA algorithm). Table 7 shows the RR results corresponding to the GA and the other optimization schemes for Set 1 images. The PSO scheme shows the best performance, especially for the pixel-shifting attack. The GA shows comparable performance with the PSO scheme. The similar comparison result is obtained in Table 8 which shows the RR results for Sets 2-5 images. Consider the computation complexity of the whole system. Table 9 shows the computation time for each optimization scheme. The GA shows the speed that is at least four times faster than that of the PSO scheme. Therefore, considering both the RR results and the computation speed, we choose the GA as the most efficient way for the pinned field image binarization process.

**Table 5 The Comparison of RR average results among the proposed, chang and lin's, and previous averaging schemes for set 1 images**

Operation	Type	Specification	Proposed GA scheme RR	Previous averaging scheme [18] RR	Chang and Lin's method [1] RR				
					t = 160	t = 180	t = 200	t = 230	t = 250
					Blurring	Gaussian filter	9 × 9	98.22%	97.73%
Surround cropping		26%	97.14%	86.72%	88.75%	88.65%	88.40%	88.26%	88.40%
Quarter cropping		25%	96.95%	85.89%	87.45%	88.70%	89.67%	90.77%	91.92%
Noise addition	Gaussian noise	Mean = 0 Variance = 0.01	95.36%	73.41%	87.84%	89.45%	90.16%	90.60%	91.09%
JPEG compression		Quality factor = 80	98.27%	97.09%	98.14%	98.00%	98.12%	98.17%	98.32%
Scaling			97.97%	97.12%	97.97%	98.07%	98.07%	98.05%	97.95%
Sharpening	Linear mapping		98.27%	97.71%	87.87%	87.50%	87.28%	88.45%	88.82%
Median filtering	Nonlinear filter	9 × 9	97.22%	90.65%	93.73%	94.53%	95.12%	95.58%	96.19%
Average filtering	Linear filter	9 × 9	97.05%	91.24%	92.72%	94.04%	94.56%	94.80%	95.41%
Gamma correction		0.7	98.00%	97.00%	94.21%	94.14%	93.80%	93.02%	93.09%
Histogram equalization		Uniform	96.48%	93.12%	71.56%	71.17%	71.00%	71.95%	73.12%
Pixel shifting		60 × 60	90.60%	51.15%	48.95%	51.37%	54.00%	58.08%	61.21%
ARR			96.79%	88.24%	87.28%	87.81%	88.19%	88.83%	89.48%

**Table 6 The comparison of average RR results among the proposed, Chang and Lin's, and previous averaging schemes for Sets 2-5 images**

Operation	Type	Specification	Proposed GA scheme RR	Previous averaging scheme [18] RR	Chang and Lin's scheme [1] RR				
					t = 160	t = 180	t = 200	t = 230	t = 250
					Blurring	Gaussian filter	9 × 9	99.68%	99.40%
Surround cropping		26%	98.52%	86.98%	88.93%	89.06%	89.14%	89.17%	89.17%
Quarter cropping		25%	98.38%	86.68%	89.84%	90.60%	91.15%	91.89%	92.26%
Noise addition	Gaussian noise	Mean = 0 Variance = 0.01	<b>95.78%</b>	77.52%	91.12%	92.18%	92.95%	93.70%	94.11%
JPEG compression		Quality factor = 80	99.89%	99.17%	99.80%	99.87%	99.89%	99.91%	99.83%
Scaling			99.86%	98.75%	99.60%	99.70%	99.74%	99.71%	99.84%
Sharpening	linear mapping		99.84%	99.66%	91.49%	91.67%	92.02%	92.80%	92.76%
Median filtering	nonlinear filter	9 × 9	98.66%	92.12%	95.83%	96.30%	96.89%	97.22%	97.50%
Average filtering	linear filter	9 × 9	98.20%	92.59%	95.44%	95.88%	96.49%	96.86%	97.15%
Gamma correction		0.7	99.35%	98.43%	95.47%	95.91%	96.15%	96.21%	96.17%
Histogram equalization		Uniform	96.98%	95.40%	78.34%	78.88%	79.69%	81.10%	81.77%
Pixel shifting		60 × 60	91.73%	50.55%	53.98%	56.03%	57.52%	60.07%	61.49%
ARR			98.07%	89.77%	89.97%	90.48%	90.80%	91.53%	91.82%

**Table 7 The comparison of RR results among the four optimization schemes for Set 1 images**

Operation	Type	Specification	GA	PSO	SCE	SIMPSA
			RR	RR	RR	RR
Blurring	Gaussian filter	9 × 9	98.22%	98.29%	98.05%	98.14%
Surround cropping		26%	97.14%	98.12%	93.70%	95.90%
Quarter cropping		25%	96.95%	98.29%	94.58%	96.09%
Noise addition	Gaussian noise	Mean = 0 Variance = 0.01	95.36%	98.19%	87.48%	93.33%
JPEG compression		Quality factor = 80	98.27%	98.32%	98.10%	98.17%
Scaling			97.97%	98.34%	97.51%	97.80%
Sharpening	Linear mapping		98.27%	98.29%	98.07%	98.19%
Median filtering	Nonlinear filter	9 × 9	97.22%	98.27%	95.39%	96.58%
Average filtering	Linear filter	9 × 9	97.05%	98.34%	94.75%	95.83%
Gamma correction		0.7	98.00%	98.32%	97.27%	97.71%
Histogram equalization		Uniform	96.48%	98.10%	94.21%	96.39%
Pixel shifting		60 × 60	90.60%	97.80%	73.14%	85.77%
ARR			96.79%	98.22%	93.52%	95.82%

**4.4. More discussions**

In digital watermarking techniques [17], there are six essential properties that must be satisfied: transparency, robustness, security, unambiguity, blindness, and multiple watermarks. The experiment results show that our scheme satisfies these six essential properties. First, our method owns the transparency because it does not modify the content of the cover image. Second, all the RR values under different attacks are greater than 88.3% for Sets 1-5 images, which represent that the retrieved watermarks are highly correlated with the original watermark. Hence, it satisfies robustness. Third, our

scheme is based on the signature procedure, so it is secure. Fourth, the retrieved watermark images are clear enough from the experiments. Therefore, it is unambiguity. Fifth, our scheme does not need the original image during the authentication procedure. Therefore, it satisfies the blind property. Finally, the owner can utilize other watermark images to generate different signature images, so it allows the use of multiple watermarks.

In the above six properties, the robustness is a more significant consideration for the use of digital watermarks in many different applications. Images are usually compressed before the transmission or storage, and

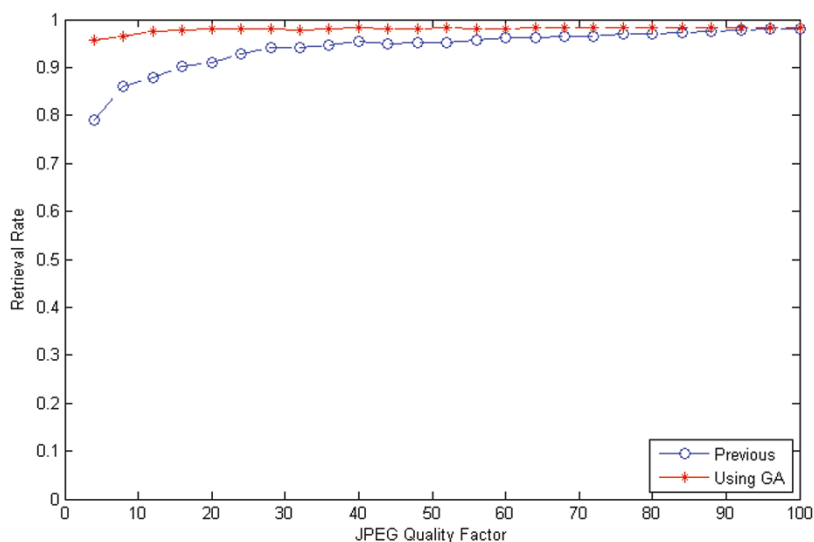
**Table 8 The comparison of the averaged RR results among the four optimization schemes for Sets 2-5 images**

Operation	Type	Specification	GA	PSO	SCE	SIMPSA
			RR	RR	RR	RR
Blurring	Gaussian filter	9 × 9	99.68%	99.98%	99.75%	99.62%
Surround cropping		26%	98.52%	99.61%	96.16%	97.76%
Quarter cropping		25%	98.38%	99.62%	96.30%	98.04%
Noise addition	Gaussian noise	Mean = 0 Variance = 0.01	95.78%	99.52%	92.54%	95.56%
JPEG compression		Quality factor = 80	99.89%	99.99%	99.83%	99.69%
Scaling			99.86%	99.99%	99.54%	99.51%
Sharpening	Linear mapping		99.84%	99.99%	99.65%	99.66%
Median filtering	Nonlinear filter	9 × 9	98.66%	99.68%	96.87%	98.20%
Average filtering	Linear filter	9 × 9	98.20%	99.66%	96.55%	98.16%
Gamma correction		0.7	99.35%	99.92%	98.60%	98.95%
Histogram equalization		Uniform	96.98%	99.52%	95.35%	97.30%
Pixel shifting		60 × 60	91.73%	98.20%	83.44%	90.54%
ARR			98.07%	99.64%	96.22%	97.75%

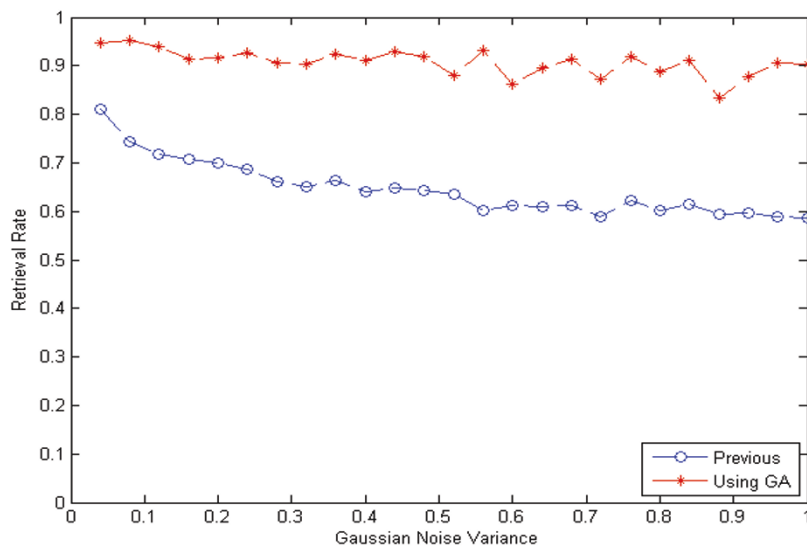
**Table 9 The computation time (in seconds) of the four optimization schemes for the five sets of images**

	SET 1	SET 2	SET 3	SET 4	SET 5
GA	10.89	9.27	13.76	12.34	8.99
PSO	51.74	53.49	53.04	53.32	55.13
SCE	74.30	71.54	72.61	72.62	70.29
SA	110.79	108.2	109.2	109.14	109.4

thus, the watermark should be robust to compression schemes. Since JPEG is one of the most efficient compression techniques, the performances of our scheme under different quality factors in JPEG compression are examined. On the other hand, images are usually transmitted on the Internet and might be interfered by Gaussian noise. The robustness to additive Gaussian noise should also be investigated. Hence, the performances of



(a)



(b)

**Figure 7** The RR comparison results of the previous averaging and the proposed GA-based methods under the effects on. (a) JPEG compression and (b) additive Gaussian noise.

our scheme under different variance values for Gaussian noise attacks are studied as well.

The cover image "Hill" in Set 1 was compressed by JPEG with different quality factors. Figure 7a shows the RRs between the embedded and extracted watermarks under different quality factors using the GA and our previous averaging schemes. As shown in this figure, the watermark RRs are greater than 0.9 even at a low quality factor 20. By decreasing the image quality factor, the GA scheme still can extract the embedded watermark very well. For example, the RR is 95.65% even when the quality factor is as low as four.

To study the noise effects, the Hill image was interfered by the additive Gaussian noise with zero mean and different variance values. Figure 7b shows the RR results under different variance values using the GA scheme and our previous averaging scheme. All the RRs are greater than 82.55% when using the GA scheme. Compared with our previous averaging scheme, the RR performance is significantly improved under different variance values.

## 5. Conclusions

A new scheme combining the pinned field of the protected image with optimization schemes for ownership verification has been proposed in this article. The pinned field partially reflects the texture information of the images and be employed to enhance the robustness of watermark. The optimization algorithm is then applied to optimize the similarity between the pinned field and the protected image. The signature and authentication procedures have been described. The experimental results demonstrate that the proposed scheme can resist and survive under different signal processing and geometric transformation attacks, such as blurring, cropping, noising, and JPEG lossy compression, etc. Compared with another copyright protection scheme and our previous averaging scheme, the GA scheme achieves better RR performance in average. Furthermore, the other optimization schemes are also employed to determine the threshold values in the binarization of the feature image. Consider both the computation complexity and the system performance. The overall comparison results show that the GA scheme is superior to other schemes. Finally, the proposed method also shows good performances for JPEG compression and Gaussian noise attacks.

## Abbreviations

ARR: average retrieval rate; DCT: discrete cosine transform; DFT: discrete Fourier transform; DWT: discrete wavelet transform; GA: genetic algorithm; PSNR: peak signal-to-noise ratio; PSO: particle swarm optimization; RR: retrieval rate; SA: simulated annealing; XOR: exclusive-or.

## 6. Acknowledgements

This study was partially supported by the National Science Council, Taiwan under the contract number NSC 99-2221-E-224-004. The authors also like to especially thank Mr. Yu-Sian Lin for his programming and collection of simulation data.

## Author details

<sup>1</sup>Department of Electronic Engineering, Kao Yuan University, Kaohsiung, Taiwan, ROC <sup>2</sup>Department of Electrical Engineering, National Yunlin University of Science and Technology, Yunlin, Taiwan, ROC

## Competing interests

The authors declare that they have no competing interests.

Received: 2 December 2010 Accepted: 23 August 2011

Published: 23 August 2011

## References

1. CC Chang, PY Lin, Adaptive watermark mechanism for rightful ownership protection. *J Syst Softw.* **81**(7), 1118–1129 (2008). doi:10.1016/j.jss.2007.07.036
2. CI Podilchuk, EJ Delp, Digital watermarking, algorithms and application. *IEEE Signal Process Mag.* **18**(4), 33–46 (2001). doi:10.1109/79.939835
3. PW Wong, N Memon, Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Trans Image Process.* **10**(10), 1593–1601 (2001). doi:10.1109/83.951543
4. M-T Lee, HT Chang, Adaptive image watermarking using phase-shifting digital holography embedded in the wavelet domain. *Int J Inf Assur Secur.* **5**(1), 603–610 (2010)
5. I Pitas, TH Kaskalis, Applying signatures on digital images, in *Proceedings of IEEE Nonlinear Signal Image Processing*, 460 (June 1995)
6. O Bruyndonckx, JJ Quisquater, B Macq, Spatial method for copyright labeling of digital images, in *Proceedings of IEEE Nonlinear Signal and Image Processing*, 456 (June 1995)
7. DC Wu, WH Tsai, A steganographic method for images by pixel-value differencing. *Pattern Recognit Lett.* **24**(9-10), 1613–1626 (2003). doi:10.1016/S0167-8655(02)00402-6
8. YH Yu, CC Chang, YC Hu, Hiding secret data in images via predictive coding. *Pattern Recognit.* **38**(5), 691–705 (2005)
9. MU Celik, G Sharma, AM Tekalp, E Saber, Lossless generalised-LSB data embedding. *IEEE Trans Image Process.* **14**(2), 253–266 (2005)
10. E Koch, J Zhao, Toward robust and hidden image copyright labeling, in *Proceedings of IEEE Nonlinear Signal and Image Processing*, 452 (June 1995)
11. IJ Cox, J Kilian, T Leighton, T Shammoon, Secure spread spectrum watermarking for multimedia. Tech Rep 95-10 NEC Res Inst. (Princeton, NJ, 1995)
12. HT Chang, C-C Hsu, C-H Yeh, DF Shen, Image authentication and tampering localization based on watermarking embedding in wavelet domain. *Opt Eng.* **48**(5), 057002 (2009). doi:10.1117/1.3127192
13. HT Chang, CL Tsan, Image watermarking by use of digital holography embedded in DCT domain. *Appl Opt.* **44**(29), 6211–6219 (2005). doi:10.1364/AO.44.006211
14. WB Lee, TH Chen, A publicly verifiable copy protection technique for still images. *J Syst Softw.* **62**(3), 195–204 (2002). doi:10.1016/S0164-1212(01)00142-X
15. CC Chang, KF Hwang, MS Hwang, Robust authentication scheme for protecting copyrights of images and graphics. *IEE Proc Vis Image Signal Process.* **149**(1), 43–50 (2002). doi:10.1049/ip-vis:20020372
16. CC Chang, JC Chuang, An images intellectual property protection scheme for gray-level images using visual secret sharing strategy. *Pattern Recognit Lett.* **23**(8), 931–941 (2002). doi:10.1016/S0167-8655(02)00023-5
17. TH Chen, G Horng, WB Lee, A publicly verifiable copyright-proving scheme resistant to malicious attacks. *IEEE Trans Indus Electron.* **52**(1), 327–334 (2005). doi:10.1109/TIE.2004.841083
18. MT Lee, HT Chang, Copyright protection scheme for still images based on an image pinned field. *Opt Eng.* **49**(9), 097005 (2010). doi:10.1117/1.3488044
19. AZ Meiri, E Yudilevich, A pinned sine transform image coder. *IEEE Trans Commun.* **29**(12), 1728–1735 (1981). doi:10.1109/TCOM.1981.1094935
20. AZ Meiri, The pinned Karhunen-Loeve transform of a two dimensional Gauss-Markov field. *Proc SPIE.* **87**, 155 (1976)

21. ATS Ho, X Zhu, YL Guan, Image content authentication using pinned sine transform. *EURASIP J Appl Signal Process*. **14**, 2174–2184 (2004)
22. X Zhu, ATS Ho, P Marziliano, A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. *Signal Process Image Commun*. **22**(5), 515–528 (2007). doi:10.1016/j.image.2007.03.004
23. V Aslantas, A singular-value decomposition-based image watermarking using genetic algorithm. *Int J Electron Commun (AEU)*. **62**(5), 386–394 (2008). doi:10.1016/j.aeue.2007.02.010
24. D Bertsimas, J Tsitsiklis, Simulated annealing. *Stat Sci*. **8**(1), 10–15 (1993). doi:10.1214/ss/1177011077
25. J Kennedy, RC Eberhart, Particle swarm optimization, in *Proceedings of IEEE International Conference on Neural Networks* (Prentice Hall, Piscataway, NJ, 1995), p. 1942
26. QY Duan, KV Gupta, S Sorooshian, Shuffled complex evolution approach for effective and efficient global minimization. *J Opt Theor Appl*. **76**(3), 501–521 (1993). doi:10.1007/BF00939380
27. Optimization algorithms, <http://biomath.ugent.be/~brecht/downloads.html> (July 7 2011)
28. N Kazakova, M Margala, NG Durdle, Sobel edge detection processor for a real-time volume rendering system, in *Proceedings of the 2004 International Symposium on Circuits and Systems*. **2**, II–913 (2004)
29. YD Qu, CS Cui, SB Chen, JQ Li, A fast subpixel edge detection method using Sobel-Zernike moments operator. *Image Vision Comput*. **23**(1), 11–17 (2005). doi:10.1016/j.imavis.2004.07.003
30. MF Cardoso, RL Salcedo, SF de Azevedo, The simplex-simulated annealing approach to continuous non-linear optimization. *Comput Chem Eng*. **20**, 1065–1080 (1996). doi:10.1016/0098-1354(95)00221-9

doi:10.1186/1687-6180-2011-44

**Cite this article as:** Lee and Chang: On the pinned field image binarization for signature generation in image ownership verification method. *EURASIP Journal on Advances in Signal Processing* 2011 **2011**:44.

**Submit your manuscript to a SpringerOpen<sup>®</sup> journal and benefit from:**

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

---

Submit your next manuscript at ► [springeropen.com](http://springeropen.com)

---