An Image Watermark Insertion and Extraction Method Based on EDA-PSO

Yanxia Jin¹,∗, Rong Zhu², Xin Qi³, Jinrui Zhang³, Qifu Cheng³, Bo Ma³ and Yao Jia³
¹School of Data Science and Technology, North University of China, Taiyuan, 030051, China
²The ShanXi Science and Technology Department, Taiyuan, 030001, China
³School of Computer Science and Technology, North University of China, Taiyuan, 030051, China
∗Corresponding author

Abstract—An innovative image watermark insertion and extraction method based on EDA-PSO is proposed to improve both the imperceptibility and robustness of the image watermark. The insertion and extraction of the watermark is performed in the discrete cosine transform domain (DCT). In the process, Watson perceptual model is first applied to find the optimal embedding position, then EDA-PSO is employed to adjust the strength of the embedded watermark and finally a new fitness value is defined as the evaluation criteria based on imperceptibility and robustness. This method embeds the watermark information of varying strengths into the low and middle frequency coefficients with the maximum visual perception threshold of each DCT block according to the different results of EDA-PSO. The simulation results proves that the proposed scheme ensures the imperceptibility of the watermark and achieves high robustness against such attacks as JPEG compaction, GLPF, addition Gaussian noise, addition impulse noise and addition product noise.

Keywords—image watermarking; high-quality particle distribution; Watson visual mode; robustness; imperceptibility

I. INTRODUCTION

With the rapid development and wide application of information technology in all fields of human society, information security becomes a common concern of the digital times. Digital watermarking technology is an information hiding technique. Its basic principle is to embed secret messages into the audio, video and image products to protect their copyright, prove their authenticity, track piracy or provide extra information [1]. Security, imperceptibility and robustness are the three inseparable characteristics of a good image watermark. The inherent structures of the watermark and improper embedding strategies cause a conflict between the imperceptibility and robustness of the watermark. How to solve this problem has become a research hotspots.

Many researchers have introduced genetic algorithm, ant-colony algorithm, particle swarm algorithm and intelligent optimization algorithms into the image watermarking technology and have proved to be quite effective. Liang Weiyi and others[2] proposed the application of genetic algorithm together with Watson perceptual modal to define a new fitness value to adjust the strength of embedded watermark in the DCT transform domain. Ansari, Irshad Ahmad and others [3] proposed the application of artificial bee colony algorithm together with the embedding strength of watermarking in order to get an optimal tradeoff between invisibility and robustness. Guo Yong and others[4] proposed a novel image watermarking method based on firefly algorithm in discrete wavelet transform (DWT)-QR transform domain. The experiment results show that the proposed image watermarking method has better or comparable robustness as compared with some related methods. LIU JING and others[5] proposed a digital watermark algorithm based on wavelet transform, which takes advantage of the distinct texture information to fine the optimal embedding position. Jero, Edward S and others [6] proposed a Continuous Ant Colony Optimization (CACO) based ECG Stenographic scheme using Discrete Wavelet Transform and Singular Value Decomposition. The scaling factor in the quantization techniques governs the tradeoff between imperceptibility and robustness. ZENG QING and others[7] proposed to combine the cuckoo search and wavelet transform to achieve fast and precise determination of the optimal embedding position and coefficients. Singh, Amit Kumar[8] proposed a new robust hybrid multiple watermarking technique using fusion of discrete watermark transforms (DWT), discrete cosine transforms (DCT), and singular value decomposition (SVD) instead of applying DWT, DCT and SVD individually or combination of DWT-SVD / DCT-SVD. The method has been extensively tested and analyzed against known attacks and is found to be giving superior performance for robustness, capacity and reduced storage and bandwidth requirements compared to reported techniques suggested by other authors. Wang Xiangyang and others[9] proposed a blind robust image watermarking approach in the nonsubsampled shearlet domain using Bessel K Form (BKF) modeling. Experimental results on test images demonstrate that the proposed approach can provide better imperceptibility and robustness. Zhu Xin-Shan and others[10] proposed an optimal watermark embedding method combining spread spectrum and quantization. Simulations on real images by using the wavelet-based implementations demonstrate the proposed method performs very well in both watermark imperceptibility and robustness .Jero, Edward S. and others[11] proposed that ECG Steganography ensures protection of patient data when ECG signals embedded with patient data are transmitted over the internet. The scaling factor in the quantization techniques governs the tradeoff between imperceptibility and robustness.
Although all the methods proposed in the above literatures succeed in finding the optimal embedding position, they fail to take the conflicting characteristics of imperceptibility and robustness of the watermark into consideration. And that is exactly the problem the author tries to solve in this paper—propose a new scheme to ensure both the imperceptibility and robustness of the watermark. The detailed procedure is: Watson perceptual modal is first employed to determine the position with the maximum visual perception threshold in the low and middle frequency of the DCT transform domain to select the optimal embedding position of the watermark; then, EDA-PSO is applied to optimize the strength of the self-adaptive embedded watermark in a effective and steady way; finally, a new fitness function is defined for comprehensive evaluation out of the need to ensure both the image quality and robustness of the watermark to achieve the best balance of the two features.

II. EDA-PSO

EDA-PSO is a new evolutionary particle swarm optimization algorithm [12]. PSO is a random search algorithm developed by simulating the bird swarm’s foraging behavior, in which birds learn from each other and cooperate with each other. It outperforms other optimization algorithms with its rapid convergence, easy operation and less parameters. The shortcomings of PSO also exposed with its wide application in many fields, such as premature reach of local least value, poor global searching ability, premature convergence and bad diversity. Unlike PSO, EDA-PSO uses statistical learning methods to build a particle distribution probability modal in the solution space and then update the location and velocity of next-generation particle based on the high-quality particle and its historical and global optimal value in the model. In this way, EDA-PSO not only retains the simplicity of PSO, it also effectively balances the local and global searching ability of the algorithm by reducing the convergence speed. The basic principle of EDA-PSO is to select several particles with better solutions in each dimension and each iteration to build a probability model using statistical learning method and this model reveals the distribution of the optimal solutions with the highest potential and helps to generate the optimal particles of the present generation.

EDA-PSO updates the particle position based on the following formulas (1) and (2).

\[
\begin{align*}
\psi(t+1) &= \alpha \psi(t) + \beta \phi(\psi(t) - \chi(t)) + \epsilon r_1(t)
\end{align*}
\]

\[
\begin{align*}
x_j(t+1) &= x_j(t) + v_j(t+1)
\end{align*}
\]

In formula (1) and (2), "i" stands for particle, "j" is dimension of particle, t is generation t , c1, c2, c3 are acceleration constants, whose values are commonly between 0 and 2, c1 is weight coefficient of self-learning by the particle, c2 is that of group experience , c3 is that of high-quality particle, particle r1j, r2j, r3j are mutually independent and are random numbers between 0 and 1, q(t) is the high-quality particle generated in each dimension. To prevent the particle from leaving the searching space too fast in the evolution process, vij, xij are generally limited to certain range, namely, vij, xij ∈ [-xmax, xmax].

Figure 1 reveals the features of the new algorithm by comparing the procedures of the two algorithms. In EDA-PSO, the probability model built according to better solution information provides the particle opportunities to learn not only from local and global optimal value, but also from it high-quality counterpart in each iteration, which greatly improves the particle’s comprehensive learning ability and enables it to hop out of the local optimal value and avoid premature convergence.

III. IMAGE WATERMARK INSERTION AND EXTRACTION METHOD BASED ON EDA-PSO

Compared with its counterpart in spatial domain, the image watermark in DCT domain is more robust and compatible with JPEC, making it an ideal object of study for this paper. The key step of the proposed scheme is to overlap the watermark information into the DCT domain of the host image. The host image is first divided into certain pixel blocks of size 8*8, which are subsequently subjected to DCT transform one by one to obtain 64 DCT coefficients. Since the human perceptual system mainly works in the low and middle frequency bands. The attacks to these bands will inevitably lead to the deterioration of the image quality. Due to this, the low and middle frequencies are chosen to embed into the watermark. To increase the robustness of the embedded watermark, the location with the greatest perceptual threshold in these frequencies are selected to according to Watson model.

A. Watson Model

Watson model is a classical perceptual model based on 8*8 block discrete cosine transform, achieving a good balance between sensitivity, luminance masking, and contrast masking [13]. Table 1 is defined sensitive table t(i,j) based on the 8*8 Watson model block discrete cosine transform contrast. Each figure in this table denotes the minimum DCT coefficient perceived by human eyes with masking. The smaller the number, the more sensitive the human eyes to its frequency. In Watson model, luminance threshold t(i,j,k) of block k is obtained by formula (3) using the DCT component coefficient of each DCT block and Table 1.

\[
t_{i,j,k} = t(i,j)[f(0,0,k) / f(0,0)]^\gamma
\]

Where f(0,0,k) represents the DC coefficient of block k after DCT transform, f(0,0) is the mean value of DC coefficients of all such blocks, and t is a constant, whose value commonly is 0.649.

The contrast masking threshold, also called perceptual threshold (JND) is obtained by formula (4).

\[
JND_{i,j,k} = \max \left \{ t_{i,j,k}, \left \lfloor f_{i,j,k} \right \rfloor^{\alpha} \times t_{i,j,k}^{(1-\alpha)} \right \}
\]

In formula (3) and (4), the dimension k of the DCT domain is 1, 2, or 3, respectively; f(0,0,k) is the DCT coefficient, t(i,j) is the perceptual threshold of the DCT component coefficient, JND_{i,j,k} is the contrast masking threshold, and α is a constant, usually between 0.5 and 0.7, that determines the importance of contrast masking.
Where \(0 \leq i, j \leq 7\), \(f(i,j,k)\) is the corresponding coefficient of pixel\((i,j)\) of block \(k\) after DCT transform, \(w_{i,j}\) is a constant between 0 and 1. \(w_{i,j}\) of all blocks is 0.7 with an exception being 0, which corresponds to DCT.

![Flow Chart of PSO and EDA-PSO](image)

**TABLE I. WATSON MODEL CONTRAST SENSITIVE TABLE**

<table>
<thead>
<tr>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.40</td>
<td>1.01</td>
<td>1.16</td>
<td>1.66</td>
<td>2.40</td>
<td>3.43</td>
<td>4.79</td>
<td>6.56</td>
</tr>
<tr>
<td>1.01</td>
<td>1.45</td>
<td>1.32</td>
<td>1.52</td>
<td>2.00</td>
<td>2.71</td>
<td>3.67</td>
<td>4.93</td>
</tr>
<tr>
<td>1.16</td>
<td>1.32</td>
<td>2.24</td>
<td>2.59</td>
<td>2.98</td>
<td>3.64</td>
<td>4.60</td>
<td>5.88</td>
</tr>
<tr>
<td>1.66</td>
<td>1.52</td>
<td>2.59</td>
<td>3.77</td>
<td>4.55</td>
<td>5.30</td>
<td>6.28</td>
<td>7.60</td>
</tr>
<tr>
<td>2.40</td>
<td>2.00</td>
<td>2.98</td>
<td>4.55</td>
<td>6.15</td>
<td>7.46</td>
<td>8.71</td>
<td>10.17</td>
</tr>
<tr>
<td>3.43</td>
<td>2.71</td>
<td>3.64</td>
<td>5.30</td>
<td>7.46</td>
<td>9.62</td>
<td>11.58</td>
<td>13.51</td>
</tr>
<tr>
<td>4.79</td>
<td>3.67</td>
<td>4.60</td>
<td>6.28</td>
<td>8.71</td>
<td>11.5</td>
<td>14.50</td>
<td>17.39</td>
</tr>
<tr>
<td>6.56</td>
<td>4.39</td>
<td>5.88</td>
<td>7.60</td>
<td>10.17</td>
<td>13.5</td>
<td>17.29</td>
<td>21.15</td>
</tr>
</tbody>
</table>

**B. Strength of the Embedded Watermark and Objective Function**

The bigger the strength of the embedded watermark, the greater the robustness is, and the poorer the imperceptibility. Given the conflicting features of the latter two elements, EDA-PSO is employed here to calculate the best strength of embedded watermark for each DCT sub-block \(a\), value of factor of embedding intensity, is relatively smaller, generally between 0 and 1.5. The detailed calculation process is as follows:

1. **Step1**: set parameters; randomly initialize the initial velocity and position of all the particles in the swarm. Solution space is \([0, 1.5]\), size of the swarm is 30, and iterations are 50.
2. **Step2**: calculate the fitness values for all the particles; record their individual and swarm historical optimal position.
3. **Step3**: compare the fitness value of each particle; sample \(M\) better particles to construct the probability model. Central-limit theorem reveals that regardless of their general distribution, most of the distribution of statistics is roughly normal, so is the distribution of the samples in each dimension. Here, the normal distribution is represented by \(N(\mu, \sigma^2)\), with the value of obtained through maximum likelihood estimating method.
4. **Step4**: generate high quality particles according to the probability distribution of better solution.
5. **Step5**: update the position and velocity of particles of each generation by formulas (1) and (2).
6. **Step6**: return to Step 2 if iterations \(n<50\), otherwise, the procedure ends.

To test the imperceptibility of the watermarking scheme, PSNR\[^{14}\] is commonly used as an objective measure because it can reveal the difference between the carrier image and the host image. The better the host image, the greater the PSNR is. To test the scheme’s robustness, NC\[^{14}\] is employed. It can measure the similarity between the extracted watermark and the original watermark. The nearer to 1 the NC is, the better the result is. PSNR is shown in formula (5) and NC is shown in formula (6).

\[
\text{PSNR} = 10 \log_{10} \frac{N^2 \max_{x,y} |I(x,y) - I_u(x,y)|^2}{\sum_{x,y} |I(x,y) - I_u(x,y)|^2}
\]
Where \(I(x,y)\) stands for the pixel value of carrier image in position \((x,y)\), \(I_w(x,y)\) is that of the host image in the same position.

\[
NC = \frac{\sum_{x,y} w'(x,y)}{\sqrt{\sum_{x,y} w(x,y)w(x,y) \cdot \sum_{x,y} w'(x,y)w'(x,y)}}
\]

(6)

Where \(w(x,y)\) represents the pixel value of host image in position \((x,y)\), and \(w'(x,y)\) is that of the extracted image in the same position.

To achieve a better trade-off between the image watermark’s imperceptibility and robustness, the influence of the embedded watermark on the carrier image and its resistance to the common attacks should be all taken into consideration. Based on this, a new comprehensive evaluation standard, namely, fitness function is proposed.

\[
\text{fitness} = \alpha \cdot R - \beta \cdot \text{PSNR}
\]

(7)

Where \(\alpha\) is the weight of robustness evaluation standard \(R\), \(\beta\) is that of imperceptibility evaluation standard, \(\alpha+\beta=1\). They are used to measure the importance of \(R\) and PSNR. \(R\) is to reveal the distortion factor between the extracted watermark image and the original image. The real information transmission will inevitably suffer from various interferences. Taking all the intentional or unintentional attacks into consideration, this paper tries to get an average distortion value for all the attacks by seeking one such value for every one of these attacks. The formula (8) is chosen as the evaluation standard.

\[
R = \frac{1}{M} \sum_{i=1}^{M} F_i, \quad F_i = \left[ \sum_{x,y} \left[ w(x,y) - w'(x,y) \right]^2 \right]^{\frac{1}{2}}
\]

(8)

In formula (8), where \(i=1,2,\ldots,M\), \(w(x,y)\) denotes the pixel value of the original watermark image in position \((x,y)\), \(w'(x,y)\) is that of the extracted image exposed to attack \(i\) in the same position. \(R\) shows the distortion factor between the extracted and original watermark after \(m\) attacks. \(M\) is the number of attacks the embedded image suffered. \(R\) is a real number equal to or great than 0. The smaller its value is, the higher the robustness. When \(R=0\), the extracted watermark has no distortion.

Given the conflicting nature of the image quality and its robustness, subtraction is applied between \(R\) and PSNR to obtain the fitness formula. The value of fitness should be as smaller as possible.

C. Insertion and Extraction Method of Image Watermark

Assume the watermark image is a binary image of size \(64^*64\), and the size of the carrier image is \(512^*512\). The detailed embedding process is as follows:

Step1 (watermark scrambling): the scrambling principle is to dispute the pixel order of the watermark information without changing the total number of the pixel. The resulted disorder image makes it difficult for illegal users to recover it without knowing the employed scrambling type and needed parameters, thereby ensuring the safety of the image. This experiment chooses Arnold transform [15] to change the image of size \(M^*M\) according to the formula (9). In formula (9), where \((x,y) \in [0,1,\ldots,M-1] \). Arnold transform shows certain periodicity, which means the original image, can be recovered after certain times of iteration. The formula (9) is used to scramble and encrypt the pixel coordinates of binary watermark image one by one to generate the scrambled watermark image \(w'(p,q)\) and save scrambling time Key as the decoding key.

\[
\begin{bmatrix}
  x' \\
  y'
\end{bmatrix} = \begin{bmatrix}
  1 & 1 \\
  1 & 2
\end{bmatrix} \begin{bmatrix}
  x \\
  y
\end{bmatrix} \mod N
\]

(9)

Step2 (DCT transform): divide the 515*512 carrier image into non-overlapping 8*8 sub-blocks \((64^*64)\) in total, and subject all the sub-blocks \(B_k=1, 2, \ldots, 64^*64-1\) to DCT transform, with each sub-block obtaining 64 DCT coefficients.

Step3 (watermarking embedding): calculating the greatest perceptual threshold value for each sub-block by Watson model and record its position \(B_k\) (row, column); obtaining embedding formulas (10) and (11) by the principle of embedding one sub-block \(w\) to one DCT block and the general embedding method.

\[
F (p,q) = \begin{cases}
-1, w'(p,q) = 0 \\
1, w'(p,q) = 1
\end{cases}
\]

(10)

In formula (11), where \(I(i,j,k)\) is the pixel of the optimal embedding position in the carrier image after DCT transform; \(a\) is the watermark strength, determined by the above EDA-PSO algorithm.

Step4 (inverse DCT transform): conduct inverse DCT transform on the embedded carrier image based on its 8*8 sub-blocks, obtaining the embedded watermark image \(I_w(i,j)\).

The extraction process is rightly opposite to that of insertion, as shown in the following:

Step1 (blocking and DCT transform): conduct DCT transform on embedded watermark image \(I_w(i,j)\) and carrier image \(I(i,j)\) based on their respective 8*8 sub-blocks.

Step2 (watermark extraction): subtract 1 from the specific value of each block of carrier image and embedded watermark image after DCT transform.

Step3 (inverse scrambling): inversely scrambling the extracted binary watermark matrix using the Arnold transform periodicity and Key \(K\), obtaining watermark image \(w''(u,v)\).
IV. SIMULATION EXPERIMENT

This paper uses 515*512 “Lena” as the carrier image, shown in Figure 2 (a) and the 64*64 binary image marked as “中北大学” as the watermark image, shown in Figure 2 (b) to implement simulation experiment on the proposed scheme. Figure 2 (c) is the resulted watermark image after 20 times of Arnold transform, which is embedded into the carrier image to generate the watermarked image, shown in Figure 2(d). The extracted watermark image after decoded by secret key is shown in Figure 2(e). Comparison of the images in Figure 2 discloses that insertion of the watermark has no big impact on the quality of the original image and the extracted watermark from the watermarked image shows no visual difference with the original watermark image.

![Carrier images](a) Carrier images

![Watermark image](b) Watermark image

![After scrambling watermark](c) After scrambling watermark

![After embedding the watermark image](d) After embedding the watermark image

![Extraction of the watermark](e) Extraction of the watermark

FIGURE II. CARRIER AND THE WATERMARK IMAGE RENDERING

To make the proposed scheme more convincing, the 512*512 grayscale image baboons, Lena and Barbara are taken as the original carrier image. As shown in Figure 2, tests such as JPEG compaction, GLPF, addition Gaussian noise, addition impulse noise and addition product noise are implemented on the watermarked images. Comparison is conducted between the performance of the watermarking method based on genetic algorithm mentioned in Literature 2 and of the proposed method in this paper. The experimental results are demonstrated in Figure 2.

![Baboon](a) Baboon

![Lena](b) Lena

![Barbara](c) Barbara

FIGURE III. IMAGE WATERMARK STANDARD TEST PATTERN

<table>
<thead>
<tr>
<th>Table II. COMPARISON OF EXPERIMENT RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Carrier image</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>NC0</td>
</tr>
<tr>
<td>NC1</td>
</tr>
<tr>
<td>NC2</td>
</tr>
<tr>
<td>NC3</td>
</tr>
<tr>
<td>NC4</td>
</tr>
<tr>
<td>NC5</td>
</tr>
<tr>
<td>R</td>
</tr>
</tbody>
</table>

Table 2 is the text of the genetic algorithm (GA) in the literature [2], PDPSO [16] and fusion of high quality particle distribution search algorithm (EDA-PSO) experimental results of different test image as the carrier image. NC0 denotes the normalized correlation coefficients of the extracted and original watermark without being subjected to any attack and processing. NC1 to NC5 respectively represents the normalized
correlation coefficients of the above two watermarks when subjected to JPEG compaction, GLPF, addition Gaussian noise, addition impulse noise and addition product noise attack. From Figure 2, it can be found that the normalized coefficients of the extracted and original images generated by the three algorithms are both 1 when there is no any attack occurred. And even under the five different attacks, their robustness indexes are all above 0.85. The robustness index of EDA-PSO is relatively higher than that of GA and PDPSO. The PSNR of the former algorithm are higher than the latter, proving that EDA-PSO generates a better imperceptibility and transparency. The fitness comparison of the three algorithms reveals a greater balance between the imperceptibility and robustness is reached by EDA-PSO.

V. CONCLUSION

The proposed scheme of this paper applies Watson perceptual model and EDA-PSO algorithm to find the optimal position and optimal embedding strength of watermark embedding in the discrete cosine transform domain and proposes a new evaluation standard taking both imperceptibility and robustness into consideration, achieving a better balance between the above two elements of the image watermark. Detailed experimental results prove that the proposed scheme can effectively combats the common attacks and processing by ensuring both the watermark’s imperceptibility and its robustness.

The proposed scheme has a heavy dependence on the original watermark in its extraction process, which is the shortcoming of the scheme and also the problem needed to be solve in the future.

ACKNOWLEDGMENT

This work was financially supported by the Nature Science Foundation of Shanxi Province (Grant: 2018011D121154, 2018011D121155).

REFERENCES