GA Based Digital Image Watermarking for Enhanced Robustness and Imperceptibility

R. Surya Prakasa Rao¹, Dr. P. Rajesh Kumar²
Dept., of ECE, AU College of Engineering, Visakhapatnam, India.
Dept., of ECE, AU College of Engineering, Visakhapatnam, India.

Abstract: The goal of image watermarking is to hide the specific information into host image and the presence of the watermark cannot be realized by human visual. The watermarking algorithm design should meet the criteria such as the rightful ownership protection, robustness against the image processing attacks and watermark imperceptibility. In this paper an optimal watermarking scheme based on singular value decomposition (SVD) and Discrete wavelet transform (DWT) using multi-objective genetic algorithm (GA) optimization is presented. The singular values of the watermark are embedded in a detail sub-band of host image after third level approximation. The GA algorithm is used to achieve the highest possible robustness and transparency. Experimental results gives improved performance in term of transparency and robustness after attacks by the proposed method compared to other existing methods.

Keywords: Digital Image watermarking, DWT, SVD, GA, Robust, Imperceptibility

I. Introduction

In the watermarking algorithm procedure, only the real owner can extract watermark correctly from a watermarked image. The watermarking proposed (1) and improved by the researchers in the SVD domain[7–22] in that the watermark is embedded into the singular value of the host image. In [7–15, 17, 19], the host image is transformed first (mostly using the wavelet transform) before performing the SVD. In SVD watermarking techniques [7–15,17, 19], the visual watermark is embedded into the singular value matrix of the host image in the transformed domain by selecting the suitable scaling factor to achieve the imperceptibility aspect in the watermarked image. The two approaches are used to embed the watermark information into a host image such as directly insert a watermark image into host image singular value matrix [1,15–22],and only inject the watermark singular value into the singular value [7–14] of host image. Both types of these methods gives a good quality watermarked image in terms of the PSNR, and robust against various attacks in terms of the correlation coefficient [1,7–22]. Still, the image quality is degraded and the transparency of the watermark is improved by a lower value of scaling factor but it is less robust against various geometric attacks. The tradeoff between these two has been addressed to get the suitable scaling factor determination as an optimization problem [16,18,20]. The genetic algorithm [16],the tiny genetic algorithm [18] and differential evolution algorithm [20] is used to get the optimum scaling factor to achieve the robustness and to improve the image quality of watermarked image. However, a major flaw is found in the SVD watermarking as reported in [2–6]. GA to optimize the watermark strength as used by Vahedi et al.[24].Basically RGB, YCbCr, YIQ, HIS, HSV and other color space models which are used by the researchers for the host image in their digital watermarking methods. The above mentioned color models are compared i.e. change in one component may affect the other components of image and image components are not independent. The compared color host image to use only one color component at a time for embedding the watermark data which forces the constraints used by the researchers. however, there exist some un compared color models such UCS, etc.[25],[26],which may be used in color image watermarking to increase the durability and resolution by using all the color image components of host images, Saraswat and Arya [26] used UCS for color transfer of images and detected that UCS outperforms the other un corresponded color spaces. In the proposed scheme is combining DWT and SVD with genetic algorithm to find the optimal scaling factor and embed the singular value of watermark in singular value of 3rd-level DWT approximation matrix of original image.

The proposed image watermarking based on Genetic algorithm is presented in the remaining part as follows: section II describes the details of related work. The complete detail of proposed watermarking scheme is illustrated in section III. Section IV reveals the details of simulation obtained after the implementation of proposed approach. Finally the conclusions are described in section V.
II. Related Work

A. Discrete Wavelet Transform

Discrete Wavelet Transformation is a wavelet filter used to transform the image. The Haar and Daubchies are commonly used filters. By using these filters single level decomposition gives four frequency components named as HH1, HL1, LH1, and LL1. In second level decomposition, apply transform to LL1 and so on to get the desired one. The model of three-level decomposition of image [21] as shown in fig.1.

Discrete Wavelet Transformation is very suitable to identify the areas in the cover image where a secret image can be embedded effectively. This property allows the exploitation of the masking effect of the human visual system such that if a DWT co-efficient is modified, it modifies only the region corresponding to that coefficient. The embedding watermark in the lower frequency sub-bands may degrade the image as generally most of the Image energy is stored in these sub-bands. However it is more robust. The high frequency part contains information about the edge of the image so this frequency sub-bands are usually used for watermarking since the human eye is less sensitive to changes in edges. The DWT splits the signal into high and low frequency parts. The low frequency part contains coarse information of signal while high frequency part contains information about the edge components. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges.

B. Singular Value Decomposition

SVD is a mathematical tool to analyze matrices. In SVD real matrix Ig decomposed in to three matrices Ig =XlSYgT Where Xl and Yg are orthogonal matrices in which columns of Xl are left singular vectors and columns of Yg are right singular vectors of image Ig. D is a diagonal matrix of singular values in decreasing order. The Singular values of grey scale original image are modified to embed the watermark image by applying multiple scaling factors, after that using GA modifications are made to get highest possible transparency and Robustness under certain attacks [10]. It is a tool in linear algebra, which is widely applied in many research fields such as principal component analysis, canonical correlation analysis and data compression. The component S is a singular value matrix in SVD domain, and is a diagonal matrix with non-negative real numbers,

\[
S_{MN} = \begin{bmatrix}
S(1,1) & 0 & \ldots & 0 \\
0 & \ddots & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & S(M,N)
\end{bmatrix}
\] (1)

Where \( S(1,1) \geq S(2,2) \geq S(3,3) \ldots \geq S(M,N) \geq 0 \).

C. Genetic Algorithm

Genetic algorithm [22] is one of the mostly used optimization technique belonging to area of evolutionary computation. GA is mainly composed of three operations: selection, genetic operation and replacement. Initially, a population is randomly generated. The fitness function then uses objective values from objective function to evaluate the fitness of each chromosome. The fitter chromosome has the greater chance to survive during the evolution process.
The objective function is the problem specific; its objective value can represent the system performance index (e.g., an error). Next, a particular group of chromosome is chosen from the population to be parents. The offspring is then generated from these parents by using genetic operation, which normally are crossover and mutation, similar to their parents, the fitness of the offspring is evaluated and used in replacement process in order to replace the chromosomes in the current population by the selected offspring. The GA cycle is the repeated until a desired termination criterion is satisfied, for example, if the maximum number of generations is reached or the objective value is bellowed the threshold.

III. Proposed Approach

In this proposal, The GA is used to obtain optimum scaling factors to meet up high Robustness under certain attacks. The Block Diagram of proposed approach as shown in Fig.3 and The steps needed for Embedding and Extraction is as follows:

A. Embedding Procedure
(i) Initialize the parameters of Genetic Algorithm: Select value for scaling factor SF from 0 to 1 and set the population size and the number of iterations.
(ii) Generate the 1st generation of individuals randomly. Perform the watermarking embedding procedure, for each iteration different watermarked image is produced.
(iii) Decompose the image $I_c$ into four sub bands using three levels Haar DWT.
(iv) Apply SVD to $LL_3$ sub band and also for remaining bands, as $I_{Gl} = X_{3i}D_{3i}Y_{3i}^T$, where $i = LL, LH, HL, HH$.
(v) Decompose the watermark image $I_w$ into four sub bands using one level Haar DWT.
(vi) Apply SVD to $LL$ sub band and also for remaining bands as $I_{wi} = X_{wi}D_{wi}Y_{wi}^T$, Where $i = LL, LH, HL, HH$.
(vii) Modify the singular value of $I_{GL}$ by embedding singular value of $W_G$ in $LL$ sub band and for remaining such that $D_{3mi} = D_{3i} + S_i * D_{wi}$, where $i = LL, LH, HL, HH$.

Where $D_{3mi}$ is the modified singular values and $S$ is the scaling factors.
(viii) Apply inverse SVD on the altered singular values of all bands. The new bands are denoted as $I_{GWL_3}, I_{GWL_2}, I_{GWH}$.
(ix) To obtain the watermarked image ($I_w$) applying three level inverse DWT using modified coefficients $I_GW$.
(x) Apply different attacks on the watermarked image.

B. Extraction Procedure
It is applied to extract the watermark from each attacked watermarked image.
(i) Apply three level Haar DWT to decompose the watermarked image into four sub bands.
(ii) Apply SVD to $LL_{3w}$ sub band and also for remaining bands, as $I_{Gwi} = X_{3wi}D_{3wi}Y_{3wi}^T$, Where $i = LL, LH, HL, HH$.
(iii) Compute $D_{3wei} = (D_{3wi} - D_{3i})/S_i$, where $i = LL, LH, HL, HH$. Here the $D_{3wei}$ is the singular matrix of the respective $i_{th}$ band of extracted watermark.
(iv) Distorted bands will be obtained by performing SVD on the obtained singular values of all bands as $I_{GWLL}^*$, $I_{GWLL}^*$, $I_{GWHL}^*$, $I_{GWWH}^*$.

(v) Then the final watermark can be extracted by applying inverse DWT on the obtained distorted wavelet bands as $I_W^*$.

(vi) Compute the robustness and imperceptibility [22] using equations (2) and (3) as

$$NC = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{w(i,j)w^*(i,j)}{(w(i,j))^2 + (w^*(i,j))^2}$$

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right)$$

Where

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I^*(i,j))^2$$

Where

$I$ = original image
$I^*$ = watermarked image

(vii) The Fitness Function (FF) is evaluated as FF = PSNR + 100·NC.

(viii) Select the best fitness values based on the Robustness and Imperceptibility.

(ix) Generate the new population performing the crossover and mutation on the selected population.

(x) Repeat the steps from 2 to 9 until the result has been reached.

IV. Simulation Results

The proposed approach implemented using Matlab R2013a taking original image of size 256x256 and watermark image of size 64x64. The proposed DWT-SVD-GA based watermarking algorithm is accomplished through genetic algorithm taking population size of 10. The entire algorithm is repeated for overall population and based on the obtained results one value is determined as optimal values at which the proposed approach obtained the optimal results. The test images considered for the implementation is shown below.

![Fig.4: Test Images (a)-(e) Host Images and (f)-(g) Watermark Images, (a) Boat (b) Peppers (c) Lena (d) Cameraman (e) Mandrill (f) Binary watermark (g) Logo Watermark](image_url)

Initially the watermarked image is not subjected to any attack. The watermark is extracted directly from the watermarked image through the extraction process specified in the third section and the obtained results are shown below.

![Fig.5: Results Observed (a)-(c) Watermarked Images (f)-(j) Extracted Watermark images](image_url)
Then the extracted watermark images are processed for analysis by measuring the NC, PSNR and MSE. The mathematical representations are shown in Equations (2), (3) and (4). The obtained PSNR, MSE and NC for the above test results (Figure.6) are described in Table.1.

Table.1: Comparison between proposed and conventional approaches under no attack scenario

<table>
<thead>
<tr>
<th>Image</th>
<th>DWT-GA (Vahedi et. al) [24]</th>
<th>DWT-SVD-GA (Proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSE</td>
<td>PSNR</td>
</tr>
<tr>
<td>Lena</td>
<td>4.3531</td>
<td>41.7428</td>
</tr>
<tr>
<td>Pepper</td>
<td>7.6888</td>
<td>39.2722</td>
</tr>
<tr>
<td>Boat</td>
<td>5.9899</td>
<td>40.3356</td>
</tr>
<tr>
<td>Cameraman</td>
<td>5.3388</td>
<td>40.8564</td>
</tr>
<tr>
<td>Mandrill</td>
<td>7.6022</td>
<td>39.3124</td>
</tr>
</tbody>
</table>

Table 1 shows the comparison between the existing method proposed by Vahedi et. al [24] and the proposed method under no attack scenario. From Table 1, it can be observed that the proposed approach obtained an increased PSNR and NC values compared to the conventional approach for all test images. Figure 7 and figure 8 illustrates the details of the obtained PSNR and NC values for both conventional and proposed approaches for all test images.
Further the performance of proposed approach is analyzed through various attacks scenarios. Under this evaluation the test image is subjected to various types if attacks and then the proposed approach is applied over the attacked watermarked image to extract the watermark. Here the attacks considered are image processing attacks such as Gaussian noise attack, salt & pepper noise, Poisson noise, Wiener filtering, median filter with varying size (3*3 and 5*5), mean filtering with varying size (3*3 and 5*5) and geometric attacks such as crop with varying % of crop, histogram equalization, rotation and scaling with varying scaling factor (0.8, 1.2 and 1.5). Then the numerical metrics such as PSNR, MSE and NC are evaluated for the extracted watermark. The obtained rests of Lena image for image processing attacks and the geometric attacks are tabulated in table.2 and table.3 respectively.

<table>
<thead>
<tr>
<th>Attack</th>
<th>DWT-GA (Vahedi et.al) [24]</th>
<th>DWT-SVD-GA (Proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE</td>
<td>PSNR</td>
<td>NC</td>
</tr>
<tr>
<td>Gaussian</td>
<td>9.7897</td>
<td>38.2231</td>
</tr>
<tr>
<td>Salt &amp; pepper</td>
<td>11.6740</td>
<td>37.4586</td>
</tr>
<tr>
<td>Poisson</td>
<td>9.7800</td>
<td>38.2274</td>
</tr>
<tr>
<td>Wiener</td>
<td>5.8704</td>
<td>40.4441</td>
</tr>
<tr>
<td>Median Filter (3*3)</td>
<td>7.5798</td>
<td>39.3342</td>
</tr>
<tr>
<td>Median Filter (5*5)</td>
<td>18.6982</td>
<td>35.4128</td>
</tr>
<tr>
<td>Mean Filter (3*3)</td>
<td>20.4536</td>
<td>35.0231</td>
</tr>
<tr>
<td>Mean Filter (5*5)</td>
<td>37.9499</td>
<td>32.3387</td>
</tr>
</tbody>
</table>

Table.3: Comparative analysis between proposed and conventional approaches for Geometric attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>DWT-GA (Vahedi et.al) [24]</th>
<th>DWT-SVD-GA (Proposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE</td>
<td>PSNR</td>
<td>NC</td>
</tr>
<tr>
<td>Crop (10%)</td>
<td>19.4716</td>
<td>35.2310</td>
</tr>
<tr>
<td>Crop (20%)</td>
<td>34.2500</td>
<td>32.7842</td>
</tr>
<tr>
<td>Crop (40%)</td>
<td>86.2066</td>
<td>28.7754</td>
</tr>
<tr>
<td>HEQ</td>
<td>13.7563</td>
<td>36.7458</td>
</tr>
<tr>
<td>Scale*0.8</td>
<td>10.5519</td>
<td>37.8975</td>
</tr>
<tr>
<td>Scale*1.2</td>
<td>11.7039</td>
<td>36.4475</td>
</tr>
<tr>
<td>Scale*1.5</td>
<td>25.1229</td>
<td>34.1289</td>
</tr>
<tr>
<td>Rotation</td>
<td>14.3830</td>
<td>36.5523</td>
</tr>
</tbody>
</table>

From table.2, it can be observed that the proposed method achieves better robustness for all types of attacks mentioned in this paper. The obtained PSNR for all the cases reveals that the proposed approach obtained an enhanced image quality. Thus the proposed approach is more robust and also gives more imperceptibly Compared to the conventional approach. Figure.9 and figure.10 describes the details of PSNR and NC respectively. Figure.9 determines the obtained PSNR under both image processing and geometric attacks of conventional and proposed approaches, similarly figure.10 gives NC details.

**Fig.9:** PSNR observations for various types of attacks (a) Image processing attacks (b) Geometric Attacks
Of figures it can be observed that the geometric attacks increases the distortion in the extracted watermark image compared to image processing attacks. The very less PSNR and NC values are observed at cropping attack (40%). In that case also the PSNR and NC of proposed approach is observed to be high. Thus the proposed approach is more robust for both image processing and geometric attacks compared with conventional approaches.

V. Conclusion

In this simulation various tests are done on different cover images named as Lena, boat, Pepper and mandrill with size 256 x 256, where the enhanced PSNR and NC values are observed between original watermarked and extracted watermark after applying attacks like Gaussian noise, salt and pepper, wiener filter, Poisson noise, cropping, median filtering, mean filtering, histogram equalization, scaling and rotation compared to conventional approach. Genetic Algorithm used to find out Superior scaling factor for watermark embedding. The above results proved that Performance of proposed watermarking scheme is good in terms of Robustness and Imperceptibility for different attacks.

References


