A New Digital Image Hiding Algorithm Based on Wavelet Packet Transform and Singular Value Decomposition

Yueli Cui¹, Shiqing Zhang², Zhigang Chen³, Wei Zheng⁴
¹,²,³College of Physics & Electronic Engineering Taizhou University, Taizhou, China
⁴College of Electronic and Information Engineering, Hebei University, Baoding, China
*Corresponding author, e-mail: cuiyueli@tzc.edu.cn¹, zsq@tzc.edu.cn², czg@tzc.edu.cn³, weizheng799@yahoo.com⁴

Abstract
The paper presents a new digital image hiding algorithm based on wavelet packets transform and singular value decomposition. The low-frequency sub-band of wavelet packets transform has strong anti-jamming capacity and the singular value has very strong stability. The presented algorithm implements bit plane decomposition on the secret image and wavelet packet decomposition on the carrier image. Then, it hides the bit planes with important information into the singular value matrix of the low frequency coefficient matrix, and also hides the bit planes with secondary information into the remainder sub-band matrix with higher entropy energy. The hiding location is adaptively determined by the carrier image. The experimental results indicate that, the proposed image hiding algorithm has strong robustness and anti-attack, and it also has good invisibility and big capability.

Keywords: image hiding, singular value decomposition, wavelet packets transform, bit plane decomposition, entropy energy

1. Introduction
With the rapid development of multimedia and the increasing bandwidth of network, digital images are becoming the main media form of the present information society. However, the problems of information security such as illegal copying, modifying and pirating of digital images are increasingly common. The problem on how to give an effective method for image encryption has become a very active research field nowadays [1-2]. Some encryption algorithms have been frequently cracked in recent years. Image hiding is an important method to confuse illegal destroyer so as to play a protecting function. The main idea of image hiding is to hide a secret image into another carrier image [2]. Image hiding methods can be divided into either spatial-domain or frequency-domain. The algorithms based on spatial-domain are discussed in the references [3-4]. In these algorithms, the hidden information is always stored in the least significant bits of the pixels of the carrier image. Spatial-domain techniques are easy realized, but have poor stability. Moreover, hidden information is easily damaged for spatial-domain techniques. In contrast, frequency-domain hiding algorithms are better in terms of rigidity robust and conducive to ensuring security of secret information [5-13].

This paper proposes a new and effective image hiding algorithm. The proposed method is an integration of several techniques including bit plane decomposition, singular value decomposition and wavelet packet transform. The experimental results indicate that the proposed algorithm has strong robustness and anti-attack, and it also has good invisibility and big capability.

2. The Theoretical Basis of Proposed Algorithm
2.1. Singular Value Decomposition
Taking the image matrix A as \( M \times M \)'s non-negative matrix, rank \((A)=r\), \( r \leq M \), then resolving this to Matrix \( A \)'s singular value is as follows:

Received November 27, 2013; Revised January 24, 2014; Accepted February 18, 2014
In the above formula,

\[
U = \begin{bmatrix}
  u_1 \\
  \vdots \\
  u_m
\end{bmatrix},
V = \begin{bmatrix}
  v_1 \\
  \vdots \\
  v_m
\end{bmatrix},
S = \begin{bmatrix}
  \alpha_1 \\
  \vdots \\
  \alpha_m
\end{bmatrix}
\]

The singular value satisfies the equation:

\[
\alpha_1 \geq \alpha_2 \geq \alpha_r \geq \ldots \geq \alpha_m = 0
\]

Non-zero singular values are equal to matrix's rank. From the above we see that the SVD unit also satisfies: \( AV_i = \alpha_i \mu_i \) and \( \mu_i^T A = \alpha_i \alpha_i^T \). Generally speaking, matrix A has many minor singular values, so the matrix can use a relatively lower matrix approximation.

Supposing \( k \leq r \), the approximate matrix \( \tilde{A}_k = \sum_{i=1}^{k} \alpha_i \mu_i v_i^T \), \( E = A - \tilde{A} \) (error matrix). Matrix A's singular value is the average non-negative real number and is also unique. The singular value has relative stability towards disturbance and unchangeableness towards matrix transformation. In linear algebra, the matrix feature value shows the matrix feature, while the matrix singular value is better than its feature value in manifesting its feature. The Image matrix singular value reflects the image’s “energy feature” while its corresponding singular vector reflects the image’s “geometrical feature”. Since the image’s singular value is not very sensitive to the change of image grayness, its very slight alteration will not affect the image vision quality.

2.2. Wavelet Packet Decomposition

Wavelet packet decomposition provides more multi-resolution analysis than wavelet decomposition. It further decomposes the high frequency part. Figure 1 and Figure 2 show the process.

![Two Level Wavelet Packet Decomposition](image1)

![Diagram of Wavelet Packet Decomposition](image2)

The low frequency part contains the main energy of image. When the secret information hides into this region, it can resist kinds of attacks such as the filtering, cropping, rotating and so on, and it has good robustness. The high frequency part corresponds to the image details. The hidden image can obtain better invisibility, but has poor robustness.
3. The Proposed Algorithm Description

3.1. The Preprocessing of Secret Image
Firstly, implementation of chaos encryption is processed on the secret image, then operation of bit plane decomposition is performed on the encrypted image. The size of plane cannot become greater than coefficient matrix after two level wavelet packet decomposition of the carrier image.

3.2. The Processing of Carrier Image
By implementing wavelet packet decomposition on the carrier image, we can get image coefficient matrix $tWP$ of 16 different frequency sub-bands as shown in Figure 2. Then we take operation of singular value decomposition on the matrix $tWP$ according to the formula (1), where $t = LL2, LH2, HL2, HH2$ and we can get the following formula.

$$WP_t = U_t S_t V_t^T$$  \hspace{1cm} (4)

After calculating of the energy entropy of the 12 remaining respective coefficient matrix, then we sort them from larger to small according to the energy entropy. Finally we can get the sorted coefficient matrix $gWP$, where $g = VV2, VW2, ... FG2, GG2$, and satisfies the following requirements $1 \leq g \leq 12$ and $WP_g > WP_g + 1$. It generates a signature vector which is used to extract the secret image.

3.3. Hiding Process of the Secret Image
Step 1: Hiding the main information bit planes $B_k$ $(k = 7, 6, 5, 4)$ into the singular value matrix $S$, as follows:

$$W_t = S_t + \lambda_t B_k$$  \hspace{1cm} (5)

Firstly, by modifying the singular values, the transformation of the modified $W_t$ is taken as follows:

$$W_t = S_t + \lambda_t B_k = U_t S_t V_t^T$$  \hspace{1cm} (6)

We can use the new singular value matrix $S_t$ to reconstruct wavelet coefficient $WP_t'$ according to the formula (4).

$$WP_t' = U_t S_t V_t^T$$  \hspace{1cm} (7)

Where $t = LL2, LH2, HL2, HH2$, $WP_t'$ will be used to reconstruct the carrier image hidden the secret image.

Step 2: Hiding the secondary information bit plane $B_k$ $(k = 3, 2, 1, 0)$ into the singular value matrix $WP_g$ as follows:

$$WP_g' = WP_g + \mu_k B_k$$  \hspace{1cm} (8)

Where $g = 1, 2, 3, 4$

Step 3: Wavelet coefficients which are obtained from step 1 and step 2 is used to reconstruct the carrier image contains the secret image.
3.4. Extraction of the Secret Image

Step 1: By taking implementation of 2 level wavelet packet decomposition on the hidden image, we can get image coefficient matrix $HWP_t$, where parameter $t$ satisfy the following conditions.

$$ t = LL^2, LH^2, HL^2, HH^2, VV^2, VW^2, WW^2, NN, NM, MM, GG, GP, FG^2, GG^2 $$

Step 2: Implementation of the singular value decomposition on coefficient matrix $HWP_t$ is performed.

$$ \Lambda_t = U_t S_t V_t^T $$

$V_t$ and $U_t$ in the formula (6) is used to calculate the $W_t$ as follows:

$$ W_t = U_t S_t V_t^T $$

The following formula (11) shows bit plane matrix extracted.

$$ B_k = (W_t - S_t) / \lambda_t $$

Where $t = LL^2, LH^2, HL^2, HH^2, k = 7, 6, 5, 4$

Step 3: Using marked vector and matrix to determine coefficient matrix $HWP_k$ containing bit planes. We can get the rest matrix of the bit planes by using the formula (8). The formula (12) describes the process.

$$ B_k = (HWP_g - WP_g) / \mu_k $$

Where $k = 3, 2, 1, 0$

Step 4: All the binary bit planes is combined to recover the gray image and to extract the secret image.

4. Experimental Result

Taking 512 × 512 gray woman image as the carrier image, and 128×128 gray map image as the secret image. PSRN is used to quantitatively measure the image hidden invisible. The normalized cross-correlation coefficient (NC) is used to measure the similarity between the secret image and the original secret image. It is also used to test the robustness of the algorithm under attacking. The original value of secret image PSRN=52.173, NC=1 without attacking.

Figure 3 shows the process of the hiding and extracting algorithm. The secret image is restored with good robustness and invisible without attacking.
With implementation of various attackings on the hidden image such as cropping, filtering, rotation and so on, the extracted image after attacking is shown in Figure 4.

(a) Cropping 1/4  (b) Cropping 1/8  (c) Gaussian noise
(d) Rotation 90°  (e) Rotation -90°  (f) Rotation 180°
(g) Low-pass filter  (h) High-pass filter  (i) Median filtering

Figure 4. The Extracted Image after the Attacking

4.1. Quantitative Analysis of Robustness
In order to evaluate the robustness of the proposed algorithm, we implement various attackings on the hidden image and compared with the results of Reference [14] and Reference [15]. The experimental results are shown in Table 1 and Table 2.

<table>
<thead>
<tr>
<th>Attacking Pattern</th>
<th>Proposed</th>
<th>Ref [14]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian noise</td>
<td>0.01</td>
<td>1</td>
</tr>
<tr>
<td>Cropping 1/4</td>
<td>0.99697</td>
<td>0.3869</td>
</tr>
<tr>
<td>Median filtering 3×3</td>
<td>0.99857</td>
<td>0.9561</td>
</tr>
</tbody>
</table>

Table 2. Comparison of NC Values between the Proposed Algorithm and Reference [15]

<table>
<thead>
<tr>
<th>Attacking Pattern</th>
<th>Proposed</th>
<th>Ref [15]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian noise</td>
<td>0.01</td>
<td>1</td>
</tr>
<tr>
<td>Rotation -90</td>
<td>0.99923</td>
<td>0.943</td>
</tr>
<tr>
<td>Rotation 180</td>
<td>0.99948</td>
<td>0.947</td>
</tr>
<tr>
<td>Cropping 1/8</td>
<td>0.9992</td>
<td>0.943</td>
</tr>
<tr>
<td>Cropping 1/4</td>
<td>0.99697</td>
<td>0.3869</td>
</tr>
<tr>
<td>Cropping 1/2</td>
<td>0.96836</td>
<td>0.701</td>
</tr>
<tr>
<td>Median filtering 3×3</td>
<td>0.99857</td>
<td>0.986</td>
</tr>
<tr>
<td>Median filtering 5×5</td>
<td>0.99704</td>
<td>0.982</td>
</tr>
<tr>
<td>Median filtering 7×7</td>
<td>0.9811</td>
<td>0.965</td>
</tr>
<tr>
<td>Low-pass filtering Gauss ambiguity</td>
<td>0.99232</td>
<td>0.911</td>
</tr>
<tr>
<td>High-pass filtering Sharpening</td>
<td>0.99471</td>
<td>0.955</td>
</tr>
</tbody>
</table>

According to the results in the above tables, we can see that the proposed algorithm has better robustness under kinds of attacking.

4.2. Quantitative Analysis of Invisibility
Another important evaluating indicator to measure the image hiding effect is analysis of invisibility. From the Table 3, We can conclude that the proposed algorithm has a higher PSRN value with good invisibility.
5. Conclusion

In the paper a new digital image hiding algorithm based on wavelet packets transform and singular value decomposition was proposed. The experimental results are satisfied with good robustness and invisibility. The algorithm can effectively resist various image processing and attacking. The using of chaotic encryption algorithm improves the safety coefficient of communication and the ability of anti-attack.

Acknowledgements

This work is supported by National Natural Science Foundation of China under Grant No.61203257, Zhejiang Provincial Natural Science Foundation of China under Grant No.Y1111058, and the key project of Taizhou University under Grant No. 2011QN13. Thanks to Dr Zhigang Chen Dr Shiqing Zhang and from the members of image research team for discussions about the algorithm. Thanks also to anonymous reviewers for their comments.

References