Remote Sensing Image Zero-Watermark Algorithm Based on Bemd

Siming Xing¹,*, Zhilin Cheng¹, Chun Yu Ji¹, Jiaying Chen¹, Luyu Qi²

¹School of Mathematics and Science, TianGong University, Tianjin, 300387, China
²School of Electronic and Information Engineering, Tiangong University, Tianjin, 300387, China

*Corresponding author: simingxing@tjpu.edu.cn

Abstract. In order to solve the problem of information security when acquiring and disseminating images and improve the performance of digital watermarking, this paper proposes a remote sensing image zero-watermarking algorithm based on Bidimensional Empirical Mode Decomposition (BEMD). Initially, to perform this algorithm the DCT transform is used to extract the characteristic image of the host image. In the next step, BEMD decomposition on the grayscaled image need to be performed. The number of watermarks embedding layers is determined according to the NC value of the original image without the i-th IMF layer and the original image. The information matrix of the watermark embedding layer is XORed with the characteristic image to obtain the image embedded with the watermark. The extraction of the watermark image is the XOR result of the first XOR and the attacked image. After the watermark is embedded, the image is processed with noise, enhanced processing attacks, etc., and the NC value of the extracted watermark and embedded watermark is mostly above 0.9. The experimental results show that the watermarking algorithm proposed in this paper has better anti-attack performance, stronger invisibility and robustness.

Keywords: Digital Watermark, Bidimensional Empirical Mode Decomposition, Feature Image, Robustness.

1. Introduction and Motivation

In this information age, the dissemination and acquisition of images is simple and fast, and this phenomenon is becoming more and more frequent. In the process of image dissemination and acquisition, information security issues gradually emerged. Remote sensing images are images that record electromagnetic wave information of ground objects. Compared with ordinary images, remote sensing images have some characteristics. The band of remote sensing images is not limited to the three primary colors of red, green and blue. In addition, in order to identify the location of the captured image, most of the remote sensing images have accurate geographic coordinates. Due to the particularity of remote sensing images, remote sensing images usually contain more information than natural images. This puts forward higher requirements for protecting the security of remote sensing images.
In order to protect the copyright information of digital images, digital watermarking technology came into being. Digital watermarking technology is a technology that embeds some identification information into an image to protect the rights of copyright owners and the integrity of the image. As a kind of information hiding technology, digital watermarking technology can protect the rights and interests of copyright owners without affecting the normal use of images [1-3].

The basic characteristics of digital watermarking technology include invisibility, robustness, and security. Invisibility means that the watermark will not change the visual effect after being embedded, that is, it is not easy to be noticed by the human visual system. Robustness means that the watermark can withstand the attack imposed on the image and will not be lost due to the attack. The watermark can still be detected in the attacked image. Security means that the embedded watermark information is safe and not easily detected, tampered or forged.

Traditional digital watermarking technologies need to modify the original data to embed the watermark. The less watermark information is embedded, the less modification to the original image. Invisibility can be more effectively achieved with fewer embedded watermarks. The possibility of extracting the watermark after the image is attacked will significantly increase as the number of embedded watermark increases. From the perspective of robustness, the more watermarks embedded, the better the robustness of the watermark. This creates a contradiction between invisibility and robustness.

Zero watermarking technology is a watermarking technology that constructs a watermark by extracting features of the original image without modifying the original data. Therefore, the zero-watermark technology has good invisibility and solves the contradiction between invisibility and robustness. Directly extracting features and storing them in a third-party database saves the time for inverse transformation from the time domain to the transform domain, and improves the time and space efficiency of the algorithm.

The remote sensing image is a reflection of real ground objects, and its data is authentic. In order to avoid modifying the original data while protecting copyright information, the zero-watermark algorithm is applied to remote sensing images. This will make the protection of copyright more reasonable and effective.

2. Related Works

At present, with the in-depth research on digital watermarking, a variety of digital watermarking algorithms have been proposed. Although the digital watermarking algorithm in the time domain is simple, the performance of watermarking is poor. Therefore, a transform domain watermark that is more in line with actual needs appears. More popular ones are the watermark algorithm based on Discrete Cosine Transform (DCT) [4-6], the watermark algorithm based on Discrete Wavelet Transform (DWT) [7], the watermark algorithm based on Discrete Fourier Transform (DFT) [8-10], etc. In order to improve the performance of the algorithm, EMD [11] and BEMD [12-13] algorithms appeared. The BEMD algorithm has high security and a large amount of embedding. BEMD greatly improves the efficiency of watermark embedding and has been widely used.

3. Preliminary

3.1. Bidimensional Empirical Mode Decomposition

The main idea of one-dimensional empirical mode decomposition (EMD) is that any signal can be decomposed into the sum of several intrinsic mode functions (IMF). EMD is suitable for analyzing nonlinear and non-stationary signal sequences. After setting the number of decomposition levels to m, the input host image is decomposed into m intrinsic mode functions IMF and residual components by EMD.

The intrinsic modal function needs to meet two constraints:

In the entire data segment, the number of extreme points and the number of zero points are equal or the difference cannot exceed one at most;
At any point, there is a local maximum and a local minimum. The average value of the upper and lower envelopes formed is zero, that is, the upper and lower envelopes are locally symmetric with respect to the time axis at any point. The host image can be decomposed by EMD as:

\[ I = \sum_{i=1}^{m} IMF_i + I_r \]

Bidimensional Empirical Mode Decomposition (BEMD) is the promotion of EMD in two-dimensional space. BEMD’s requirements for IMF are the same as EMD’s requirements for IMF. The algorithm steps of BEMD are:

**Step 1.** Find all local extreme points of the input image surface.

**Step 2.** Perform surface fitting according to the extreme points obtained in the first step, and find the maximum envelope surface, the minimum envelope surface and the mean envelope surface.

**Step 3.** The new image surface is the original image data minus the mean envelope data.

**Step 4.** Determine whether the new image surface meets the condition \( SD < \sigma \), where \( \sigma \) is the threshold set in advance, and the calculation formula is:

\[
SD = \sum_{i=0}^{M} \sum_{j=0}^{N} \frac{|I'_m(i,j) - I'_s(i,j)|^2}{I^2_s(i,j)}
\]

If the above conditions are not met, repeat Step1~Step3 until the conditions are met. At this time, the first IMF of the original image is obtained. Using the remaining amount \( I_{r1} \) of the first layer as the new original image, perform Step1~Step4 again. Repeat the above steps until the number of IMFs is equal to the preset value. The final several IMFs and residuals are the two-dimensional empirical mode decomposition results of the original image.

### 3.2. Common Types of Attacks

After the watermark is embedded in the original image, it needs to be attacked to test the performance of the watermark. The attack types selected in this article include filtering, sharpening, histogram equalization, Gamma transformation, noise and scaling. Among them, sharpening, low-pass filtering, histogram equalization, and Gamma transformation are enhanced processing attacks [14-15].

The main goal of sharpening is to enhance edge and contour effects. Histogram equalization transforms the image histogram to cover all gray levels as much as possible and the gray level distribution is uniform. Gamma transformation is to correct bleached or too dark photos through nonlinear transformation. Image scaling belongs to the category of geometric transformation. After geometric transformation, the spatial position of the original image pixels in the new image changes.

### 3.3. Evaluation Method of Digital Watermark

In order to measure the performance of digital watermarking, some parameters need to be introduced for evaluation. Two commonly used parameters are Peak signal-to-noise Ratio (PSNR) and Normalized correlation (NC).

PSNR provides a measure of the degree of image distortion. In this article, it is used to reflect the difference between the watermarked image and the original image. The distortion of the image is smaller and thus the performance of the digital watermark is better as a smaller PSNR value is achieved. The calculation formula of PSNR is:

\[
PSNR = 10 \times \log \left( \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{255^2}{(I(i,j) - I'(i,j))^2} \right)
\]
Among them, \( M \times N \) is the size of the original image, \( I' \) is the image with embedded watermark, and \( I \) is the original image.

The NC value reflects the similarity between the watermark extracted after attacking the original image and the embedded watermark. The closer the NC value is to 1, the greater the degree of similarity between the extracted watermark and the embedded watermark, that is, the higher the robustness of the watermark. The calculation formula of NC value is:

\[
NC = \frac{\sum_{i=1}^{p} \sum_{j=1}^{q} W(i, j) \ast W'(i, j)}{\sum_{i=1}^{p} \sum_{j=1}^{q} W^2(i, j)}
\]

Among them, \( p \times q \) is the size of the watermark image, \( W \) and \( W' \) respectively represent the embedded and extracted watermark image.

4. Algorithm flow
This paper proposes a remote sensing image zero watermarking algorithm based on BEMD. In this section, 100 color remote sensing images with different sizes and different contents are used as the host image, and the feature image after binarization is used as the watermark image to show the watermark construction, embedding and extraction algorithm of this article.

4.1. Constructing a watermark
Discrete Cosine Transform (DCT) is one of the commonly used transforms in image watermarking, which is mainly used to compress data or images. DCT transform is lossless and has symmetry, so embedding watermark through DCT has better stability.

In the zero-watermark algorithm, the watermark image is not used for embedding, but the characteristic watermark is extracted from the original image. This article uses DCT method to transform the original image and extract its high frequency part. After that, it can be binarized to get the characteristic image. The transformation matrix determined by DCT reflects the correlation characteristics of the image signal to the greatest extent. Taking image No. 049 and No. 038 as examples, the extracted feature images are:

![Image](image.png)

**Figure. 1 Feature Image Display**
4.2. Embedding of watermark information

In order to reduce the amount of information in the image and speed up the calculation speed, the original image is grayed first. The specific formula is:

\[ \text{Gray} = \sqrt{\frac{R^2 + (1.5G)^2 + (0.6B)^2}{1 + 1.5^2 + 0.6^2}} \]

Perform BEMD decomposition on the gray-scaled host image to obtain IMF and remaining amount. In this paper, the decomposition level of BEMD is set to 6. Take image No. 049 as an example to show the result of BEMD decomposition.

![IMF decompositions](image)

**Figure. 2 BEMD Decomposition Result of 049**

In general, the first few IMFs contain the high frequency information of the original image, and the latter few IMFs contain the low frequency information of the original image. Generally, low-frequency information is more robust than high-frequency information. Therefore, choose one IMF from the latter to embed the watermark. The following table shows the NC value of the original image and the original image after the i-th IMF is missing. The larger the corresponding NC value, it means that embedding the watermark in the layer of IMF has the least impact on the original image.

| Layers Number | 1     | 2     | 3     | 4     | 5     | 6     |
|---------------|-------|-------|-------|-------|-------|-------|
| 038           | 0.8357| 0.8524| 0.8843| 0.9052| 0.9031| 0.9899|
| 049           | 0.8329| 0.8578| 0.8943| 0.8960| 0.9019| 0.9888|

It can be seen from the above table that the NC value is the largest under the 6th IMF. Therefore, the feature image is embedded in the sixth layer IMF.

XOR the information matrix of the 6th layer IMF of the host image with the feature image:

\[ x \ominus r_{ij} = d'_{ij} \oplus w'_{ij} \]

\( x \ominus r \) is the result obtained after the original image information is embedded in the feature image.

The algorithm flow of watermark embedding is:

**Step 1.** Grayscale the input original image;
Step 2. Perform BEMD decomposition on the grayscaled image to obtain 6 IMFs and the remaining amount.

Step 3. Calculate the NC value of the original image and the original image after the i-th IMF is missing.

Step 4. Embed the feature image in the IMF layer corresponding to the maximum NC value.

Step 5: XOR the information matrix of the 6th layer IMF of the host image with the feature image to obtain the image embedded with the watermark.

4.3. Extraction of watermark

Attack the image embedded with the watermark and extract the watermark from the attacked image. Perform another XOR between the attacked image and the result of the first XOR to obtain the extracted watermark information. At each pixel, the calculation formula is:

\[ x_{ij}' = x_{ij} \oplus \text{attack}_{ij} \]

4.4. Algorithm summary

The overall flow of the algorithm is:

Step 1. Perform a two-dimensional empirical mode decomposition of the original image, and separate six IMF layers and a margin.

Step 2. Binarize the watermark. In order to make the binarization result more balanced and better, you need to choose a suitable algorithm.

Step 3. Take XOR (first XOR) between the binarized watermark information and the original image information.

Step 4. After attacking the image, perform BEMD processing to separate six IMF layers and one margin.

Step 5. XOR the result of the first XOR with the binary information of the image after the attack.

Figure. 3 Algorithm flowcharts

5. Experimental results

5.1. Some experimental results

By comparing and extracting the watermark in the attacked image and the embedded watermark, the performance of the digital watermark can be evaluated. The following shows the extracted watermark and the NC value of the embedded watermark. The result of the original image No. 049 is displayed as follows:
### Table. 2 NC value under various attack types

| Attack method        | Attack name                        | NC value of BEMD sixth layer |
|----------------------|-----------------------------------|-----------------------------|
| GausLowpass1         | Gaussian filter [2, 2]             | 0.939424148                |
| GausLowpass2         | Gaussian filter [3, 3]             | 0.832548528                |
| GausLowpass3         | Gaussian filter [5, 5]             | 0.858100656                |
| GausLowpass4         | Gaussian filter [7, 7]             | 0.777504712                |
| GausLowpass5         | Gaussian filter [9, 9]             | 0.426044256                |
| Middle1              | median filtering [2, 2]            | 0.602536544                |
| Middle2              | median filtering [3, 3]            | 0.941587043                |
| Middle3              | median filtering [5, 5]            | 0.723746384                |
| Middle4              | median filtering [7, 7]            | 0.956979028                |
| Middle5              | median filtering [9, 9]            | 0.588342491                |
| Wiener1              | Wiener filtering [2, 2]            | 0.995289142                |
| Wiener2              | Wiener filtering [3, 3]            | 0.932737681                |
| Wiener3              | Wiener filtering [5, 5]            | 0.727353768                |
| Wiener4              | Wiener filtering [7, 7]            | 0.906662315                |
| Wiener5              | Wiener filtering [9, 9]            | 0.98560794                 |
| Average1             | Average filter [2, 2]              | 0.939424148                |
| Average2             | Average filter [3, 3]              | 0.892933713                |
| Average3             | Average filter [5, 5]              | 0.652540756                |
| Average4             | Average filter [7, 7]              | 0.549962959                |
| Average5             | Average filter [9, 9]              | 0.678482743                |
| Sharpening1          | sharpen amount 2                   | 0.960663208                |
| Sharpening2          | sharpen amount 3                   | 0.986362782                |
| Sharpening3          | sharpen amount 5                   | 0.976548168                |
| Sharpening4          | sharpen amount 7                   | 0.965463391                |
| Sharpening5          | sharpen amount 9                   | 0.867063599                |
| Histogram1           | histogram equalization 128 bit     | 0.93171121                 |
| Histogram2           | histogram equalization 64 bit      | 0.964322176                |
| Histogram3           | histogram equalization 32 bit      | 0.98909921                 |
| Histogram4           | histogram equalization 16 bit      | 0.95780107                 |
| Histogram5           | histogram equalization 8 bit       | 0.725249747                |
| GammaTransaction1    | Gamma transform attack 3           | 0.90237959                 |
| GammaTransaction2    | Gamma transform attack 2           | 0.927543424                |
| GammaTransaction3    | Gamma transform attack 0.75        | 0.888780132                |
| GammaTransaction4    | Gamma transform attack 0.5         | 0.60821755                 |
| GammaTransaction5    | Gamma transform attack 0.25        | 0.98091773                 |
| Salt1                | salt-and-pepper noise 0.01        | 0.905400489                |
| Salt2                | salt-and-pepper noise 0.03        | 0.913151365                |
| Salt3                | salt-and-pepper noise 0.05        | 0.943134108                |
| Salt4                | salt-and-pepper noise 0.1         | 0.927845533                |
| Salt5                | salt-and-pepper noise 0.12        | 0.958571104                |
| Speckle1             | Speckle noise 0.001                | 0.958312655                |
| Speckle2             | Speckle noise 0.005                | 0.960440968                |
| Speckle3             | Speckle noise 0.007                | 0.984917285                |
| Speckle4             | Speckle noise 0.009                | 0.972310475                |
| Speckle5             | Speckle noise 0.011                | 0.927277269                |
It can be seen that the NC values corresponding to the sixth layer IMF are almost all above 0.9, and some NC values are close to 1. The experimental results show that the similarity of the watermark before and after the attack is relatively high, the common attacks do less damage to the watermark, and the watermark has a strong anti-attack ability.

6. Robustness experiment of watermarking

In order to verify the robustness of the watermark, it is necessary to calculate the distortion rate of the attacked image compared to the original image. The smaller the distortion rate, the stronger the robustness of the watermark. The PSNR values of the attacked images No. 049 and No. 038 and the original image are shown as follows:

![Figure 4 PSNR results](image)
It can be seen from the above figure that, except for Gamma attacks and histogram equalization, the PSNR values corresponding to most of the other attacks are between the ideal value of 20-30. Since the principle of PSNR is related to the number of bits represented by pixels, and histogram equalization will change the number of bits represented by pixels, Gamma transformation greatly changes the pixels of the entire picture, so the PSNR results corresponding to Gamma attacks and histogram equalization are basically no significance.

7. Conclusions and Prospects

7.1. Conclusions
This paper proposes a zero-watermark algorithm for remote sensing images based on BEMD. The feature image extracted by DCT is unique and robust, which enhances the security of the watermarking algorithm. Calculate the NC values of the original image and the original image after the i-th IMF is missing. The position where the watermark is embedded is the number of IMF layers corresponding to the largest NC value. This embedding method minimizes the loss of original image information and enhances the invisibility of the watermark. The experimental results show that the algorithm proposed in this paper has strong ability to resist attacks, and the digital watermark has high invisibility and robustness.

7.2. Prospects
In the era of big data, the dissemination of images will become more frequent, and the research on digital watermarking will become more and more in-depth. BEMD does not need to set the basis function, and is self-adaptive, so it has certain advantages. But BEMD makes the algorithm slower. The future direction of improvement is to increase the speed of the algorithm.

References
[1] Hsu C T, Wu J L. Hidden digital watermarking in images [J]. IEEE Transactions on Image Processing, 1999, 8(1):58-68.
[2] Changjiang Zhang, Jinshan Wang, Xiaodong Wang. Digital Image Watermarking Algorithm with Double Encryption by Arnold Transform and Logistic [C]. In: Fourth International Conference on Networked Computing and Advanced Information Management. Gyeongju, 2008, 329-334.
[3] Cox I J, Miller M L, Bloom J A. Digital Watermarking [M]. Morgan Kaufmann Publishers, 2002.
[4] Lin, S.D; Chin-Feng Chen. A robust DCT-based watermarking for copyright Protection [J]. Consumer Electronics, IEEE Transactions on, 2000, 46(3):415-420.
[5] Dongyang Teng, Renghui Shi, Xiaoqun Zhao. DCT Image Watermarking Technique Based on the Mix of Time-domain [C]. In: Information Theory and Information Security, International Conference on IEEE. Beijing, 2010, 826-830.
[6] Hsu C-T, Wu J L. Hidden signature in images [J]. IEEE Trans. on Image Processing, 1999,8(1):58-68.
[7] Wang S H, Lin Yuanpei. Wavelet Tree Quantization for Copyright Protection Watermarking [J]. IEEE Trans. on Image Processing, 2004, 13(2): 154-165.
[8] Poljicak A, Mandic D, Agic D (2011) Discrete Fourier transform–based watermarking method with an optimal implementation radius. J Electron Imaging 20(3):033008-033008
[9] Savakar D G, Ghuli A. Non-blind digital watermarking with enhanced image embedding capacity using DMeYer wavelet decomposition, SVD, and DFT [J]. Pattern Recognition and Image Analysis, 2017, 27(3): 511-517
[10] Tsui T K, Zhang X P, Androutsos D. Color image watermarking using multidimensional Fourier transforms [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 16-28
[11] Huang N E, Zheng Shen, Long S R. The empirical mode decomposition and hilbert spectrum for nonlinear non-stationary time series analysis [J]. Proc R Soc London Ser A, 1998, 454(1971): 903-995.

[12] J. C. Nunes, Y. Bouaoune, E. Delechelle et al. Image analysis by bidimensional empirical mode decomposition. Image and Vision Computing, Vol.21, No.12, 2003, 4: 1019-1026.

[13] NUNES J C, BOUAOUNE Y, DELECHELLE E, et al. Image analysis by bidimensional empirical mode decomposition [J]. Image and Vision Computing, 2003, 21(12): 1019-1026.

[14] Su J K, Eggers J J, Girod B. Optimum attacks on digital watermarks and its Defense [C]. In: Thirty-Fourth Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, 2000, 1836-1840.

[15] Voloshynovskiy S. Pereira S., Pun T., et al. Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks [J]. IEEE Commun. Mag., 2001,39(8): 118-126.