Zero-Frequency and Low-Frequency Information Hiding Algorithm Based on Scale-Invariant Local Features Postprint

Authors: Ren Shuai, He Yuan, Liu Yunong, Xu Zhenchao, Zhang Tao, Wang Zhen, Mu Dejun

Date: 2018-08-13T00:00:00+00:00

Abstract

To address the weak resistance of current information hiding algorithms against steganalysis, we propose a zero-low-frequency information hiding algorithm based on scale-invariant (binary robust invariant scalable keypoints, BRISK) local features. First, a first-order CL multiwavelet transform is performed on the carrier image, and BRISK feature points are extracted from the low-frequency LL2 subband to generate an image feature matrix. Second, zig-zag scanning and Logistic chaotic scrambling are used to decorrelate the secret information. Third, the image features and encrypted information are compared through feature values to form an association sequence. Finally, the association sequence is embedded into the three least significant bits (LSBs) of the high-frequency HL2 and HH2 subbands. The algorithm hides the association information constructed from the feature matrix of high-energy regions and twice-encrypted information in the high-frequency region, which benefits the robustness and anti-analysis capability of the algorithm. Under analysis tests using high-order statistics on 200 images, the maximum detection rate is below 7.516%, demonstrating that the proposed algorithm has good anti-analysis capability.

Full Text

Preamble

Zero-Low-Frequency Information Hiding Algorithm Based on Local BRISK Features

Ren Shuai[1], He Yuan[1], Liu Yunong[1], Xu Zhenchao[1], Zhang Tao[1]†, Wang Zhen[1], Mu Dejun[2]

(1. a. School of Information Engineering; b. School of Electronic & Control Engineering, Chang' an University, Xi' an 710064, China; 2. College of Automation, Northwestern Polytechnical University, Xi' an 710072, China)

Abstract: To address the weak resistance of current information hiding algorithms against steganalysis, this paper proposes a zero-low-frequency information hiding algorithm based on Binary Robust Invariant Scalable Keypoints (BRISK) local features. First, the algorithm performs a first-order CL multi-wavelet transform on the carrier image and extracts BRISK feature points in the low-frequency LL2 subband to generate an image feature matrix. Second, it decorrelates the secret information using zig-zag scrambling and Logistic chaotic scrambling. Third, it constructs an association sequence by comparing feature values between the image features and encrypted information. Finally, the association sequence is embedded into the three least significant bits (LSBs) of the high-frequency HL2 and HH2 subbands. By hiding the association information—constructed from the feature matrix of high-energy regions and twice-encrypted data—in high-frequency regions, the algorithm achieves favorable robustness and anti-analysis performance. Under high-order statistical analysis of 200 images, the maximum detection rate remains below 7.516%, demonstrating the algorithm' s strong resistance to steganalysis.

Keywords: zero-low-frequency information hiding; BRISK feature; CL multi-wavelet transform; anti-analysis capability

0 Introduction

With the explosive growth of network information, information security has attracted significant attention. As an important branch of information security, information hiding serves as a crucial means for secret communication and has become a hot research topic. In recent digital image information hiding algorithms, existing approaches exhibit several limitations. Some methods embed information by modifying low-frequency coefficients, which affects visual quality due to substantial changes. Others consistently modify the same coefficient pairs, resulting in obvious local feature transformations. While combining CL multi-wavelet transform with composite bit-plane theory leverages energy distribution characteristics, the variety of robust information hidden in low-frequency components compromises invisibility. Techniques using compressed sensing and GHM multi-wavelet transforms modify singular values, but large-scale alterations make image features vulnerable to attacks. Similarly, histogram-based embedding in the AMBTC domain introduces distortion issues. These algorithms share a common weakness: they directly hide information by modifying relatively important pixel locations, resulting in poor invisibility and weak anti-steganalysis performance since attackers can analyze transformed image features.

Zero-watermarking technology achieves embedding by establishing a mapping relationship between carrier image features and the digital watermark without

modifying any image characteristics, thereby resisting steganalysis. Considering that low-frequency components contain primary image information, this paper proposes an information hiding approach based on zero-low-frequency technology. To ensure the extracted low-frequency information approximates the original image, we employ CL multi-wavelet transform. For robust feature mapping, particularly against cropping attacks, we utilize BRISK features from computer vision. To enhance security through decorrelation, we apply zigzag scrambling for position disruption and Logistic chaotic sequences with good pseudo-random properties to alter pixel values. This yields a zero-low-frequency information hiding algorithm based on BRISK features. The algorithm extracts BRISK features from the low-frequency subband after CL multi-wavelet transform, performs dual scrambling on secret information, generates an association sequence between image features and encrypted data, and finally embeds this sequence into high-frequency components. MATLAB experiments demonstrate excellent invisibility, robustness, tamper detection capability, and resistance to steganalysis.

1 Proposed Information Hiding Algorithm

The proposed algorithm consists of four main stages: (a) performing first-order CL multi-wavelet transform on the carrier image; (b) extracting BRISK feature points in the high-energy LL2 region based on the unique energy distribution characteristics of CL multi-wavelet transform, selecting points from regions with high texture complexity; (c) generating 512-bit binary feature descriptors using the BRISK algorithm and converting them into an 8×8 image feature matrix; (d) establishing an association between the hidden information and feature matrix to achieve information hiding.

1.1 CL Multi-Wavelet Transform Processing

CL multi-wavelet transform is constructed using symmetry, offering short support, second-order vanishing moments, and orthogonality. Notably, energy concentrates in the lowest resolution subband' s low-frequency LL2 region [7], as shown in Table 1 . Leveraging this property, we perform first-order CL multi-wavelet transform on the carrier image [Figure 1: see original paper], extracting feature vectors from the LL2 region containing 96.53% of the original image' s energy to ensure robustness and anti-analysis capability. The association information generated from secret data is embedded into the high-frequency HL2 and HH2 subbands, which originate from the LL1 decomposition and contain 97.36% of the energy, thereby guaranteeing both robustness and invisibility.

1.2 BRISK Feature Point Extraction

BRISK feature points exhibit rotation invariance, scale invariance, noise resistance, and compression robustness [8]. The algorithm detects features using a FAST9-16 operator in pyramid scale space, applies non-maximum suppres-

sion to points meeting FAST criteria, and performs sub-pixel interpolation for precise localization [Figure 2: see original paper]. The pyramid comprises 4 octaves (c) and 4 intra-octaves (d), where i = 0,1,2,3. The original image is c , d represents 1.5× downsampling, and adjacent octaves/intra-octaves have 2× downsampling relationships. The scale relationships are t(c) = 2 and t(d) = 2 .

We extract features from the LL2 subband after first-order CL multi-wavelet transform. Since BRISK features correspond to pixel discontinuities, regions with more neighboring features indicate stronger textures—representing important image areas. These complex texture regions are selected because they remain robust even under cropping attacks, as losing such regions would compromise the image' s transmission value. The feature point with the maximum number of neighboring features within its region is selected to generate the feature descriptor. The neighborhood radius is adaptively determined using Equation (1), where is a constant controlling radius size and t represents the feature point' s scale value, ensuring scale invariance.

1.3 Image Feature Matrix Generation

Using the selected feature points from Section 1.2 as centers, we define a sampling pattern with 4 concentric circles of different radii [Figure 3: see original paper]. We obtain 60 equally spaced sampling points on each circle, apply Gaussian filtering to eliminate aliasing effects, and form all possible pairs (60×(60-1)/2 pairs). Using thresholds from the original BRISK algorithm (9.57t for short-distance pairs, 13.67t for long-distance pairs), we classify point pairs accordingly. The sampling pattern is rotated by angle to ensure rotation invariance, where represents the feature point's dominant orientation calculated from long-distance pair gradients using Equation (3). We select 512 short-distance pairs and compare their intensity values using Equation (4) to generate a 512-bit binary descriptor. This descriptor L is divided into 8-bit segments, converted to decimal integers (0-255), and rearranged into an 8×8 matrix J serving as the image feature matrix.

1.4 Hidden Information Embedding Steps

a) Perform zig-zag scrambling on secret image T using a custom rule: scan from the matrix' s bottom-right corner in a "Z" pattern upward, storing pixel values in 1D array S. Reverse S to generate array S with iteration count Z = 10, producing scrambled image W.

b) Apply Logistic chaotic map scrambling to W using Equation (5) with control parameter and initial value t to generate chaotic sequence T . Divide W into 16 blocks, sequentially taking one pixel per block into array G. Use the first 8 bits of T as permutation vector A and the last 8 bits as vector B. Based on each adjacent bit pair in T , perform bitwise XOR or XNOR operations between G values and A or B according to Table 2

to obtain new gray values, producing scrambled bit sequence D.

c) Randomly select four integers e,f,g,h [0,7] to construct coordinates (e,f) and (g,h) in matrix J. Compare J(e,f) and J(g,h). If equal, reselect values; otherwise, establish bitwise association between J and secret sequence D according to Table 3 . Repeat until all bits of D are associated, then serially connect the association information to form sequence K.

d) Embed K into the three LSBs of HL2 and HH2 coefficients using minimal modification: for each association value (0-7), modify at most 3 bits with probabilities of modifying 1-2 bits = 3/8 and modifying 3 bits or none = 1/8, ensuring high invisibility.

e) Embed zig-zag parameter Z and Logistic parameters , t into the LH2 component.

f) Perform inverse CL multi-wavelet transform to obtain the stego-image T .

1.5 Information Extraction Steps

a) Perform first-order CL multi-wavelet transform on stego-image T to decompose subcomponents LL2, LH2, HL2, HH2.

b) Extract BRISK features from LL2, match them with saved descriptor L to locate feature point C, and regenerate image feature matrix J using Section 1.3' s procedure.

c) Extract LSBs from HL2 coefficients, convert each 3-bit segment to decimal, and serially connect to form association sequence K . Read coordinates (e,f) and (g,h) sequentially, compare J (e,f) and J (g,h) to decode secret bits: if J (e,f) < J (g,h) → "0" , otherwise → "1" . Repeat to obtain secret sequence D . Perform identical operations on HH2 to get D .

d) Compare D and D to verify transmission integrity. If identical, information was transmitted securely. If different, check sequence lengths—completeness indicates no attack, while significant shortage suggests attack. Select the complete sequence as the final extracted secret.

e) Extract scrambling parameters Z, , t from LH2. Apply inverse Logistic scrambling to D or D using , t to obtain W , then inverse zig-zag scrambling using Z to recover original secret information T .

2 Experiments and Results Analysis

Experiments were conducted in MATLAB R2013a using 512×512 grayscale "barbara"as carrier image [FIGURE:4(a)] and 64×64 binary "baboon"as secret image [FIGURE:4(b)]. The resulting stego-image is shown in [FIGURE:4(c)].

2.1 Invisibility Experiments

Testing 100 images (512×512) with the proposed algorithm yields PSNR results shown in [Figure 5: see original paper], where the x-axis represents embedding capacity 2 bits and y-axis shows Peak Signal-to-Noise Ratio (PSNR) [11]. At k = 14 (16,384 bits embedded), PSNR = 42.082 dB, indicating high invisibility for k 14.

Comparing our hybrid-domain algorithm (BRISK-ZLF) with frequency-domain W-W [3] and hybrid-domain AMBTC-HS [6] at equivalent embedding strengths, BRISK-ZLF achieves an average PSNR of 42.625 dB versus 38.204 dB for W-W, representing an 11.57% improvement. AMBTC-HS averages 41.235 dB, similar to BRISK-ZLF. At embedding strengths of 0.125 and 0.25, AMBTC-HS maintains slightly higher PSNR due to encountering equal high-low mean sequence blocks that don' t affect quality after shifting. However, AMBTC-HS operates on 512×512 AMBTC domains while BRISK-ZLF uses only 128×128 high-frequency regions, giving AMBTC-HS higher capacity. Nevertheless, at embedding strengths 0.25, BRISK-ZLF demonstrates superior overall invisibility performance.

2.2 Robustness Experiments

Robustness measures algorithmic robustness—the integrity of secret information after attacks. Since our algorithm requires re-extracting BRISK features, robustness testing is critical. We use Normalized Correlation (NC) coefficient [11] as the evaluation metric, where higher NC indicates better robustness and secret information completeness, defined in Equation (6).

The stego-image underwent cropping, rotation, scaling, salt-and-pepper noise, Gaussian noise, and filtering attacks. Extracted secret information results are shown in [Figure 6: see original paper]. Visual experiments confirm that secret information becomes recognizable when NC 0.56. Our algorithm shows strong robustness: for cropping rates < 60% and rotation angles < 100.5°, NC 0.56.

Comparing BRISK-ZLF with W-W and AMBTC-HS [Figure 7: see original paper]: at 45% cropping rate, BRISK-ZLF achieves NC = 0.719 versus 0.490 (W-W) and 0.530 (AMBTC-HS), representing 46.73% and 35.66% improvements respectively. At 60° rotation, BRISK-ZLF' s NC = 0.598 versus 0.410 (W-W) and 0.480 (AMBTC-HS), showing 45.85% and 24.58% improvements. Overall, BRISK-ZLF' s average NC is 0.601, compared to 0.452 (W-W) and 0.483 (AMBTC-HS), demonstrating robustness improvements of 32.96% and 24.43% respectively.

2.3 Tamper Detection Experiments

By comparing extracted sequences D and D from HL2 and HH2, the algorithm achieves tamper detection. At cropping rate 6%, rotation 10°, scaling 5%, salt-and-pepper noise (d = 0.05), white noise parameters (0.1, 0.004), and Wiener

filtering ([3,3]), the detection rate reaches 96.22% across 200 images , indicating excellent tamper awareness.

2.4 Anti-Analysis Experiments

Anti-analysis capability is the macroscopic performance indicator. Our algorithm constructs association sequences between fully decorrelated secret information (via dual scrambling) and low-frequency BRISK features, then hides them in the three LSBs of high-frequency HL2 and HH2 subbands—regions with negligible energy and strong concealment. Using a high-order wavelet statistics detection algorithm [12], experimental results [Figure 8: see original paper] show that across 50 random images, no threshold can separate stego-images from cover images. Testing 200 images yields a maximum detection rate below 7.156% [FIGURE:8(b)], confirming strong anti-steganalysis performance.

3 Conclusion

This paper proposes a zero-low-frequency information hiding algorithm based on BRISK features. BRISK features provide inherent robustness, and their extraction from low-frequency components further enhances algorithmic robustness. The zero-low-frequency approach extracts features only from low-frequency regions while embedding in high-frequency regions, strengthening anti-analysis capability. The algorithm utilizes the three LSBs of high-frequency subbands for embedding with 3 bit modifications, ensuring invisibility. Dual scrambling removes correlation from secret information, and the final hidden association sequence theoretically improves anti-analysis performance significantly. Embedding identical information in both HL2 and HH2 regions achieves 96.22% tamper detection accuracy. Future work will focus on increasing capacity through optimized embedding region selection and secret information compression preprocessing while maintaining invisibility.

References

[1] Liu Yanbo. Information hiding algorithm of wavelet transform based on JPEG image [J]. Journal of Beihua University: Natural Science, 2017, 18(5): 697-700.

[2] Cai Zhengbao. Research and practice of an improved digital image hiding algorithm based on wavelet transform [J]. Journal of Jiamusi University: Natural Science Edition, 2015, 33(6): 861-863.

[3] He Ziheng, Zhang Jiawen, Hou Tong, et al. A new image information hiding method based on frequency domain [J]. Journal of Software, 2014, 13(5): 167-169.

[4] Zhang Tao, Ren Shuai, Ju Yongfeng, et al. Secret information sharing algorithm based on CL multi-wavelet transform and combination bit plane for con-

fidential communication [J]. Journal of Computer Applications, 2013, 33(11): 3232-3234.

[5] Zhang Tao, Kang Yuan, Ren Shuai, et al. Information hiding algorithm based on compression sensing and GHM multi-wavelet transform [J]. Journal of Computer Applications, 2017, 37(9): 2581-2584.

[6] Zhang Tao, Liu Yunong, Xing Yalin, et al. Lossless information hiding in AMBTC domain based on histogram shift [J/OL]. Application Research of Computers, 2019, 36(6): 1-8 [2018-04-08]. http://kns.cnki.net/kcms/detail/51.1196.TP.20180408.1051.076.html.

[7] Xu Tao, Wu Dengfeng, Liu Jie, et al. Application of multiwavelet orthogonal expansion algorithm in image processing [J]. Journal of Jilin University: Engineering Science, 2006(5): 778-781.

[8] Leutenegger S, Chli M, Siegwart R Y. BRISK: binary robust invariant scalable keypoints [C]// Proc of International Conference on Computer Vision. 2011: 2548-2555.

[9] Lu Ping, Dong Husheng, Ma Xiaohu. An image scrambling algorithm based on extended ZigZag and bit exchange [J]. Computer Applications and Software, 2012, 29(10): 310-313.

[10] Zhang Yonghong, Zhang Bo. Image encryption algorithm based on Logistic chaotic system [J]. Application Research of Computers, 2015, 32(6): 1770-1773.

[11] Mohd B J, Abed S, Al-Hayajneh T, et al. FPGA hardware of the LSB steganography method [C]// Proc of International Conference on Computer, Information and Telecommunication Systems. 2012: 1-4.

[12] Farid H, Lyu S. Higher-order wavelet statistics and their application to digital forensics [C]// Proc of Conference on Computer Vision and Pattern Recognition Workshop. 2003: 94-94.

Note: Figure translations are in progress. See original paper for figures.