A Highly Robust Zero-Watermarking Algorithm Based on Curvelet-DSVD and Visual Cryptography (Post-print)

Authors: Qu Changbo, Wu Deyang

Date: 2018-05-18T00:00:00+00:00

Abstract

To better represent the curve characteristics of natural images and further enhance the robustness of digital watermarking algorithms, a strongly robust zero-watermarking algorithm combining Curvelet-DSVD and visual cryptography is proposed. First, Arnold scrambling is applied to the original image; second, a Curvelet transform is performed to obtain low-frequency domain information, which is then divided into blocks, with each block undergoing double singular value decomposition (DSVD). The feature matrix is constructed by exploiting the relationship between the maximum singular value of each block and the overall mean of singular values, while simultaneously employing visual cryptography to generate two share images from the watermark information; finally, one of the share images is subjected to Arnold scrambling and then XORed with the feature matrix to generate the zero watermark. Experimental results demonstrate that the proposed algorithm can effectively resist common attacks and, compared with existing zero-watermarking algorithms, exhibits stronger robustness and higher security.

Full Text

Preamble

Strong Robust Zero-Watermarking Algorithm Based on Curvelet-DSVD and Visual Cryptography

Qu Changbo, Wu Deyang
(College of Software, Liaoning Technical University, Huludao, Liaoning 125105, China)

Abstract: To better represent the curve characteristics of natural images and further improve the robustness of digital watermarking algorithms, this paper

proposes a robust zero-watermarking algorithm based on Curvelet-DSVD and visual cryptography. First, the original image undergoes Arnold scrambling. Second, Curvelet transform is applied to obtain low-frequency domain information, which is then partitioned into blocks for double singular value decomposition (DSVD). A feature matrix is constructed by exploiting the relationship between each block' s maximum singular value and the mean of all singular values. Simultaneously, visual cryptography is employed to generate two shares of the watermark information. Finally, one share is Arnold-scrambled and XORed with the feature matrix to generate the zero-watermark. Experimental results demonstrate that the proposed algorithm effectively resists conventional attacks and exhibits stronger robustness and security compared to existing zero-watermarking algorithms.

Keywords: Curvelet transform; double singular value decomposition (DSVD); visual cryptography; robustness

0 Introduction

Traditional transform-domain watermarking algorithms face an inherent conflict between transparency and robustness. To address this, Wen Quan et al. [**?**] introduced the concept of zero-watermarking. Since zero-watermarking algorithms do not embed copyright information into the carrier image, they provide excellent protection for content integrity, leading to widespread adoption in copyright protection applications [**?**, **?**].

Most conventional zero-watermarking algorithms construct feature information using wavelet transforms and singular value decomposition (SVD) [**?**]. Reference [**?**] constructs zero-watermarks via discrete wavelet transform and SVD, demonstrating good stability against small-scale noise, filtering, and compression attacks, but showing poor robustness against high-intensity attacks. Reference [**?**] proposes a robust zero-watermarking algorithm based on invariant centroids, which effectively resists geometric attacks but suffers from low watermark similarity under shear and rotation attacks due to its failure to account for geometric impacts. Reference [**?**] presents a dual zero-watermarking scheme based on DWT-SVD, applying Haar wavelet twice to extract the low-frequency LL2 subband for zero-watermark construction. However, filtering and noise attacks still affect the feature matrix construction.

Recent research has introduced novel watermarking algorithms [**?**]. Reference [**?**] constructs feature matrices from regions of interest and generates zero-watermarks through XOR operations with watermark images. While robust against conventional attacks, this approach has limitations when ROIs are targeted. Reference [**?**] leverages DCT' s energy concentration properties for zero-watermarking, but feature matrices based on block means exhibit poor stability. To enhance stability, Zeng Wenquan et al. [**?**] propose an integer wavelet transform-based robust zero-watermarking algorithm using chaotic encryption principles, showing strong robustness against non-geometric attacks but neglect-

ing geometric impacts, resulting in low similarity under shear and rotation attacks.

To overcome geometric attacks, Qu Changbo et al. [**?**] combine wavelet transform with visual cryptography for zero-watermarking based on edge detection, demonstrating good robustness against small-scale noise but poor performance against geometric attacks. Xiao Zhenjiu et al. [**?**] propose a zero-watermarking algorithm using enhanced SVD and cellular neural networks, addressing diagonal distortion through singular value uniformization and neural networks, though at the cost of increased computational complexity. While wavelet transforms effectively separate high and low frequencies, natural images contain abundant texture features with prominent curve singularities. Wavelet transforms excel at point singularities but poorly represent curve singularities, causing significant watermark degradation under attacks.

To address these limitations, this paper proposes a robust zero-watermarking algorithm based on Curvelet-DSVD and visual cryptography. Curvelet transform captures curve features more effectively than wavelet transforms, while DSVD enhances security and reduces false positives. Visual cryptography splits the watermark into two shares, enabling three-party authentication and improving security.

1 Theoretical Background

1.1 Curvelet Transform Theory

Curvelet transform is a multiresolution, bandpass, directional function analysis method implemented through specialized filtering and multiscale Ridgelet transforms. It achieves near-optimal nonlinear approximation error decay for image curve edges, providing excellent representation of curve feature information [**?**]. For input $f(t_1, t_2)$ in Cartesian coordinates, the discrete form of Curvelet transform is:

$$c^D(j, l, k_1, k_2) = \sum_{\substack{0 \le t_1 < n \\ 0 \le t_2 < n}} f[t_1, t_2] \phi^D_{j,l,k}(t_1, t_2)$$

where j is the scale parameter, l is the orientation parameter, and $k = (k_1, k_2)$ is a translation parameter. Candès and Donoho proposed a fast discrete Curvelet transform implementation based on USFFT (unequally spaced fast Fourier transform) [**?**]:

a) Perform 2D FFT on the given 2D function in Cartesian coordinates to obtain frequency domain information $\widehat{f}[n_1, n_2]$.

b) Resample $\widehat{f}[n_1, n_2]$ to obtain corresponding sample values at each scale and orientation.

c) Multiply the interpolated $\hat{f}$ with window function $\tilde{U}_{j,l}$ to get $\tilde{f}_{j,l}[n_1, n_2] = \hat{f}[n_1, n_2]\tilde{U}_j[n_1, n_2 - n_1 \tan\theta_l]$.

d) Apply inverse FFT to $\tilde{f}_{j,l}$ to obtain the discrete Curvelet coefficient set $c^D(j, l, k)$.

[Figure 1: see original paper] shows a Curvelet decomposition example. Figure 1(a) is a 512×512 Lena image, (b) shows the Curvelet transform decomposition, and (c) shows wavelet transform decomposition. The Lena image is decomposed into 6 scale layers by Curvelet transform: the first layer is the Coarse scale, the sixth (outermost) layer is the Fine scale, and layers 2-5 are Detail scales with 8, 8, 16, and 16 directional subbands respectively, each composed of high-frequency coefficient matrices. In contrast, wavelet transform divides the image into only 4 layers as shown in Figure 1(c).

[Figure 2: see original paper] compares the energy distribution histograms. The horizontal axis represents transform layers, and the vertical axis represents energy. Curvelet transform concentrates most energy in the first layer with minimal energy in other layers, while wavelet transform distributes significant energy across layers 2-4 (primarily high-frequency information).

1.2 Double Singular Value Decomposition (DSVD)

SVD is a fundamental matrix analysis tool that decomposes a matrix into three matrices. For an $m \times n$ matrix I, SVD is expressed as:

$$I_{m\times n} = U_{m\times m}\Sigma_{m\times n}V^T_{n\times n}$$

where U is the left singular matrix, Σ is the diagonal singular value matrix, and V^T is the right singular matrix. SVD is crucial for image denoising and compression, and its inherent attack resistance makes it popular in digital watermarking. However, traditional SVD has low security and suffers from false positive problems [**?**].

To address these issues, we propose Double Singular Value Decomposition (DSVD), which enhances security and reduces false alarms. Unlike direct SVD, DSVD first performs bidiagonalization:

a) Decompose matrix I into bidiagonal form:

$$I = U_B\Sigma_B V_B^T$$

where U_B and V_B are orthogonal matrices.

b) Perform SVD on the bidiagonal matrix Σ_B to obtain the maximum singular value matrix:

$$\Sigma_B = U_S\Sigma_S V_S^T$$

1.3 Visual Cryptography

Visual cryptography, proposed by Moni Naor and Adi Shamir [**?**], is a novel cryptographic scheme for visual systems. Its core idea encrypts a secret image into two shares: the first share acts as ciphertext, and the second as a decryption key. Each share appears as random noise, preventing attackers from obtaining information about the other share or the secret image.

This paper uses visual cryptography to generate two keys from the watermark. One key is Arnold-scrambled and combined with image features to create the zero-watermark, while the other is used for verification. The encryption process follows:

$$\begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \\ 1 \end{bmatrix} & \text{for black pixels} \\ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \text{for white pixels} \end{cases}$$

[Figure 3: see original paper] shows a visual cryptography example: (a) is the watermark image, (b) and (c) are the two non-overlapping shares (share1 and share2) generated through visual cryptography.

2 Zero-Watermarking Algorithm

2.1 Zero-Watermark Generation

The zero-watermark generation process constructs image feature information as follows. First, a 512×512 image undergoes Arnold scrambling, followed by Curvelet transform, block partitioning, and DSVD to construct a feature matrix. Simultaneously, the copyright watermark is encrypted using visual cryptography to generate two shares. One share is Arnold-scrambled and XORed with the feature matrix to produce the zero-watermark. The zero-watermark and the other share are stored at the copyright protection center.

The detailed steps are:

a) Perform Arnold scrambling on the 512×512 carrier image I_c:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$$

b) Apply Curvelet transform to the scrambled image to obtain the coefficient matrix $I_{256\times256}$.

c) Partition $I_{256\times256}$ into blocks B_k:

$$B_k(i,j) = \begin{cases} I_{c_{mn\times mn}}(i/4, j/4) & \text{if} \mod(i,4) = 0 \text{ and} \mod(j,4) = 0 \\ 0 & \text{otherwise} \end{cases}$$

where $i, j \in \{1, 2, 3, ..., 256\}$ and $k \in \{1, 2, 3, ..., 64\}$.

d) Compute the maximum singular value $S_{\max}^{i,j}$ for each block B_k using equations (6) and (8) to form the maximum singular value matrix $S_{\max}$. Then calculate its mean M_T using equation (13).

e) Construct the feature matrix F using the relationship between each block' s maximum singular value $S_{\max}^{i,j}$ and the overall mean M_T:

$$F(i,j) = \begin{cases} 1 & \text{if } S_{\max}^{i,j} > M_T \\ 0 & \text{otherwise} \end{cases}$$

f) Encrypt the watermark image W using visual cryptography to generate two secret shares w_1 and w_2. Arnold-scramble w_1 to obtain w_1'.

g) XOR the scrambled share w_1' with feature matrix F to generate zero-watermark Z: $Z = w_1' \oplus F$. Store Z and w_2 at the copyright protection center, while clients keep the two scrambling keys K_1 and K_2.

[Figure 4: see original paper] illustrates the zero-watermark generation process.

2.2 Copyright Authentication

The authentication process retrieves zero-watermark Z and secret share w_2 from the copyright protection center. The feature extraction process mirrors steps a)-e) from Section 2.1 to obtain a new feature matrix F'.

The steps are:

a) XOR zero-watermark Z with the newly constructed feature matrix F' to recover the scrambled secret share: $w_1' = Z \oplus F'$.

b) Obtain key K_2 from the client and apply Arnold inverse scrambling to w_1' to get the decrypted share w_1.

c) Overlap decrypted share w_1 with w_2 from the copyright center to reconstruct the copyright watermark W.

[Figure 5: see original paper] shows the copyright authentication process.

3 Experiments

3.1 Parameter Configuration

Experiments were conducted on a 64-bit Windows 7 system with MATLAB R2014a. Carrier images were standard 512×512 grayscale images: Airplane, Lena, Baboon, Paper, and Bride [FIGURE:6(a)-(e)]. The copyright watermark was a 64×64 binary image containing the text "版权水印" [FIGURE:6(f)]. Visual cryptography generated two shares [FIGURE:6(g)-(h)], and share1 was further scrambled to enhance security and robustness [FIGURE:6(i)].

3.2 False Alarm Rate Experiment

To evaluate false alarm issues, we computed similarities between zero-watermarks generated from the five carrier images in [Figure 6: see original paper]. Lower similarity indicates lower false alarm rates. Results are shown in .

The maximum similarity between different zero-watermarks is 0.5777, the minimum is 0.4385, with an average of 0.5033, demonstrating low false alarm rates for the proposed algorithm.

3.3 Non-Geometric Robustness Attacks

Common non-geometric attacks include noise, filtering, and compression. Experiments focus on these attack types.

1) Noise Attack: We tested salt-and-pepper noise resistance across different intensities on five carrier images, computing NC values. Results are in .

As noise intensity increases, NC values remain high across all images, averaging above 0.9100. For Lena, NC values range from 0.8938 to 0.9769. Other images average above 0.9123, showing strong robustness.

2) JPEG Compression Attack: Different compression strengths were applied to five carrier images. Results in show average NC values above 0.9945, indicating strong resistance to JPEG compression.

3) Median Filtering Attack: Using filter templates of 3×3, 5×5, 7×7, and 9×9, results in demonstrate NC values between 0.9637-0.9991, with even 9×9 templates averaging above 0.9813.

3.4 Geometric Robustness Attacks

Geometric attacks (rotation, row/column shifting) cause significant image changes, substantially affecting watermark extraction.

1) Rotation Attack: Small-angle rotations of 1°, 2°, and 3° were applied. shows the algorithm exhibits good robustness against rotation attacks.

2) Row/Column Shifting Attack: Images were shifted in four directions with lost pixels set to 0. shows NC values above 0.9671 for 2-column shifts, and above 0.9236 for 5-row shifts. Curvelet' s multiscale, multidirectional properties enable effective watermark extraction under directional attacks.

3.5 Combined Attacks

To further validate robustness, combined attack experiments were conducted: rotation+noise, JPEG compression+noise, JPEG compression+median filtering, shift+median filtering, and shift+Gaussian noise. shows strong performance, with NC values above 0.9913 for JPEG 30%+median filtering, and averaging 0.9668 for JPEG 30%+Gaussian noise 0.05.

3.6 Comparative Experiments

Using 512×512 Lena as carrier and 64×64 binary watermark, we compared our algorithm with references [?, ?, ?]. and figures show superior performance.

1) Robustness Analysis: Our algorithm outperforms [?, ?, ?] against both non-geometric and geometric attacks. For salt-pepper noise 0.2, [?] achieves only 0.8040 NC. [Figure 7: see original paper] shows our NC values consistently higher across noise intensities. [Figure 8: see original paper] demonstrates comparable or better JPEG compression performance. Curvelet-DSVD enhances robustness by better preserving edge information compared to wavelet transforms' local limitations.

For geometric attacks, improvements are substantial: ~6% better than [?] against shearing, and ~5% higher NC values across rotation angles [Figure 9: see original paper]. At 3° left rotation, our NC remains ~0.93 while [?, ?, ?] drop below 0.9. Row/column shifting improvements range 2-9% over [?, ?, ?] because block maximum singular values are more stable than block means under pixel position changes.

2) Security Analysis: Our algorithm offers higher security than [?, ?, ?], which use only traditional encryption. We scramble the carrier image during feature extraction to eliminate pixel correlation and enhance security. Attackers cannot extract consistent features without the scrambling key. Visual cryptography and Arnold scrambling encrypt the watermark such that the zero-watermark is constructed from noise-like shares rather than directly from the copyright watermark, preventing information leakage even if the zero-watermark is compromised.

4 Conclusion

This paper proposes a robust zero-watermarking algorithm based on Curvelet transform, DSVD, and visual cryptography. The algorithm overcomes traditional zero-watermarking' s inability to represent natural image curve characteristics and its poor robustness against high-intensity attacks. Visual cryptography splits the copyright watermark for three-party authentication, while Arnold scrambling of shares enhances security. Experimental results demonstrate strong robustness against noise, filtering, compression, rotation, and shifting attacks, with high security. However, robustness against high-intensity combined attacks requires further optimization. Future work will focus on improving anti-attack capabilities in complex environments.

References

[1] Wen Quan, Sun Tanfeng, Wang Shuxun. Concept and application of zero-watermarking [J]. Acta Electronica Sinica, 2003, 31(2): 214-216.

[2] Wu Weimin, Ding Ran, Lin Zhiyi, et al. Tamper localization zero-watermarking algorithm for medical images based on chaos [J]. Application Research of Computers, 2014, 31(12): 3685-3688.

[3] Rao Y R, Nagabhooshanam E. A novel image zero-watermarking scheme based on DWT-BN-SVD [C]//Proc of International Conference on Information Communication and Embedded Systems. 2014: 1-6.

[4] Rani A, Bhullar A K, Dangwal D, et al. A zero-watermarking scheme using discrete wavelet transform [J]. Procedia Computer Science, 2015, 70: 603-609.

[5] Liu P, Tan Y. Robust zero-watermarking algorithm based on invariant centroid [C]//Proc of International Conference on Computational and Information Sciences. 2013: 758-761.

[6] Chen Weiqi, Li Qian. Dual zero-watermarking algorithm for images based on DWT-SVD [J]. Computer Engineering and Science, 2014, 36(10): 1991-1996.

[7] Zhang L, Cai P, Tian X, et al. A novel zero-watermarking algorithm based on DWT and edge detection [C]//Proc of the 4th International Congress on Image and Signal Processing. 2011: 1016-1020.

[8] Zhao Jie. Image zero-watermarking algorithm based on DCT mean [J]. System Simulation Technology, 2015, 11(4): 304-306.

[9] Zeng Wenquan, Xiong Xiangguang. Robust zero-watermarking algorithm based on integer wavelet transform [J]. Microelectronics & Computer, 2016, 33(4): 97-101.

[10] Qu Changbo, Li Dongdong. Zero-watermarking algorithm based on visual cryptography and edge detection [J]. Computer Applications and Software, 2016, 33(9): 328-333.

[11] Xiao Zhenjiu, Zhang Han, Chen Hong, et al. Zero-watermarking algorithm based on enhanced singular value decomposition and cellular neural networks [J]. Journal of Image and Graphics, 2017, 22(3): 288-296.

[12] Wang Taiyue, Li Hongwei, Li Zhiming. Digital watermarking algorithm based on Curvelet transform [J]. Mathematics in Practice and Theory, 2012, 42(17): 124-128.

[13] He Bing. Blind watermarking algorithm resisting rotation attacks based on SVD and Radon transform [J]. Computer Engineering and Applications, 2012, 48(20): 200-205.

[14] Srilakshmi P, Himabindu C. Image watermarking with path based selection using DWT & SVD [C]//Proc of International Conference on Computational Intelligence and Computing Research. 2016: 1-5.

[15] Naor M, Shamir A. Visual cryptography [C]//Advances in Cryptology-Eurocrypt' 94. 1995: 1-12.

[16] Qu Changbo, Yang Xiaotao, Yuan Duoning. Zero-watermarking algorithm based on visual cryptography in wavelet domain [J]. Journal of Image and Graphics, 2014, 19(3): 365-372.

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