https://doi.org/10.1051/matecconf/201926702007

Research on Digital Watermarking Algorithm for Anti-geometric Attack

Lixuan Lin

School of Instrumentation Science and Opto-electronics Engineering, Beihang University, Beijing, China

Abstract. For the problem that the traditional digital watermarking algorithm is less robustness against geometric attacks, this paper introduces the related content of digital watermarking technology, which combs digital watermarking technology, digital watermarking attack technology and digital watermarking evaluation method, and summarizes the improved algorithms proposed in recent years. Next, the traditional wavelet transform algorithm and the improved algorithm based on DCT transform are selected for comparison experiments. The latter combines Arnold scrambling and SVD decomposition, which has better shear resistance. Finally, combined with the research status, the future research focus of digital watermarking algorithm is prospected.

1 Overview

1.1 Digital watermarking technology

Digital watermarking technology refers to an information technology that uses the redundancy of media such as images and sounds to embed other secrets that are not perceived in the information content[1]. This embedded information is usually not visible, but can be detected or extracted by calculation means. Digital watermarking technology is commonly used for digital media copyright protection.

The basic characteristics of digital watermarking technology include imperceptibility, robustness, watermark capacity, validity, security, blind detection, false detection and missed detection, and provability[2].

In particular, the robustness of digital watermarking[3] is an indicator for evaluating the strength of a watermark against attack. The water-printed multimedia products will produce some distortion or artificial attacks in the process of network circulation. The highly robust algorithm can still completely extract the water-printed multimedia products after being attacked, and determine the property rights information. Obviously, the higher the robustness, the better the watermark's resistance to attack, and the more effective it is to protect the intellectual property of digital products.

1.2 Digital watermark attack technology

The editing and modification of digital images often leads to information loss, and the watermark and image are closely combined, which will affect the normal detection and extraction of watermarks. These operations can be regarded as attacks on watermarks[4].Watermark attacks are divided into active attacks and passive attacks. The so-called active attacks destroy the watermark so that the information carried by them is unreadable, and the passive attack is to break the watermark algorithm. Most watermark attacks are active attacks. Digital watermark attacks include geometric attacks, interpreted attacks, watermark removal attacks, collusion attacks, and statistical attacks.

Geometric attack[5] is to make some changes in space or time of watermarked image works through processing operations (such as scaling, cropping, rotating, distorting, panning, cropping, projection, etc.). The geometric attack can only make the watermark information existing on the image not detected by the watermark detection machine, but the watermark information cannot be completely removed.

This method of attack does not make any changes to the original watermark, but rather falsifies the original image for confusion, so that the ownership of the work cannot be determined.

The removal of watermark attacks[4] mainly includes common processing for images such as denoising, filtering, histogram modification, quantization, and lossy compression. These operations result in loss of image information, especially compression, which can eliminate redundancy as much as possible while ensuring certain information quality, resulting in loss or even undetectable watermark information.

The collusion attack is to add multiple different watermarks on the same work to generate multiple copies to obtain an approximate image, so that the watermark in the image cannot be recognized by the detection system.

The statistical attack is to achieve the purpose of removing the watermark, and use the statistical model and probability to estimate and predict the watermark signal or the original image.

1.3 Digital watermarkevaluation method

The method and standard for evaluating watermarking algorithms is an important part of digital watermarking research. In the evaluation process of performance testing, a series of attacks on the watermark system are needed to test its performance[6]. The watermark test is mainly considered from the perspective of watermark robustness, that is, when the watermark is subjected to various attacks, it can still be extracted. However, there is currently no uniform test standard, and most test standards can only be applied to a certain watermark algorithm. In order to get a unified watermarking test standard, many scholars and organizations have studied the benchmark of watermarking test standard, and obtained some results of evaluation methods.

First, Peak Signal Noise Power Ratio (PSNR) is used to measure the invisibility of the embedded watermark, and the normalized cross correlation coefficient (NC) is used to measure the similarity between the extracted watermark and the original watermark. The formula is as follows:

$$PSNR = 10\lg\left(\frac{c_1 c_2 \max I^2}{\sum_{i=1}^{c_1}\sum_{j=1}^{c_2}[I(i,j) - I^{'}(i,j)]^2}\right) \tag{1}$$

$$NC = \frac{\sum_{i=1}^{c_2}\sum_{j=1}^{c_1} W(i,j)W^{'}(i,j)}{\sum_{i=1}^{c_2}\sum_{j=1}^{c_1} W^2(i,j)} \tag{2}$$

Second, Stir Mark[7] is a universal watermark benchmark software designed by Fabien Petitcolas of the University of Cambridge, England, which has become the most widely used watermarking technology evaluation tool in the watermark field. Stir Mark can evaluate the robustness of watermarking algorithms from many aspects, and simulate various watermarking attacks to test the robustness of watermarking. Stir Mark is a general-purpose watermarking algorithm robustness test program that evaluates its security and robustness by applying various attacks to water-based prints. It now only supports image media, and has extended interfaces for other media. When given watermarked images, Stir Mark generates a certain number of modified images. These modified images are used to verify if the watermark can be detected.

Third, the median truth value measurement method and MMTD method[8]. Applying the method of mediating truth value measurement and MMTD method to the robustness of watermark is an intelligent algorithm.

$$y = f(x) = |1 - \frac{\text{watermark carrier size}}{\text{receiver watermark carrier size}}| \tag{3}$$

The greater the watermark robustness detection function value, the stronger the attack intensity of the watermark and the serious damage of the watermark; on the contrary, the smaller the value, the weaker of the attack intensity against the watermark, the weaker of the watermark damage.

1.4 Digital watermarking algorithm for anti-geometric attack

Geometric attacks are more destructive to image watermarking algorithms. An imperceptible damage may invalidate the watermarking algorithm, while most word image watermarking algorithms have weaker ability to resist geometric attacks. In recent years, experts and scholars have proposed many watermarking algorithms against geometric attacks.

Feature point extraction is used to extract feature points. Several typical feature point extraction methods are Harris feature points, MSER (Maximally Stable Extremal Region), and Hessian Affine feature points. Use the end-stopped wavelet to detect the end point, corner point, or point with high curvature of the curve. The first derivative of the filter is applied to these linear structures, which can detect the end points of the line or the points with larger curvature, and has better robustness and robustness than other methods.[9]Aiming at the problem of poor anti-geometric attack ability of wavelet transform domain digital watermarking algorithm, a DWT digital watermarking algorithm based on SIFT feature point matching is adopted. It combines the characteristics of rotation, scaling and translation invariance of the matching feature points with the DWT watermarking algorithm, and realizes the geometric attack parameter estimation and correction of the watermarked image according to the scale feature and coordinate relationship of the SIFT feature points[10].In addition, if the watermark is embedded, the image is firstly partitioned, and then the watermark is embedded in the non-subsampled Contourlet transform low frequency subband of the subblock, which simplifies the watermark embedding and increases the embedding capacity[11].

In order to improve the ability of zero watermarking technology to resist attacks, [12] proposed a new robust zero watermarking algorithm based on integer wavelet transform. First the algorithm preprocesses the copyright information and performs a second-order integer wavelet transform on the carrier image. Secondly, the low-frequency sub-bands are not overlapped, and the feature matrix is obtained according to the relationship between the mean value of each block and the mean value of the low-frequency sub-bands. Finally, this feature matrix is combined with the pre-processed copyright information to construct zero watermark information, which is then pre-registered into the intellectual property database.[13] There is a zero digital watermarking method based on LPM (log polar coordinates) and bispectrum analysis is proposed to resist rotational geometry transformation. The two-level redundant discrete wavelet transform constructs the feature matrix and constructs a zero watermark together with the encrypted watermark image and the feature matrix[14].

SVD (Singular Value Decomposition) is also a typical algorithm, and an improved algorithm based on SVD is also very common. In order to resist the geometric attack of QR code digital watermark image, in [15]a digital watermarking technique based on singular value decomposition and discrete wavelet transform is proposed. In [16] a wavelet domain digital image watermarking algorithm combining SVD and HVS features is proposed. First, the algorithm performs a second-level DWT on the carrier image, extracts the second-order low-frequency sub-band and performs blocking; Then SVD is performed on each sub-block, and the contradiction between watermark transparency and robustness is solved.

Arnold transform is used in many robust watermarking algorithms. In [17] a watermarking algorithm based on Daisy descriptor is proposed. It also performs Arnold transformation on the watermark information before embedding the watermark, which improves the security of the watermark image. It uses the Daisy descriptor to describe each pixel in the image, then it uses the BSP tree to divide the Daisy feature space. In [18] a robust blind watermarking algorithm based on QR decomposition for Contourlet domain is proposed. First the algorithm performs Arnold scrambling preprocessing on the binary watermark image, then performs Contourlet transform on the host image, extracts the low frequency subbands for non-overlapping partitions, and finally performs QR decomposition on each subblock.

2 The method of this paper

A digital watermarking algorithm based on wavelet transform domain is a typical algorithm. It realizes the embedding and extraction of watermarks through the second-order wavelet transform, and has good resistance to various types of noise attacks, but it performs poorly in anti-geometric attacks.

Based on this, this paper chooses an improved algorithm based on DCT transform. The main idea of the digital watermarking algorithm in the DCT domain is to first divide the digital image into equal-sized blocks of pixels and transform them to obtain frequency blocks composed of DCT coefficients. Then, some frequency blocks are selected according to certain criteria, and the digital watermark information is embedded by slightly changing the coefficients of the selected DCT frequency block to satisfy a specific relationship.

In the improved algorithm using DCT (Discrete Cosine Transform), the current frequency domain watermarking technology cannot effectively resist the problem of rotation attack. Therefore, an anti-rotation attack digital watermarking algorithm based on structural similarity index (SSIM) is proposed[19].Its water-printed image has a peak signal-to-noise ratio (PSNR) of 43, which is effective against 1~360°rotation attacks. The watermark information has certain complementarity through positional transformation. Through reconstruction, the integrity of the image in the process of extracting watermark information is guaranteed, which can effectively resist the shear attack[20].

In this paper, the binary sub-watermark image Arnold is scrambled and DCT transform is performed on the sub-block image sub-block. The gray layer of the carrier image is divided into 8×8 small blocks, and each block is subjected to two-dimensional DCT transformation, and then combined with SVD decomposition and inverse transformation. When extracting the watermark, the gray layer is subjected to DCT transformation, and the previously changed value is extracted, and compared with the random frequency to restore the watermark pattern. Experiments show that the algorithm is robust against geometric attacks.

3 Experimental result

In this paper, the grayscale (256×256) image is used as the carrier image, and the binary image with the letter BUAA (32×32) is used as the watermark image to perform the shear attack comparison experiment. The experiment was carried out in the environment of matlab2012b.

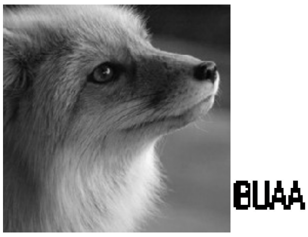

Figure 1. Original image&Original watermark.

In the next figures, there are watermarked image, the image when above is cut and the extracted watermark.

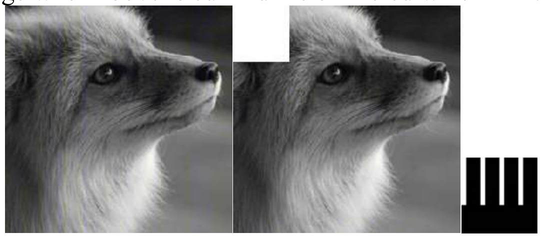

Figure 2. Based on wavelet transform.

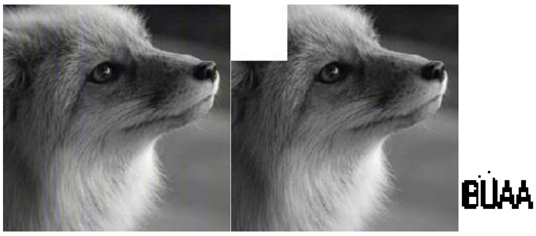

Figure 3. Based on DTC transform.

It can be seen that the improved algorithm based on DTC transform obviously has better performance against shear attack.

4 Conclusion

In this paper, a typical algorithm and an improved algorithm are selected for comparison experiments. The superiority of the improved algorithm against shear attack can be clearly seen from the experimental results.

In view of the significance of studying digital watermarking algorithms against geometric attacks, And the current research status, most improved algorithms focus on the geometric attack on the image as a whole and the algorithm is more complicated. Therefore, increasing the amount of information embedded and reducing the computational complexity and resisting local geometric attacks (such as deformation and distortion) may become important research directions.

References

1. Lv Jiu-ming. Study on digital watermarking technique and jamming. Communication Countermeasures, 2004(04):18-21.
2. Xiao Di, Deng Mi-mi, Zhang Yu-shu. Robust and separable watermarking algorithm in encrypted image based on compressive sensing. Journal of Electronics & Information Technology, 2015, 37(5):1248-1254.
3. Li Xun. Research on digital watermarking algorithms against geometric attacks. Changchun University of Technology, 2018.
4. Yang Yongfeng. Research on attack and test of image digital watermark. Gansu Science and Technology, 2014, 30(21):15-16.
5. Nie Xuan, Huang Deng-shan, Guo Da-wei, Cao Bei. Overview of digital image watermarking technology. Computer Knowledge and Technology, 2015, 11(03):189-192.
6. Sun Chao. Research on DWT-SVD based blind digital image watermarking. South China University of Technology, 2012.
7. Li Lin-jing, Zheng Yue-zhai. Application of stir mark in the analysis of robust watermark. Computer Knowledge and Technology, 2015, 11(07):256-260.
8. Zhu Lizhi. A method for evaluating the degree of damage of digital watermarks. Electronic World, 2014(16):357-358.
9. Zhao Yan-li, Wang Xing, Ma Xiao-pu, Li Zheng-yan. Robust image watermarking scheme against geometric attacks. Journal of Chinese Computer Systems, 2014, 35(08):1931-1936.
10. Wang Zu-hui, Sun Liu-jie, Jiang Zhe-wei, Wang Xiao-hong, Liu Xuan-xuan. A watermarking algorithm against geometric attack in DWT domain. Packaging Engineering, 2015, 36(21):102-107+114.
11. Jia Chao, Zhang Zheng-bao. Resistance to geometric attacks watermarking algorithm based on RIT-SIFT. Journal of Ordnance Engineering College, 2013, 25(05):49-54.
12. Zeng Wen-quan, Xiong Xiang-guang. Robust zero watermarking algorithm based on integer wavelet transform. Microelectronics & Computer, 2016, 33(04):97-101+107.
13. He Bing. A zero image watermarking resisting to rotation attack based on LPM and bispectrum analysis. Journal of Weinan Normal University, 2017, 32(16):29-34.
14. Liu Wanjun, Sun Siyu, Qu Haicheng, Feng Lin, He Muze. Anti-geometric rotation attack zero watermarking algorithm. Application Research of Computers, 2019(10):1-9[2018-09-27].
15. Xue Qing-chen, Wu Dan, Chen Da-qing, Chen Wei-xia, Gu Ji-hua. Geometrical attack resistant digital watermarking technology based on DWT-SVD and QR code. Packaging Engineering, 2016, 37(11):158-163.
16. Ren Keqiang, Liang Liangliang, Yu Lingjuan. Robust digital image watermarking in wavelet domain based on SVD and HVS. Journal of Electronic Measurement and Instrumentation, 2017, 31(06):869-875.
17. Gao Kaikai. Digital watermarking algorithm based on daisy descriptor for geometric attack images. Software Guide, 2016, 15(01):43-46.
18. Liu Hai, Chen Jun. Robustblind watermarking algorithm in contourlet domain based on QR decomposition. Computer Applications and Software, 2016, 33(06):306-310+324.
19. Bao Guan-xiao, Sun Liu-jie, Li Yu-bin, Yu Hai-jiao. Digital watermarking technology against arbitrary rotation attack. Journal of Optoelectronics·Laser, 2015, 26(01):156-161.
20. Bai Wei. Shearing attack research based on DCT watermarking algorithm. Journal of Taiyuan Normal University (Natural Science Edition), 2014, 13(03):63-66.