Asymmetric watermarking technique based on Fourier Transform

Junpeng Wu[1, a],Shouzheng Li[2,b] ,Ye Yuan[3,c] , Yuanyuan Wang[4,d] , Chao Liu[5,e] , Weimiao Feng[6,f] ,and Min Yu[7,g]

[1]Harbin Engineering University, Harbin , China, 150001

[2]Harbin Engineering University, Harbin , China, 150001

[3]Harbin Engineering University, Harbin , China, 150001

[4]Northeast Forestry University, Harbin , China, 150001

[5]Institute of Information Engineering,Chinese Academy of Sciences,Beijing,China,100093

[6]Institute of Information Engineering,Chinese Academy of Sciences,Beijing,China,100093

[7]Institute of Information Engineering,Chinese Academy of Sciences,Beijing,China,100093

[a]wujunpeng@hrbeu.edu.cn, [b]26407166@qq.com, [c]569093011@qq.com, [d] stdong0451@163.com, [e]2443532866@qq.com, [f]330227346@qq.com, [g]272523869@qq.com

Keywords: Asymmetric digital watermarking, Fourier transform, signal reconstruction.

Abstract. In this paper an asymmetric digital watermarking technique based on the Fourier transform. The technique utilizes phase and magnitude component and their one-way combination methods of both components in order to protect the watermark sign being reconstructed with detection signal. A method that using the phase component as the public key and magnitude component as the private key is proposed this paper, as an example of this technique.

Introduction

Digital watermarking technology in media files, especially for voice, video and image copyright protection data has been fully studied. For different media files, application scenarios, the watermark verification purposes have a lot based on signal processing, human perception watermark loading algorithm sensitivity analysis. Currently, the vast majority of watermarking technology is to rely on the use of the watermark signal when loaded to extract the signal modulated by the watermark information, the watermark such model has a congenital defect, i.e., the watermark can be detected can also be the person watermark data from the carrier Clear or partially cleared, thereby reducing the detection efficiency of the watermark. Such watermarking algorithm is called by people the "symmetricwatermarking"technology.

Another emerging research direction is the watermark to verify the conditions required to load and separation makes it possible to detect the watermark information is insufficient for removal. This method is called "asymmetric watermarking" technology, can greatly improve the security of watermark information.

Based on asymmetric watermark Fourier transform algorithm

In this paper, a one-way operation and watermark verification protocols respective advantages designing a complete asymmetric public key watermark uniform testing load detection algorithm. Rely on the encryption algorithm analysis, simulation, design asymmetric watermarking algorithm. This paper proposes the use of Fourier watermark signal amplitude and phase components, respectively, as a public and private key to extract the watermark. The more traditional use of the full implementation of the watermark signal operation to extract the watermark, the proposed method uses only part of the watermark signal extraction, if you cannot get both at the same time is difficult to calculate the complete component watermark signal to be separated from the host signal. Therefore, using the relationship between two sets of signal amplitude and phase angle, and can be used as a public key and private key pairs, the following formula：

$$k_n = w_n = A_n e^{-jf_n} \tag{1}$$

Separation of public and private key pairs, so：

$$k_n^u = DFT^{-1}(A_n) \tag{2}$$

$$k_n^r = DFT^{-1} e^{-jf_n} \tag{3}$$

Wherein the private key; is the public key in the form of a Fourier series of the phase angle or amplitude components of the watermark signal. As we all know, only the Fourier amplitude or phase angle signal is completely impossible to reconstruct the watermark signal can only choose between one of the two components as a public announcement.

Detecting a watermark signal when the carrier signal is assumed that the watermark is loaded without any attack in the case of using the correlation detection result is:

$$\{r_n\} = \sum_{n=0}^{N-1} x_n k_n^u \tag{4}$$

Formula can perform the fast Fourier transform, on the one hand to improve the speed, on the other hand, facilitate energy analysis.

$$\begin{aligned} \{r_n\} &= DFT^{-1}(XK^{u+}) \\ &= DFT^{-1}((C+W)K^{u+}) \\ &= DFT^{-1}(CK^{u+} + WK^{u+}) \\ &= DFT^{-1}(CK^{u+}) + DFT^{-1}(WK^{u+}) \end{aligned} \tag{5}$$

If no watermark is detected the data X, the equation (1) in the entry does not exist, and therefore two separate signals correlated power spectral density PDS, its repercussions Fourier transform should be a relatively flat noise signal.

If the test data X containing a watermark, then {r} The watermark signal is self-Fourier transform correlation equation, then the {} is a pulse equation (Delta Function).

Therefore, the existence of the criteria of the watermark signal is correlated compare output {r} Is a pulse equation host.

Effect detection by the ratio, ie the SNR performance. If the noise is too large can make detection of failure.

Reason is due to noise generated by the correlation of the generated frequency domain fluctuation. Analysis of detection results from the analysis of two methods in the fluctuation component frequency domain i.e. (1) produced concluded.

Further analysis (\ ref {detection}) can be obtained:

$$\{r_n\} = DFT^{-1}\left(A_n^c A_n^w\right) + DFT^{-1}(A_n^w A_n^w) \tag{6}$$

$$\{r_n\} = DFT^{-1}\left(e^{f_n^c} e^{f_n^w}\right) + DFT^{-1}(e^{f_n^w} e^{f_n^w}) \tag{7}$$

(5)represented by the formula is a conventional DSS algorithm based correlation detector. Some of these two signals will have to meet a certain randomness high sequence length and independence conditions, and therefore its inverse Fourier transform will be a high randomness, volatile value group, so the detection affect the outcome will be very small. Another part is the watermark signal autocorrelation amplitude components, the result will be a set of relatively smooth positive value, therefore, the result of inverse Fourier transform will be very close equation. However, the energy of these two very different parts, the first part is the average carrier amplitude is multiplied by the ratio of the energy of the watermarking energy carrier (DWR), this ratio is usually small. In contrast, the other part is a square of the amplitude and phase watermark. Only in the first part, i.e., the average value of the carrier power approaches 0 with the case, the detection of the effect will be guaranteed.

Relative amplitude components, the two portions (6) completely eliminates the A part of the energy carrier and unified into the watermark portion is between -π and π. Eliminating the energy difference between the detection of the effect will be greatly improved.

Security Analysis

Previously mentioned, to detect the watermark component is public, then the private key can be used to load the watermark, also can be used to remove the watermark. In the application point of view that the owner of the private key is the watermark watermark signal protection methods. So you need to be aware algorithm design, the two components of which one is more suitable as a private key. As standard the private key must be difficult to be guessed causing rebuild the entire watermark signal.

From the theoretical analysis is not difficult to see that the amplitude component of the range is very broad, the only limitation is the DWR. DWR is due to an average ratio of, if not the power value of the original carrier signal or original signal can not accurately estimate the power of the watermark signal. Is concerned, in the range of the phase signal is compared to a fixed, theoretically the interval, the result is computer implemented quotient of the imaginary part of the Fourier coefficient of the real part, i.e.,

$$\arg(a + jb) = b / a \tag{8}$$

Which is within the range (-π, π] interval. The difference between the theoretical and the realization of the result of the correlation detector does not generate the difference, and therefore no longer distinguish.

Thus, the phase component ranges within a certain range of accuracy is quite easy to guess. Is this permissible range of accuracy of the test results may be related to the position pulled low and thus can not be done effectively detect. The following two results are the phase components as public key, whereby vandals can generate additional recombinant amplitude components of the watermark signal and the watermark information is removed from the watermarked portion of the carrier. However, due to the magnitude of the signal is private watermark signal, because it is difficult to be rebuilt, so when necessary, you can also use the private key for further testing.

Generating a set of Fc = 30% of the carrier signal and a set of white noise signal as a watermark. 1000 randomly generated set of amplitude components comply with the characteristics of white noise distribution, and separately with a public key of the watermark signal are combined into a phase component signal of the watermark signal attack loaded attack, the attack power of the signal is represented as the horizontal axis in Fig. 4, respectively, four load strength (80dB, 60dB, 40dB and 20dB) original watermark attack. Each curve in Fig presence highest, lowest and average detection values.

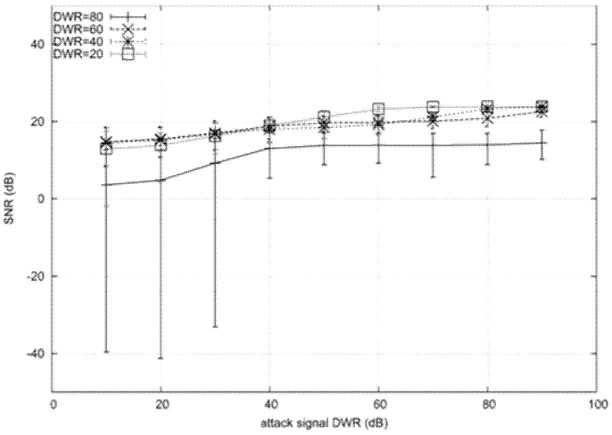

Fig.1: The use of phase signal reorganization watermark damage detection of public key results

Seen from Figure 1, when the watermark energy is relatively small, DWR = 80dB, and the attack of the signal energy is large, DWR = 10 to 30dB, vandals can be more successful results, the detection result is almost no credibility, -40dB. Watermark signal DWR = 80dB minimum value several curves, a large gap between the average and therefore it can be seen, even under such harsh conditions, the probability of a successful attack is relatively low. It should also be noted that the attack signal so strong that the carrier signal can lose value, even if a successful attack, cannot be used again Further, the test results show that the worst possible, i.e. only spoilers unknown information is the private key test watermark signal amplitude characteristics and the energy ratio (DWR) are all known as the attackers involved in the attack items. In practice may be a more random watermark signal amplitude characteristics, increase the difficulty of attack.

Even in the attack is successful, the watermark is still the owner of the private key can be used for testing, certification and thus its ownership. Figure 2 describes the results of FIG. 1 is identical, the only difference being that the result of the detection is carried out by the private key, i.e. amplitude component watermark. As can be seen from Figure 2, since the private key is not damaged, can still provide reliable results.

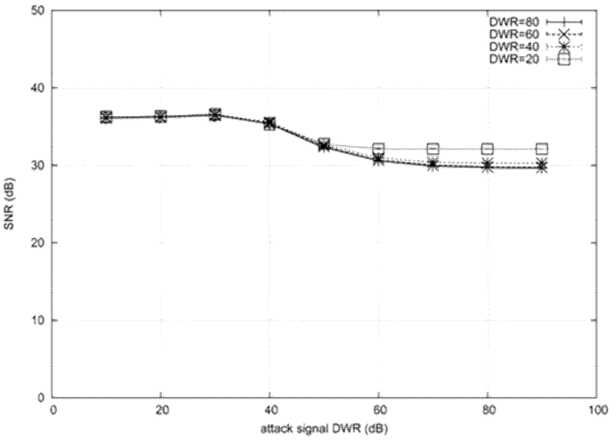

Fig.2: The use of phase signal reorganization watermark damage detection of private key results

Conclusions

Through analysis of the Fourier transform, and use its polar coordinate representation in the traditional watermark signal based on the establishment of a public / private key detection methods. And analyzing the amplitude and phase components by Fourier transform results can be used as public and private key pair watermark detection in different occasions. Through the analysis of the application conditions, the use of the results of this paper can design safe, effective public and private key pairs watermark detection scheme. By public and private key detection method, in the premise of ensuring the watermark cannot be completely removed while still providing effective results. The use of classical spreading embedding and detection methods, so this is no longer analyze its robustness. Further, the object used in the experiments herein is used instead of random signal images, video, sound, and other conventional real signal watermarks paper used, and its object is to avoid too much emphasis on embedding algorithm and the embedded position, it limits the use of this method range.

Acknowledgements

The research is supported by the National Science Foundation of China under Grant No. 61202455; the Doctoral Program of Higher Education Foundation of China under Grant No. 20112304120025; the Specialized Fundation for the Basic Research Operating expenses Program of Central College No. HEUCF100612, HEUCFT1202.

References

[1] HARTUNG F., Girod B.. Watermarking of uncompressed and compressed video [J]. Signal Process, 1998.66: p.283-301.

[2] COX I.etc.. Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 1997. 6: p.1673-1687.

[3] SVALBE D.I.,SCHYNDEL R., TIRKEL A. Key independent watermark detection. IEEE international conference on multimedia computing and systems, 1999.1: p.580-585.

[4] EGGERS J., SU J., GIROD B. Asymmetric watermarking schemes [C], in Sicherheit in Mediendaten, GMD Jahrestagung, Proceedings, 2000

[5] FURON T., DUHAMEL P. An asymmetric public detection watermarking technique [C]. Third internatioanl workshop on information hiding, 88-100, 1999.

[6] HOU Y. Visual cryptography for color images [J], Pattern Recognition, 36(7):1619-1629, 2003

[7] CHOI, LEE, KIM. Transformed-key asymmetric watermarking system [J]. IEEE singal processing Letters, 11(2):251-254, 2004.

[8] GUI, JIANG, HE. A new asymmetric watermarking scheme based on a real fractional DCT-I transform [J]. Journal of Zhejiang University SCIENCE A, 7(3):285-288, 2006.

[9] MUNIR, RIYANTO, SUTIKNO, AGUNG. An asymmetric watermarking method in the DCT domain based on rc4-permutation and chaoitc map [J]. ITB Journal of information and communication technology, 1:71-83, 2007.

[10]]MUNIR, RIYANTO, SUTIKNO AGUNG. A public-key watermarking method for still images based on random permutation [C]. International joint conference in engineering, 2008