ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Robust Encryption Based Watermarking Technique.

Divya S*, and Usha Nandini D.

Computer Science and Engineering, Sathyabama University, Chennai, India.

ABSTRACT

In recent years, the technology is characterized by the innovation and the revolution in the digital world, the field of media has become important. The communication using the multimedia data and replication have become major concerns of researchers. Therefore, protecting copyrights and ensuring service security is needed. Cryptography has a major role, is to protect secret files against unauthorized access. This project presents a robust encryption based watermarking technique. In the cryptographic watermark method, Discrete Cosine Transform (DCT) and Advanced Encryption Standard (AES) are used to split the image and hide the secret message within it.

Keywords: copyright, watermark, DCT, AES.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Steganography is a unique method of information hiding techniques. It embeds the secret messages into a host medium in order to conceal so as not arousing suspicion by an eavesdropper. A typical steganographic application includes covert communications between two parties whose existence is not known to the attackers and whose success depends only on detecting the existence of this communication. The host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3Dmodel etc.

In the cryptographic watermark method, the host image is divided into different number of blocks using the 2D- cosine transformation, followed by the encrypted data into the image. For each blocks, the rank based key is generated based on the Discrete Cosine Transform (DCT) [6]. In addition to splitting up of blocks and hiding the message, an encrypted private key is attached to it. The secret message that is to be transmitted is also encrypted using AES algorithm and hided inside the watermarked image and sent to the receiver along with the key. The receiver gets a private key while registering for the service and also receives the watermarked blocks as a whole image. The receiver can decrypt the message using the private key [11]. Since, the proposed system is highly secured by detecting and resisting against the attacks and hence the system improves the robustness of the technique.

The main aim of this project is to provide a secure communication between the sender and the receiver. For this the Discrete Cosine Transform (DCT) is used to split the images into number of blocks and Advanced Encryption Standard (AES) is used to encrypt the message.

DESIGN AND IMPLEMENTATION

In the cryptographic watermark method, the host image is divided into different number of blocks using the 2D- cosine transformation [9], followed by the encrypted data into the image. For each blocks, the rank based key is generated based on the Discrete Cosine Transform (DCT). In addition to splitting up of blocks and hiding the message, an encrypted private key is attached to it. The secret message that is to be transmitted is also encrypted using AES algorithm and hided inside the watermarked image and sent to the receiver along with the key. The receiver gets a private key while registering for the service and also receives the watermarked blocks as a whole image. On the receiver side the decryption process is done by the use of private key. Since, the proposed system is highly secured by detecting and resisting against the attacks and hence the system improves the robustness of the technique.

DCT ENCODING

The general equation for a 1D(N data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{1/2} \sum_{i=0}^{N-1} \wedge(i).\cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

And the corresponding inverse 1D DCT transform is $F^{-1}(u)$
Where

$$\wedge(i) = \begin{cases} \frac{1}{\sqrt{2}}, & \varepsilon = 0 \\ 1, & otherwise \end{cases}$$

The general equation for a 2D(N by M image) DCT is defined by the following equation

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \wedge(i).\wedge(j).\cos\left[\frac{\pi.u}{2.N}(2i+1)\right] \cos\left[\frac{\pi.v}{2.M}(2j+1)\right] f(i,j)$$

And the corresponding inverse 2D DCT transform is $F^{-1}(u,v)$

$$\wedge(\varepsilon) = \begin{cases} \frac{1}{\sqrt{2}}, & \varepsilon = 0 \\ 1, & otherwise \end{cases}$$

A digital watermarking is a technique that covertly embedded in a noise-tolerant signal such as an audio, video or image data [15]. It is typically used to identify ownership of the copyright of such signal. Digital watermarks may be used to verify the integrity or authenticity of the carrier signal or to show the identity of its owners. Traditional watermarks may be applied to visible media (images/videos) [10]. Digital watermarking has the signal which may be audio, pictures, videos, and text or 3D models. A signal can carry several different watermarks at the same time.

In this paper Discrete Cosine Transform (DCT) is used to divide the image into different parts of the same image (with respect to the image's visual quality). It is similar to the DFT[5] that transfers the image from the spatial domain to the frequency domain. To increase the security of the system the encrypted data is added to the image and also the secret key is also encrypted using Advanced Encryption Standard (AES). i.e.,(sender send these to the receiver a s watermark and finally the key is decrypted to view the encrypted data in the image).

The two cryptographic protocols that employ watermark operations as basic primitives to improve security are:

1. Dispute resolving schemes in order to assure the resistance against an important class of attacks.
2. To detect forgeries in image files or video stream by embedding a watermark carrying a cryptographic signature.

ADVANCED ENCRYPTION STANDARD

AES is an iterated symmetric block cipher, which means that:

- The multiple steps are repeated continuously to get the output.
- AES is a private key encryption algorithm.
- AES operates only on a fixed number of bytes.

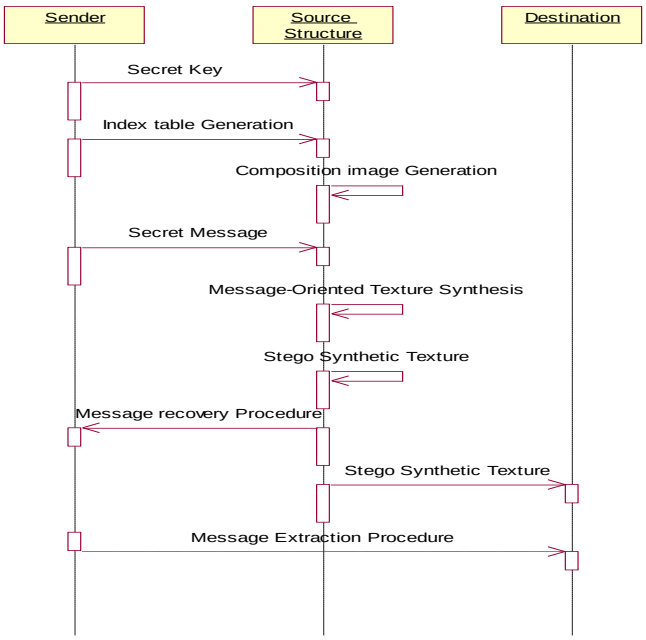
AES is reversible like any other algorithms. It is defined that almost the same steps are performed to complete both encryption and decryption in reverse order process. The AES algorithm operates on bytes, which makes it simpler to implement and get the desired output. This key is expanded into individual sub keys, a sub keys for each operation round. This process is called KEY EXPANSION [14]. As mentioned before AES is an iterated block cipher model. All that means is that the same operations are performed many times on a fixed number of bytes.

These operations can easily be broken down to the following functions:

ADD ROUND KEY
BYTE SUB
SHIFT ROW
MIX COLUMN

3. An iteration of the above steps is called a round. The amount of rounds of the algorithm depends on the size of the key.

ISSN: 0975-8585



RELATED WORKS

In this section, we evaluate the performance of the proposed image watermarking method by simulations, when comparing with the methods found in the following papers [12], [19] and [20]. Eight standard 512 × 512 8 -bit gray scale images *Bee*, *Elaine*, *Goldhill*, *Hill*, *Lena*, *Lighthouse*, *Truck*, and *Zelda* are used as host images. The peak signal-to-noise ratio (PSNR) index and the bit error rate (BER) index are used to measure perceptual quality and robustness, respectively. The performance indices PSNR and BER are calculated by averaging the results obtained from the eight images. Considering imperceptibility, if the larger PSNR value is obtained there will be better perceptual quality. It is mentioned in [25] that the PSNR value of 40dB indicates good perceptual quality. For example, the bottom two rows of Fig. 1 show the watermarked counterparts of the afore-mentioned eight images by our method, where PSNR = 40.32 dB. Clearly, there is no visual difference between the original images and their watermarked versions. With regard to robustness, a smaller BER value indicates better robustness, and vice versa.

Figure 1. Upper two rows: original images of *Bee*, *Elaine*, *Goldhill*, *Hill*, *Lena*, *Lighthouse*, *Truck*, and *Zelda*. Lower two rows: watermarked counterparts of all these images, where PSNR = 40.32 dB.

In the simulations, we choose N=4096 for all images. Two embedding rates: 12288 and 20480 watermark bits per image are considered, which correspond to K=3 and 5, respectively. As for T, in order to experimentally choose a suitable value, we embed 20480 watermark bits into each host image and then apply Gaussian noise addition to the watermarked images. Four different noise variances are considered, which are σ2=1, 4, 7 and 10, respectively. The simulation results about robustness and perceptual quality are shown. As expected, as T rises, BER decreases (or the resistance against Gaussian noise addition increases). Meanwhile, the perceptual quality, measured by PSNR, degrades with the escalation of T. To achieve satisfactory robustness while maintaining good perceptual quality, we choose T=15 for our method.

CONCLUSION

In this paper, we proposed a unique method for image watermarking in the DCT domain. Based on the rank-based watermark embedding and detection rules, the proposed watermarking method possesses some desirable features. Our method can use two DCT coefficients to embed one watermark bit. It is free of HSI. It can considerably tolerate the errors caused by attacks. The first feature leads to high embedding capacity. The second and third features make the proposed method robust against common attacks. The superior performance of the new method was analyzed theoretically in detail and demonstrated by simulation results.

REFERENCES

[1] Xia, C. Boncelet, and G. Arce, “A Multiresolution Watermark for Digital Images,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551

[2] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[3] B. Chen and G. W. Wornell, ``Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,'' *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423_1443, May 2001.

[4] S. Xiang, H. J. Kim, and J. Huang, ``Invariant image watermarking based on statistical features in the low-frequency domain,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777_790, Jun. 2008.

[5] Yuan Y., Huang D., Liu D., “An Integer Wavelet Based Multiple Logo- watermarking Scheme”, In IEEE, Vol-2, pp. 175-179, 2006.

[6] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, ``Digital watermarking robust to geometric distortions,'' *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2140_2150, Dec. 2005.

[7] S.H. Wang and Y.-P. Lin, ``Wavelet tree quantization for copyright protection watermarking,'' *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 154_165, Feb. 2004.

[8] Q. Cheng, ``Generalized embedding of multiplicative watermarks,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 978_988, Jul. 2009.

[9] M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama, and M. J. Medley, ``Extracting spread-spectrum hidden data from digital media,'' *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1201_1210, Jul. 2013.

[10] Wu, X., Hu, J., Gu, Z. and Huang, J “A secure semi fragile watermarking for image authentication based on integer wavelet transform with parameters” Conferences in Research and Practice in Information Technology Series; Vol. 108, 2005.

[11] M. Shensa, “The discrete wavelet transform: Wedding the a trous and mallat algorithms,” IEEE Transactions on Signal Processing, vol. 40, no. 10, pp. 2464–2482, 1992.

[12] B. Ankayarkanni, A. Ezhil Sam Leni, “A technique for classification of high resolution satellite image using object-based segmentation”, Journal of theoretical and applied information technology, vol.68, No.2, pp.275-286.

[13] T. Zong Y. Xiang I. Natgunanathan S. Guo W. Zhou G. Beliakov "Robust histogram shape-based method for image watermarking" IEEE Trans. Circuits Syst. Video Technol. vol. 25 no. 5 pp. 717-729 May 2015.

[14] M. Alghoniemy A. H. Tewfik "Geometric invariance in image watermarking" IEEE Trans. Image Process. vol. 13 no. 2 pp. 145-153 Feb. 2004.

[15] J. S. Seo C. D. Yoo "Image watermarking based on invariant regions of scale-space representation" IEEE Trans. Signal Process. vol. 54 no. 4 pp. 1537-1549 Apr. 2006.

[16] X. Gao C. Deng X. Li D. Tao "Geometric distortion insensitive image watermarking in affine covariant regions" IEEE Trans. Syst. Man Cybern. C vol. 40 no. 3 pp. 278-286 May 2010.
[17] I. J. Cox J. Kilian F. T. Leighton T. Shamoon "Secure spread spectrum watermarking for multimedia" IEEE Trans. Image Process. vol. 6 no. 12 pp. 1673-1687 Dec. 1997.
[18] J. Cannons P. Moulin "Design and statistical analysis of a hash-aided image watermarking system" IEEE Trans. Image Process. vol. 13 no. 10 pp. 1393-1408 Oct. 2004.
[19] H. S. Malvar D. A. F. Florencio "Improved spread spectrum: A new modulation technique for robust watermarking" IEEE Trans. Signal Process. vol. 51 no. 4 pp. 898-905 Apr. 2003.
[20] A. Valizadeh Z. J. Wang "Correlation-and-bit-aware spread spectrum embedding for data hiding" IEEE Trans. Inf. Forensics Security vol. 6 no. 2 pp. 267-282 Jun. 2011.