www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13678-13680

Watermarking For Digital Content- A SURVEY

I.Kalaivani[1], R.R.Bhavani[2]

[1]Assistant Professor
Dr.Sivanthi Aditanar College of Engineering
kalai15_1985@yahoomail.com

[2] Assistant Professor
Dr.Sivanthi Aditanar College of Engineering
aparnabhavani2003@gmail.com

Abstract: ***In the digital world, digital media is having a great impact and protection on such digital content is becoming necessary nowadays. Various image file formats are available for digital media. The digital content is often encrypted for security purpose. The encryption will change the content into unreadable format. Then the digital content can also be watermarked for tamper detection or for copyright protection. Encryption is often used but once it is decrypted it is not protected. So watermark is another level of security for digital content. Watermark remains also after decryption to identify owner of the digital content. This paper provides a survey on various ways to provide copyright protection for media content***.

Keywords*:* Digital watermarking, Spread Spectrum, Rational Dither Modulation.

1. Introduction

The success of the Internet provides a way to transmit the digital content in an effortless way. Encryption provides security and Digital watermarking data provides authentication to the digital content. In Information hiding, this became an important study area. Encryption changes the information to a format which is unreadable except intended receiver. Watermark is the secret message which is hidden in the cover image. It may be visible or invisible. This is used for copyright protection by hiding the ownership information in the digital image. Here, the ownership information is considered as the watermark. Watermark can be a simple text, number, company logo or an image. A good watermarking technique should be employed for embedding a strong watermark. Watermark can be affected by various attacks. Some common attacks are cropping, rotation, salt & pepper noise etc. The effect of such attacks can be reduced by using efficient watermarking techniques.

If the message is decrypted by the unintended users then this will no longer protected. So watermark is used to protect the data also after the decryption process. The quality of watermarking techniques is determined by the following parameters: robustness, imperceptibility, payload and security. Robustness means the watermark should be strong so that it cannot be destroyed or modified by any attacks. Imperceptibility refers to the host image quality. It should not be degraded because of watermark insertion. Payload is the total number of bits embedded in the host image. Nowadays watermarking is used mainly for the purpose of tamper detection, copyright or ownership declaration. The watermark is embedded into the image and later the information which is embedded should be extracted to identify the owner of the digital content. So it has two modules: watermark embedding and watermark extraction.

2. Existing Techniques for providing watermark

This section presents the working of various techniques for securing digital content.

2.1 Least Significant Bit (LSB)[1]

This is the simplest invisible watermarking technique.

Input: Cover Image ‘I’, information bits ‘b’

Output: Watermarked Image ‘W’

Method

- Convert RGB to gray image.
- Take the watermark image and perform shift operation the MSB of watermark shifts to LSB.
- Add this shifted watermark bits to cover image to generate the watermarked image.

Advantage

- It is simple and easy to implement.
- Degradation is less.

Disadvantage

- It is not robust against any attacks

2.2 DWT and DCT based Watermarking [2]

DWT is used for its improved secrecy and robustness.

Input: Cover Image ‘I’, Watermark image ‘b’

Output: Watermarked Image ‘W’

Method

- Perform DWT and divide the image into different subbands.
- Choose the highest level for embedding watermark.
- Choose a threshold value for that block.
- Perform DCT on watermark.
- Embed the watermark into the chosen block.
- Perform IDWT to get watermarked image.

Advantage

DOI:10.18535/ijecs/v4i8.10

Security and robustness is improved because of the chosen block for watermark embedding.

Disadvantage

Image quality is not considered.

2.3. Spread Spectrum Watermarking [3]

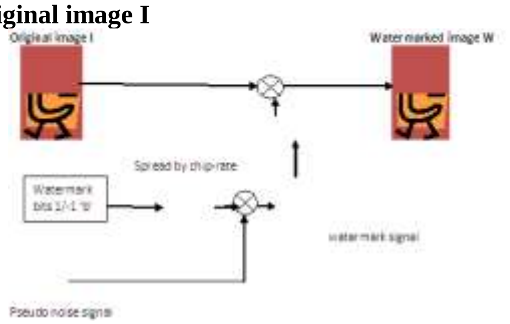
Input: Image ‘I’, information bits ‘b’

Output: Watermarked Image ‘W’

Method:

- To generate a spread sequence, spread the watermark bits using chip-rate.
- Modulate the spread sequence by pseudo noise sequence.
- Watermark bits are inserted into the input image to generate the watermarked image.

Original image I



Then the watermark signal can be fed to the watermark detector to detect inserted watermark. The embedded bits are extracted and it is demodulated by pseudo noise signal to get the watermark bits.

Advantage:

- It is more robust against noise attack.
- It also keeps the image quality as well.

Disadvantage

- Vulnerable to scaling attack

2.4. Buyer-seller watermarking protocol [4]

Input: Image ‘I’, information bits ‘b’

Output: Watermarked Image ‘W’

Players: Seller, Buyer, Certified authority (CA), trusted party

Method:

3 sub-protocols

- Watermark generation protocol
- Watermark insertion protocol
- Copyright violation detection protocol

Watermark generation protocol

- Buyer sends his identity and public key and request for a watermark.
- The Certified authority generates a watermark randomly and sends to buyer along with public key and signature.

Watermark insertion protocol

- Buyer sends to seller the encrypted watermark along with signature.
- Seller generates a secret watermark and insert into the image to get watermarked image which buyer wants to purchase.
- Seller permutes the encrypted watermark and inserted as the second watermark.
- Buyer decrypts the content got from seller.

Copyright violator identification protocol

Buyer can determine the copyright violator along with CA and trusted party.

Advantage

- The seller cannot create copy of original because they don’t know what watermark copy the customer receives.
- If unauthorized copy is found the seller can able to know the buyer from the inserted watermark.

Disadvantage

- Some overhead occurs because of the communication between buyer and seller.
- It is efficient if it works along with other cryptographic techniques.

2.5 Joint watermarking protocol based on CRT (Chinese Remainder Theorem) [8]

This joint watermarking protocol will overcome the traditional two-party case because this will not work for multi level content distribution. Here the watermark is jointly generated by all the parties involved.

Players: Owner, Number of distributers, Consumer.

- The watermark information is individually generated by the party using their own public key and digital signature.
- All the parties then jointly generate watermark information based on the prime numbers assigned to them.
- For joint watermarking following steps are followed
  - Owner sends the license to the server.
  - Server examines the license and extracts the public key and generates a random session key.
  - Owner decrypts session key and generate a unique watermark signal and embed into the content.
- Watermark detection
  - Owner checks for the watermark if it is present sent to judge.
  - Judge also checks for watermark.
  - Judge get the watermark information from server and compute the watermark signal and checks for the presence.
  - Judge also checks whether the watermark is a valid one.

Advantage

- DRM architecture involves multiple parties in distribution of digital content. So this suits well more than two-party scheme.
- The size of watermark is independent of number of distributors.

Disadvantage

- Computationally inefficient.

2.6 Partial Encryption and Watermarking. [5]

Partial Encryption is useful for watermark and encrypts the digital content with less degradation.

Consider wavelet codec:

- In DWT the image is divided into several sub bands.
- The sub bands in the lowest level contain more number of details and should be encrypted fully because a small modification will lead to degradation.
- Middle level sub bands can be both encrypted and watermarked.
- The high level sub bands are sign encrypted.

Advantage

- It is robust against signal processing operations like compression, addition of noise.

Disadvantage

- Security and robustness should be enhanced.

2.7 Rational dither modulation [7]

Rational Dither Modulation (RDM) is based on Quantization Index Modulation (QIM) which is robust against scaling attack because of dynamically modifying the step size of the quantizer based on the data available.

Input: Image ‘I’, information bits ‘b’

Output: Watermarked Image ‘W’

Method

It modifies a signal in to watermark one. For each future element it computes a function based on the past k watermarked symbols. So it is clear that watermark is done based on the preceding elements. In the decoding side the reverse process is done to get the watermark which is embedded during encoding step.

Advantage

- Invariant to volumetric scaling.

Disadvantage

- Not robust against filtering attack.

2.8 Scalar-Costa watermarking technique [6]

To provide ownership identity to the digital content this technique used and it is robust against noise and amplitude scaling attack. This needs usage of structured codebook at sender and receiver side to detect watermark. But this would not work in practical if the codebook is too large. So the codebook is replaced by the use of quantizer.

Input: Image ‘I’, information bits ‘b’

Output: Watermarked Image ‘W’

Method

This will encode the message by using the following three steps.

- Transform the message to binary vector elements.
- Encode the vector elements using binary error correcting codes.
- Encoded elements are transformed to watermark. Then at the receiver side it is demodulated to get the data.

Advantage

- Better information carrying capacity than SS and RDM,

Disadvantage

- Not robust against filtering attack.

The above presented are some of the techniques for watermarking. LSB technique is most simple to implement but it resists any attacks. If we need to create a watermark which is robust against attacks then prefer other attack resistant techniques like spread spectrum, scalar-Costa etc. These techniques overcome the disadvantage of LSB and DWT watermarking. Such robust techniques can be used to generate a watermarked object where the watermark is stronger to provide copyright protection. Like DRM architecture, where we want to distribute the content through many distributors we use joint watermarking protocol.

6. CONCLUSION

This paper has presented a survey on the providing watermarking for digital contents. This survey gives a brief introduction about watermarking, security of multimedia. Several watermarking techniques are explored to make the digital media secure. More research works have to be carried out based on encryption and watermarking to give high level of security.

References

[1] Image Watermarking Using LSB (Least Significant Bit) Gurpreet Kaur Kamaljeet Kaur International Journal of Advanced Research in Computer Science and Software Engineering

[2] A Digital Watermarking Algorithm Based On DCT and DWT Mei Jiansheng, Li Sukang and Tan Xiaomeiin International Symposium on Web Information Systems and Applications (WISA’09) *Nanchang, P. R. China, May 22-24, 2009, pp. 104-107*

[3]A.Subramanian,S.Emmanuel, and M. Kankanhalli, “Compressed encrypted domain JPEG2000 image watermarking,” in *Proc. IEEE Int. Conf. Multimedia and Expo*, 2010, pp. 1315–1320.

[4] M. Deng, T. Bianchi, A. Piva, and B. Preneel, “An efficient buyer-seller watermarking protocol based on composite signal representation,” in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[5] S. Lian, Z. Liu, R. Zhen, and H. Wang, “Commutative watermarking and encryption for media data,” *Opt. Eng.*, vol. 45, pp. 1–3, 2006.

[6] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, “Scalar Costa scheme for information embedding,” *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1003–1019, Apr. 2003.

[7] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, “Rational dither modulation: A high-rate data-hiding method invariant to gain attacks,” *IEEE Trans. Signal Process.*, vol. 53, no. 10, pt. 2, pp. 3960–3975, Oct. 2005.

[8] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, “Joint watermarking scheme for multiparty multilevel DRM architecture,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 758–767, Dec. 2009.