Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444
Volume 5, Issue 3, March-2018

A Review on Digital Watermarking and Its Issues

Parameshwaran[1], Marrynal S Eastaff[2]

[1]*PG Scholar, PG Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore*
[2]*Asst. Professor, PG Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore*

Abstract — ***Watermark is nothing but the data embedding and information hiding. we can simply say that digital watermarking is a pattern of bits inserted into a digital image, audio or video file which helps to identify the copyright information i.e. author, rights etc. In another way it is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced of digital content. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content.***

Keywords- Digital Watermarking; Copyright protection; Singular value decomposition; Watermark embedding procedure; Watermark extracting procedure .

I. INTRODUCTION

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song,video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, and it is merely used as a cover to hide its existence [13]. Watermarking can be considered as a special method of steganography where one message is embedded in another and the two messages are related to each other. An entity called watermark key used for embedding and detecting watermark signal. It can be categorized as visible or invisible. Example of visible watermarking superimposed on the corner of television channel. On the other hand, invisible watermark is hidden in the object, which can be detected by an authorized person.

II. CHARACTERISTICS OF DIGITAL WATERMARKING

Digital Watermarking has the following characteristics

2.1 Invisibility: an embedded watermark is not visible.

2.2 Robustness: piracy attack or image processing should not affect the embedded watermark.

2.3 Readability: A watermark should convey as much information as possible. A watermark should be statistically undetectable.

2.4 Security: A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. The owner of the intellectual property image is the only one who holds the private secret keys.

III. CLASSIFICATION OF DIGITAL WATERMARKING

The watermarking is classified in following ways

3.1 Robust & Fragile Watermarking

3.2 Visible & Invisible Watermarking

3.3 Public & Private Watermarking

3.1 Robust & Fragile watermarking-

If there is any modification in original data then there is no change in watermark whereas fragile watermarking means if there is any change or original data the watermark will change.

3.2 Visible & Invisible Watermarking-

Visible Watermarking is visual to human eye whereas Invisible Watermarking is invisible to human eye.

3.3 Public& Private Watermarking-

Public watermark does not require the original data to recover the watermark information but the private watermark requires the original data to recover the watermark all information.

IV. WATERMARKING ISSUES

The important issues that arise in the study of digital watermarking techniques are:

4.1 Capacity: what is the optimum amount of data that can be embedded in a given signal?

4.2 What is the optimum way to embed and then later extract this information?

4.3 Robustness: How do we embed and retrieve data such that it would survive malicious or accidental attempts at removal?

4.4 Transparency: How do we embed data such that it does not perceptually degrade the underlying content?

4.5 Security: How do we determine the information embedded has not been tampered, forged or even removed it?

Indeed, these questions have been the focus of intense study in the past few years and some remarkable progress has already been made. Perhaps a key reason the digital watermarking is inherently a multi-disciplinary topic that builds on developments in diverse subjects. The areas that contribute to the digital watermarking include are following:

4.6 Information and Communication Theory

4.7 Decision and Detection Theory

4.8 Signal Processing

4.9 Cryptography and Cryptographic Protocols

Each of these areas deals with a particular aspect of the digital watermarking problem. Generally, information and communication theoretic methods deal with the data embedding side of the problem. For example, information theoretic methods are useful in the computation of the amount of data that can be embedded in a given signal subject to various constraints such as peak power of the embedded data or the embedding induced distortion. The host signal can be treated as a communication channel and various operations such as compression/decompression, filtering etc. can be treated as noise.

Decision theory is used to analyze data-embedding procedures from the receiver (decoder) side. Given a data-embedding procedure how do we extract the hidden data from the host signal which may have been subjected to intentional or unintentional attacks? The data extraction procedure must be able to guarantee certain amount of reliability. What are the chances that the extracted data is indeed the original embedded data? Even if the data-embedding algorithm is not intelligent or sophisticated, a good data extraction algorithm can offset this effect. In watermarking applications where the embedded data is used for copyright protection, decision theory is used to detect the presence of embedded data. In applications like media bridging, detection theoretic methods are needed to extract the embedded information. Therefore, decision theory plays a very important role in the context of digital watermarking for data extraction and detection. In fact, it is shown that in the case of using invisible watermarks for resolving rightful ownership, uniqueness problems arise due to the data detection process irrespective of the data embedding process. Therefore, there is a real and immediate need to develop reliable, efficient, and robust detectors for digital watermarking applications.

A variety of signal processing algorithms can be and have been used for digital watermarking. Such algorithms are based on aspects of the human visual system, properties of signal transforms (e.g., Fourier and discrete cosine transform (DCT)), noise characteristics, properties of various signal processing attacks etc. Depending on the nature of the application and the context these methods can be implemented at the encoder, at the decoder, or both. The user has the flexibility to mix and match from different techniques depending on the algorithmic and computational constraints. Although issues such as visual quality, robustness, and real-time constraints can be accommodated, it is still not clear if all the desirable properties for digital watermarking discussed earlier can be achieved by any single algorithm. In most

cases these properties have an inherent trade-off. Therefore, developing signal processing methods to strike an optimal balance between the competing properties of a digital watermarking algorithm is necessary.

Cryptographic issues lie at the core of many applications of information hiding but have unfortunately seen little attention. Perhaps this is due to the fact that most work in digital watermarking has been done in the signal processing and communications community whereas cryptographers have focused more on issues like secret communication (covert channels, subliminal channels), and collusion resistant fingerprinting. It is often assumed that simply using appropriate cryptographic primitives like encryption, time-stamps, digital signatures, hash functions, etc. would result in secure information hiding applications. We believe this is far from the truth. In fact, we believe that the design of secure digital watermarking techniques requires an intricate blend of cryptography along with information theory and signal processing.

V. CONCLUSION

The digital watermarking, allows inserting and reliably detecting multiple watermarks sequentially embedded into a digital image, as it is required by challenging Digital Right Management applications such as confidential data tracing and shared property handling. One key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. Another key problem is the development of semi-fragile authentication techniques. The solution to this problem will require application of known results and development of new results in the fields of information and coding theory, adaptive signal processing, game theory, statistical decision theory, and cryptography. Digital watermarking can be utilized for authentication of data, copyright protection and communication process. It provides a consistent performance on different original image and watermarked image in all the experiments.

REFERENCES

[1] Anjali R.Mundhe , Sneha M.Narhare, Prema B.Saudagar, Prof.D.V.Birada, "Digital Watermarking to Insert Multiple Watermarks Sequentially", International Journal Of Engineering Sciences & Research Technology, [Mundhe, 3(3): March, 2014].

[2] Manjit Thapa,Dr. Sandeep Kumar Sood,A.P Meenakshi Sharma,"Digital Image Watermarking Technique Based on Different Attacks",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011

[3] M. Barni and B. Bovid, "Digital Watermarking for Copyright Protection: A Communication Perspective", IEEE Communication Magazine, vol. 39, no. 8, pp. 90-91, 2001.

[4] A. Kumar and V. Santhi, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 12, no. 14, pp.31-36, 2010.

[5] F. Petitcolas, R. Anderson and M. Kuhn, "Attacks on Copyright Marking Systems in Information Hiding", LNCS, Berlin, vol. 1524, pp. 218-238, 1998.

[6] C. C. Chang and P. Tsai, "SVD-based Digital Image Watermarking Scheme", Pattern Recognition Letters, vol. 26, pp. 1577-1586, 2005.

[7] T. V. Nguyen and J. C. Patra, "A Simple ICA based Digital Image Watermarking Scheme", Digital Signal Processing, vol. 18, pp. 762-776, 2007.

[8] I. J. Cox and J. P. Linnartz, "Some General Methods for Tampering With Watermark", IEEE Journal on Selected Areas in Communications, vol. 16, pp. 587-593, 2010.

[9] Z. Bojkovic and D. Milovanovic, "Multimedia Contents Security :Watermarking Diversity and Secure Protocols", 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, vol. 1, no. 3, pp. 377-383, 2003.

[10] S.J. Lee, S. H. Jung, "A Survey of Watermarking Techniques Applied to Multimedia", IEEE Transactions on Industrial Electronics, vol. 12 pp. 272-277, 2001.

[11] Y. Trank and W. Frank," Robust Image Watermarking in The Spatial Domain", Signal Processing, vol. 13, no 14, pp. 385-403, 1997.

[12] E. Koch and J. Zhao, "Robust Labels into Images for Copyright Protection", International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, pp. 1064-1087, 1985.

[13] Raj Jain, Aditya Balooni, Harshit Jain , "DIGITAL WATERMARKING" , International Journal of Innovations & Advancement in Computer Science , IJIACS ISSN 2347 – 8616 Volume 4, Special Issue March 2015