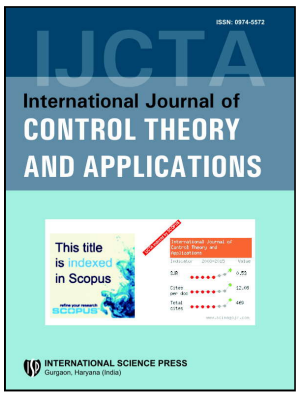

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 18 • 2017

Digital Watermarking Approaches and its Applications: A Review

Hemani1 and H.L. Mandoria2

[1] *PG Student,Department of Information Technology, G.B.P.U.A&T, Pantnagar, India*
[2] *Professor, Department of Information Technology, G.B.P.U.A&T, Pantnagar, India*

Abstract: This paper gives the meticulous study of Digital Watermarking approaches reported by various investigators. Some watermarking techniques have the steganography features of not being perceivable by the human eye. Watermarking is not new nor obsolete, but this method is always the most talked about. Data security is always the prime concern for everyone. This paper focuses on watermarking processes, watermarking types, properties, different attacks on watermarks, application of watermarking, advantages and as well as disadvantages.

Keywords: Watermarking, Fragile, Perceptual, Bit-stream

1. INTRODUCTION

Digital watermarking is solitary such technology that has been made to protect digital images from illicit manipulations[7].The rapid growth of the internet, results in creation and delivery of content in digital form. A need for developing technology that will help to provide security as well as authenticity. To prevent the data from being misled, Digital watermarking techniques are very useful in which a secret image called as watermarks which can be a logo or label is embedded into multimedia data impalpable(not easily grasped by the mind) which would be then used for various applications.

The paper is organized as follows sections:

- Overview of digital watermarking
- Advantages and Disadvantages of digital watermarking
- Types of watermarking
- Properties of watermarking
- Attacks on watermark
- Application of watermarking
- Conclusion

2. GENERAL INTRODUCTION OF WATERMARKING

Watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to a digital image, audio, video, and documents. Image Watermarking is the technique of embedding of owner copyright identification with the host image. At first, it is used in paper mills as a paper mark of the company[8]. Nowadays the term "Information Hiding" relates to watermarking.

2.1. Watermarking Process

The process Watermarking is basically bifurcated into two major parts:

1. Embedding of a watermark into the host image.
2. Extraction of a watermark from the image.

2.2. Embedding Process

In embedding process, Original image and watermark get combined with the help of embedding process afterward, we get a watermarked image.

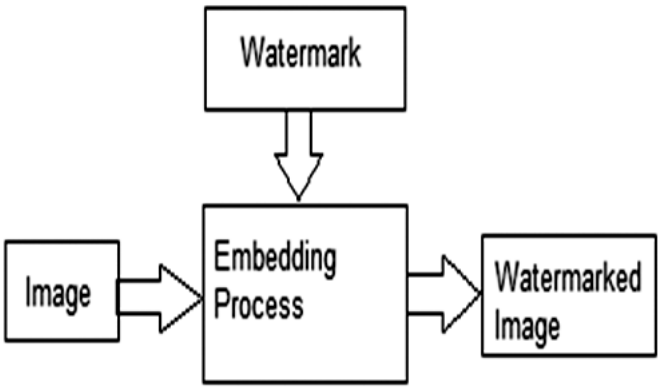

Figure 1: Digital Watermarking Embedding Process

2.3. Extraction Process

In extraction process, we used to get original image and watermark from the watermarked image i.e. the reverse of the embedding process.

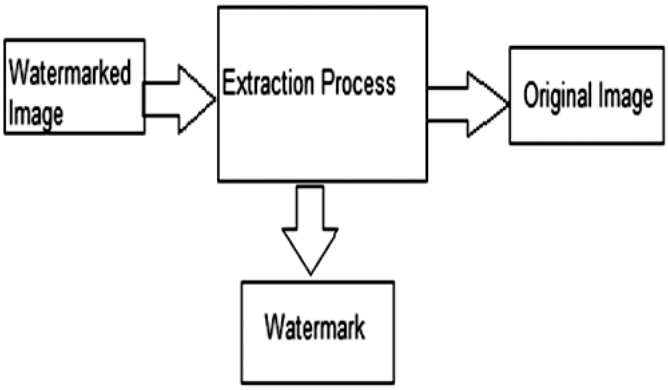

Figure 2: Digital Watermarking Extraction Process

Advantages of Digital Watermarking

- The visual distortion should be less, because on an average while embedding the checksum half the number of pixels gets changed.
- Multiple watermarks can be their as long as they don't overlap.
- Any modification to the checksum causes the failure of the verification procedure. We can say that they are extremely fragile.
- They are extremely fast and simple. Disadvantages of Digital Watermarking
- Some section can be easily replaced by another section of equal size by the forger.
- The whole watermark can be easily removed, by removing the LSB plane. Can't survive lossy compression.
- Another possible threat(Collusion attack) to digital watermarking schemes arises when the same data is watermarked multiple time and the distributed.

3. TYPES OF WATERMARKING

3.1. Visible watermark

The term logos and the concept of logos are associated with the visible watermarks. These watermarks are applicable to images only. These logos are transparent in spite of the fact that they are studded into the image. These type of watermarks cannot be removed by cropping the center part of the image. Further, such watermarks are protected against attacks such as statistical analysis[1].

3.2. Invisible watermark

These watermarks are not very easy to see with the naked eyes, they are hidden in the content. We can detect it using an appropriate watermark extraction and detection algorithm. Such watermarks are used for content or author authentication and for detecting unauthorized copier[2].

3.3. Public watermark

These watermarks are in readable form or can be retrieved and then misused by anyone using the specialized algorithm. So we can say that public watermarks are not secure enough. However, they are very much useful for carrying IPR information or good alternatives to labels.

3.4. Fragile watermark

Another name of Fragile watermark is tamper-proof watermarks. Someone can easily destroy these watermarks by data manipulation.

3.5. Private watermark

Private watermarks are also known as secure watermarks. You required a secret key, if you want to read or retrieve such watermark.

3.6. Perceptual watermarks

These watermarks provide high-quality content and also known as a transparent watermark. A perceptual watermark exploits the aspects of a human sensory system to provide invisible yet robust watermark.

3.7. Bit-stream watermark

The term is sometimes used for watermarking of compressed data such as video.

4. PROPERTIES OF DIGITAL WATERMARKING

4.1. Robustness

The watermark should be robust, as watermarks could be removed by performing image processing operations and it should be unaffected against a variety of attacks.

4.2. Effectiveness

The watermark should be effective that means it should be a detective, this is the foremost property of watermark.

4.3. Capacity

This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermarking should be able to carry enough information to represent the uniqueness of the image.[7]

4.4. Transparency

The prime concern in embedded the watermark in the image is that it doesn't affect the quality of the original image.

4.5. Host signal Quality

In the watermarking process, the watermark is embedded in a host signal, this may affect the host signal. So, the overall watermarking process must show minimal changes to the host signal and it should be unnoticeable when a watermark is invisible.

4.6. Watermark Size

The size of the watermark should be minimum because it will increase the size of data to be transmitted.

5. ATTACKS ON WATERMARKING

5.1. Geometric Attack

Any exercise that is done on any image that affects the geometry of an image is considered as Geometric Attack such as translation, rotation, flipping, cropping. An example of these type of attack are cropping attack from the side and bottom of the image and cropping attack is overcome by DWT.

5.2. Removal Attack

The prime intention of removal attack is to remove the watermark from the watermarked image. These attacks include noise, blur, filter, sharpen attacks.

5.3. Security Attack

Under this attack, attacker tries to modify the watermark after he get the details about the watermark algorithm

5.4. Protocol Attack

An example of protocol attack is copy attack, where the attacker just copies the content of watermark without the knowing the secret key. These attacks are very difficult to detect.

5.5. Active Attack

The attacker tries to remove the watermark continuously and make it subtle so that no one notices it. These type of attack plays a vital role in fingerprinting, copy control or copyright protection.

5.6. Passive Attack

The attackers tries to monitor and scan the system for open port. The main objective of the attacker is to gain the information that is being transmitted in the message.

5.7. Forgery Attack

Insertion, deletion and substitution of any object is the result of forgery attack.

5.8. Interference Attack

The attacker tries to add some noise to the watermarked object. Some of the well known examples of interference attack are quantization, compression, demodulation, averaging, denoising.

5.9. Cryptographic Attack

An attempt to break the security is commonly known as a cryptographic attack.

5.10. Collusion Attack

Under this attack, an attacker tries to use the several copies of the same data, containing a different watermark, to make a new copy without any watermark. Here the main motive of the attacker is same as for the active attacks but uses slightly different methodology.

5.11. Image Degradation

Under this attack, some part of the image get removed so its damage the robustness of the image. Some of the examples are row removal, column removal, partial cropping.

6. APPLICATION

Watermarking technologies is applied in every digital media whereas security and owner identification is needed[3].Some of the application are as follows

6.1. Owner identification

One of the foremost application of watermarking to which he developed is to identify the owner of any media. By some small exercise of attacker some paper watermark can be easily removed i.e. the digital watermark comes in picture. Digital media is the internal part of a watermark, it cannot be easily detected and removed.

6.2. Copy protection

Illegal copying is also prevented by watermarking with copy protect bit. This protection requires copying devices to be integral with the watermark detecting circuitry.[4]

6.3. Content Archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio, video[6].

6.4. Medical applications

Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster[11].

6.5. Fingerprinting

Fingerprints are the characteristic of an individual that is unique to the owner of the digital data and help it to distinguish from another unauthorized user. This provide a security to the digital data.

6.6. Data authentication

Authentication is a process that ensures and confirms a user's identity. Data should not be leaked to some third party, So for that purpose a sender embedded the digital watermark with the host data and it would be extracted at the receivers end and should be verified.

6.7. Broadcast monitoring

The number of television and radio channels has increased very drastically in some recent years and the amount of content being broadcast through these medium. The watermark plays a vital role in broadcast monitoring, as it supposed to be supervised whether the content should be broadcasted has really been broadcavery important for t copyright holders,sted or not. And it ishe content owners, distributors and broadcaster to know the real broadcast reality in this fast changing market.

6.8. Meta-data Insertion

Meta-data refers to the data of data. Images can be labelled with its content and can be used in search engine[6], Manufacturer of the appliances can give the details of the model in the appliances, ATM cards could store the details of an individual records.

6.9. Content filtering

The lean-back experience of watching television has radically changed over the last few years. People wished to watch television in their own time and space. The STB(set-top boxes) has become an interactive devices providing multiple services[9].

7. CONCLUSION

In this paper , we reviewed the digital watermarking. Digital watermarking technique is a very useful technique to transmit data over an insecure channel. In this paper, we are going to study the different types of watermarking, its properties, application , different attacks on the watermark and its advantages as well as disadvantages. This paper gives you the brief explanation about digital watermarking.

REFERENCES

[1] J.-K. Kamarainen, V. Kyrki, and H. K¨ alvi¨ ainen, "*Invariance properties of Gabor filter based features - overview and applications," IEEE Trans. on ImageProcessing, vol. 15, no. 5, pp. 1088–1099, 2006.*

[2] D.Gabor, "Theoryof communication," Journal of Institution of Electrical Engineers, vol. 93, pp. 429–457,1946.

[3] Mei Jiansheng, Li Sukang, "A DigitalWatermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[4] Lalit Kumar Saini at el, "A Survey of Digital Watermarking Techniques and its Applications" International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, 2014.

[5] Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", International Conference on Intelligent Computation Technology and Automation, 2010.

[6] Vinita Gupta, "A Review on Image Watermarking and its Techniques", International journal of advanced Research in Computer Science and Software Engineering, 2014.

[7] Cox,IJ,Miller,ML & Bloom,JA, Digital Watermarking,Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

[8] Http://cameo.mfa.org/wiki/Watermar k.

[9] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques,Applications and Attacks", International Journal of Engineering and Innovative Technology(IJEIT), Volume 2, Issue 9, 2013.

[10] Manjeet kaur, Ramneet Singh Chadha, "A Review on Various Techniques, Classification, Attacks and Applications of Digital Image Watermarking", International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[11] G.Coatrieux,L.Lecornu,Members,IEE E,Ch.Roux,Fellow,IEEE,B.Sankur,M ember,IEEE "A Review of Digital Image Watermarking in Health care".

[12] Rupali Narula, Meenakshi Chaudhary, "A Survey of Digital Image Watermarking Techniques",2016

[13] Palak Patel, Yask Patel, "Secure and Authentic DCT image steganography through DWT-SVD based Digital watermarking with RSA encryption", IEEE, 2015

[14] T. Vimala, *"Salt and Pepper Noise Reduction Using Mdbtum Filter With Fuzzy Based Refinement", IJMIE, Volume 2 Issue 5, 2012*

[15] Fang Li, "*Salt and Pepper Noise Removal by Adaptive Median Filter and Minimal Surface Inpainting",* Image and Signal Processing, 2009. CISP '09. 2nd International Congress on, *2009*

[16] J.-K. Kamarainen, V. Kyrki, and H. K ¨ alvi¨ ainen, *"Invariance properties of Gabor filter based features - overview and applications," IEEE Trans. on Image Processing, vol. 15, no. 5, pp. 1088– 1099, 2006.*

[17] T. Serre, L. Wolf, S. Bileschi, M. Riesenhuber, and T. Poggio, *"Object recognition with cortex-like mechanisms," IEEE Trans. on PAMI* vol. 29, no. 3, 2007.

[18] Alexander Sverdlov, "Secure DCT- SVD Domain Image Watermarking: Embedding Data in All Frequencies", Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003

[19] Anthony T.S.Ho et.al "A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform", *Springer,* 2011

[20] Mansouri, A., A. Mahmoudi Aznaveh, and F. Torkamani Azar "SVD-based digital image watermarking using complex wavelet transform." *Sadhana* 34, no. 3 (2009): 393-406.

[21] Singh, Surya Pratap, Paresh Rawat, and Sudhir Agrawal "A robust watermarking approach using DCT- DWT."*International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8* (2012).

[22] Al-Haj, Ali "Combined DWT-DCT digital image watermarking." *Journal of computer science* 3, no. 9 (2007): 740.

[23] Himanshu Sharma, Ashok Kumar, H.L.Mandoria "Study and Comparison Analysis of a Video Watermarking Scheme for Different Attacks."IJERMT,2015

[24] Poonam Singh, Binay Kumar Pandey, H.L.Mandoria "Performance Analysis of Image and Video Coding by Wavelet Transform using Region of Interest" IJERMT, 2015

[25] Ravish Kumar Dubey, H.L.Mandoria "Study of Different Transformation Algorithms in Digital Image Watermarking" IJCSEITR,2016

[26] Bhoomika Pandey, H.L.Mandoria "A Comprehensive Study on Text And Image Steganography" IJETTCS, 2016

[27] Manish Kumar, Rajesh Shyam Singh and H.L.Mandoria "Preventing Character Recognition Attacks on CAPTCHA:A Customizable CAPTCHA Approach" International Journal of Emerging Science & Technology,Volume- 2,Issue-7,2015

[28] Nutan Gussain,Ashok Kumar and H.L.Mandoria "Performance Analysis of Image and Audio Compression Technique Using Discrete Wavelet Transform", International Journal for Research in Management and Technology, Volume-4,Issue9,2015.

[29] Sanjay Singh Arya,Rajesh Shyam Singh and H.L.Mandoria "Image De- Noising using Wiener Filter Algorithm", International Journal of Research in Information Technology,Volume-3,Issue-9,2015

[30] Rashmi Agarwal [2015] "Block Based Digital Watermarking using Singular Value Decomposition on Color Images"