

Various Properties and Classification of DWM for Data Protection

Dr. Mohd Ashraf

Associate Professor, CSE

Maulana Azad National Urdu University, Hyderabad

Email: ashraf.saiffee@gmail.com

Abstract: The present world is digital world. These days, in each field there are enormous uses of digital contents. Information handled on internet and multimedia network system is in digital form. The replicating of digital content without quality loss isn't so troublesome. Because of this, there are more chances of replicating of such digital information. Thus, there is extraordinary need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the great solution for this issue. Digital watermarking is only the innovation where there is inserting of different information in digital content which we need to protect from illegal duplicating. This embedded information to secure the information is embedded as watermark. Past the copyright security, Digital watermarking is having some different applications as fingerprinting, proprietor recognizable proof and so forth. Digital water-marks are of various kinds as robust, fragile, visible and invisible.

Keywords: *Robustness, Replication, Watermarking etc.*

I. INTRODUCTION

Digital documents for example records made in digital media are having some points of interest like-

- Efficient data storage, duplication, control and transmission.
- Copying without loss.

Such digital documents comprise of pictures, sound clips and recordings and so on. Be that as it may, because of some delimits of digital documents, they become inefficient to utilize. These delimits are as per the following

- Illegal replicating
- Falsification (duplication)
- No copyright assurance
- No ownership recognizable proof

The enormous utilization of networked multimedia system has made the need of "Copyright Protection" for various digital medium as pictures, sound clips, recordings and so on. The expression "Copyright Protection" includes the validation of possession and distinguishing proof of illegal duplicates of digital media. In spite of the fact that digital media gives different proficient facilities like conveyance, multiplication and control of pictures, sound clips and video, they increment unlawful replicating of digital media.

The answer for this issue is to include the obvious or imperceptible structure to digital media which is to be shielded from copyright. These structures are known as "Digital Watermarks" and the way toward adding digital watermarks to digital media is known as "Digital Watermarking".

Digital watermarking is made by embedding a digital signal or pattern into digital content. Digital watermarking is only procedure of passing on information by vaguely inserting it into digital media. The reason for inserting the data relies on application and need of client of digital media. Digital watermarking gives the answer for troublesome issue of giving assurance to coordinator and customer of digital substance about their lawful rights. Copyright security for sight and sound data is only a brilliant key for multimedia industry. Digital watermarking is an innovation that opens another entryway for creators, makers, distributors and specialist organizations for assurance of their privileges and enthusiasm for sight and sound documents.

II. PROPERTIES AND CLASSIFICATION OF DWMs

Properties

For better activeness, watermark ought to be – perceptually undetectable inside host media, measurably imperceptible to unapproved removal, promptly separated by proprietor of image, robust to incidental and proposed signal contortion like filtering, compression, resampling, retouching, crapping e and so forth. For a digital watermark to be powerful for

6871

possession, it must be vigorous, recoverable from a report, ought to give the first data inserted dependably and furthermore expelled by approved clients.

All these significant properties of digital watermarks are depicted as-

1. Robustness=>The watermark ought to be powerful with the end goal that it must be hard to remove. The watermark ought to be robust to various assaults.

The robustness describes whether watermark can be reliably detected after performing some media operations.

2. Perceptual transparency=>This property depicts that whether watermark is visible or invisible to human sensor organ. Perceptible watermarks are noticeable to human while imperceptible are most certainly not. Imperceptible watermarks are with the end goal that content stays same in the wake of applying digital watermarking system.

3. Security=>Security property depicts that how simple to remove a watermark. This is by and large alluded to as "attack" on watermarking. Attack alludes to discovery or adjustment of watermark.

4. Complexity=>This is significant property which is to be considering continuously applications like video. Complexity property is worried about measure of exertion expected to extricate or recover the watermark from content.

5. Capacity=>Capacity property of digital watermarks alludes to measure of data that can be embedded inside the content. The significant point is that more information is

utilized in watermark, watermark will turn out to be less robust.

Notwithstanding these properties, watermarks are having some additional properties as unambiguity, alter opposition, inseparable from the works and ready to experience some change as works.

Classification

Digital watermarks are ordered by their applications. The watermarks are classified as perceptible watermarks and imperceptible watermarks, robust and fragile, public and private. This classification of watermarks is broadly described in following sections.

1. Perceptible watermarks and imperceptible watermarks

Perceptible watermarks are visible to human eye while imperceptible watermarks are invisible. The perceptible watermarks are valuable for essential application for example for explanation proprietorship or authorship. So therefore it ought to be unmistakable. Then again imperceptible watermarks are helpful for complex applications, for example, record recognizable proof in which substance being watermarked must show up in unaltered structure.

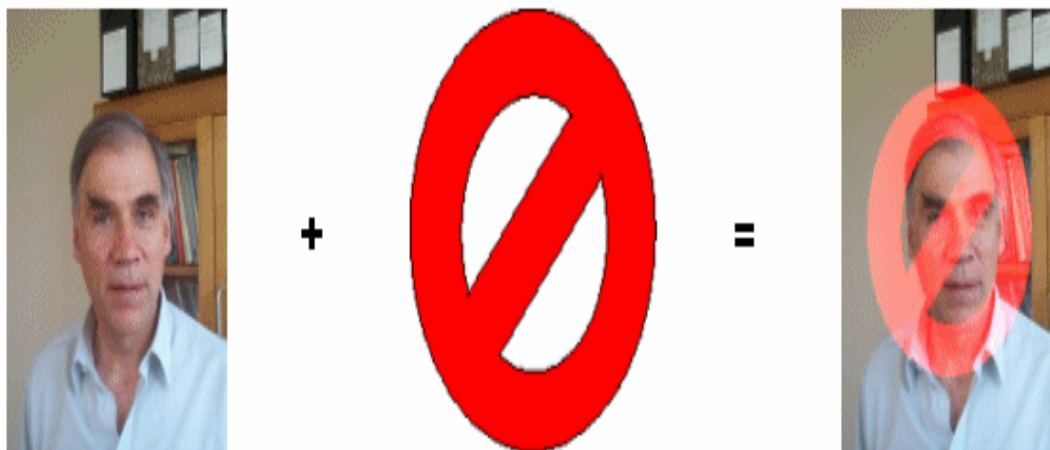


Fig. 1 Visible (Perceptible) watermark

2. Robust watermarks and fragile watermarks

Robust or fragile is only degree to which watermarks can withstand any alterations of any kinds caused because of the transmission or lousy compression. Perceptible watermarks are more robust in nature than imperceptible one. Yet, which means of this isn't imperceptible watermarks are fragile one.

Robust watermarks are those watermarks which are hard to remove from the object in which they are embedded. Fragile watermarks are those watermarks which can be effectively annihilated by any endeavor to mess with them. Fragile watermarks are destroyed by data manipulation.

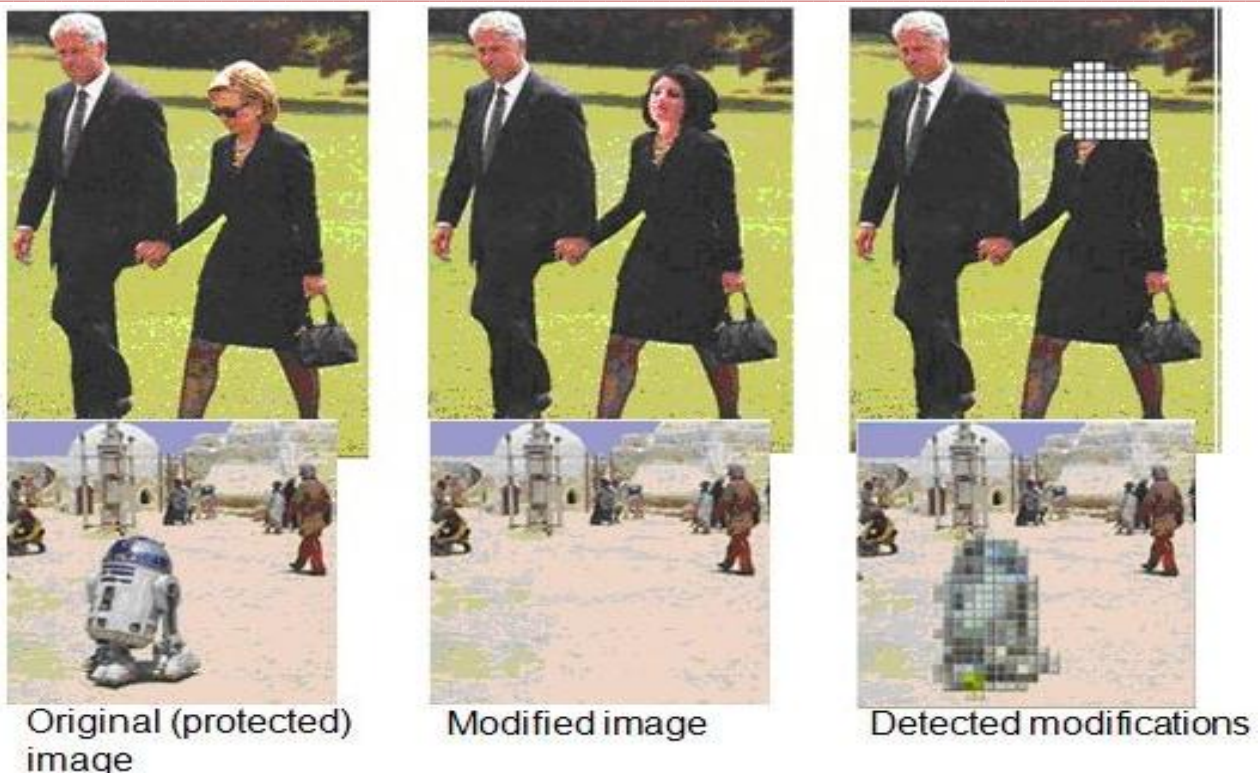


Fig. 2 Fragile watermarking for authentication

3. Private watermarks and public watermarks

Private watermarks requires at least original data to recover watermark information .Public watermarks requires neither original data nor embedded watermarks to recover watermark data. Private watermarks are otherwise called secure watermarks. To peruse or recover private watermark, it is important to have secret key. Open watermark can be peruse or recover by anybody utilizing particular algorithm. In this sense open watermarks are not verify. Open watermarks are valuable for conveying IPR data. They are great options in contrast to marks.

III. CONCLUSION

The huge need of networked multimedia system has made the need of "COPYRIGHT-PROTECTION". It is essential to secure intellectual properties of digital media. Web assuming a significant job of digital data transfer. Digital watermarking is the extraordinary arrangement of the issue of how. To ensure copyright Digital watermarking is the answer for the security of legitimate privileges of digital content proprietor and client.

These watermarks, be that as it may, are not great, and more should be possible to improve a watermark's power or exactness in recognition. Moreover, the topic of copyright encroachment stays a legitimate issue. Courts need to figure out which techniques might possibly be utilized. Until these

legitimate guidelines are set, the Internet keeps on being perilous for pictures.

Digital watermarking has been proposed as one approach to ensure such interests. Despite the fact that much research stays before watermarking frameworks become strong and generally accessible, there is a lot of guarantee that they will contribute altogether to the insurance of exclusive interests of electronic media. Different organizations have extends toward this path arrangements will before long be accessible. Notwithstanding mechanical advancements, promoting and business issues are critical and require top to bottom examination and key arranging. It is essential to set up the business to the utilization of advanced watermarks and all things considered, completely working to persuade them regarding the additional worth their items can pick up on the off chance that they utilize digital watermarking advances.

REFERENCES

- [1] Navneet Kumar Mandhani, "Watermarking Using Digital Sequences", MS thesis, Andhra University, August 2004.
- [2] Prabhishkek 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, March 2013.
- [3] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 0-7803-9094-6/05/\$20.00 ©2005 IEEE.

- [4] Ioannis Retsas, "A DCT – Based Image Watermarking Algorithm Robust to Cropping and Compression", MS Thesis, Naval Postgraduate School Monterey, California, March 2002.
- [5] B. Surekha, Dr. G. N. Swamy, "A Spatial Domain Public Image Watermarking ", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011