# DIGITAL WATERMARKING A TECHNOLOGY OVERVIEW

**Hebah H.O. Nasereddin**
Middle East University, P.O. Box: 144378, Code 11814, Amman-Jordan
Email: hebah66@hotmail.com

## ABSTRACT

The paper introduces the digital watermarking technology which is a data hiding technique that embeds a message into a multimedia work such as an image or text or other digital object. The proposed technique has several important applications; the majorly important is the digital copyrights protection. The digital watermarking system as any other data hiding technique has its own requirements that make the digital watermark strong as possible.
Technologies of digital watermarking are mainly classified depending on their domain to spatial domain watermarks, Watermarks belonging to frequency (transform) domain and wavelet domain watermarks. The digital watermarks suffer from different types of attacks that include either state-of-the-art watermarking attacks or watermark estimation attacks. The recovery from these attacks requires strong detection techniques; the digital watermark agent provides a professional solution for these attacks. The paper also mentions a new paradigm in digital watermarking that is 3d objects watermarking.

## 1. INTRODUCTION

Often Watermarks are marks that added to the paper during the paper manufacturing process .these marks identify the paper manufacturer. Historically the first watermarks were noticed in Italy during the 13th century.[1] an example of a watermark is shown in figure1. in the 18th century watermarks appeared in America and Europe they where used in money and as trade marks .the term watermark was used to clarify the effect of water on the paper .[2]
Digital watermarks are messages embedded in a multimedia work such as an image or text or other digital objects. [2]. Digital watermarking gains its popularity as a research topic during the 1990s [1, 2]. The speed evolution of digital objects, software programs and the simple communication and access techniques to these products make a necessary demand for the digital copy right protection, digital watermarking systems form a practical mean to protect the digital content [3].
In the digital watermarking systems the digital information which also called payload, do not affect the carrying object; it fights changes or manipulation in the carrier. [4]
Many Digital watermarking algorithms appeared during the last 20 years these algorithms use the carrier object properties to embed the desired watermark. [5]
The motivation for this paper is to investigate digital watermarking techniques, its requirements, types, applications and it's advantageous.

## 2. DIGITAL WATERMARKING SYSTEM

In digital watermarking system the watermark m is embedded into a multimedia object o producing the watermarked data M as in the following equation
M=E (m, o)
E resembles the embedding algorithm. The extraction process of the watermark applies the embedding algorithm reversely so the watermark can be extracted. [6]

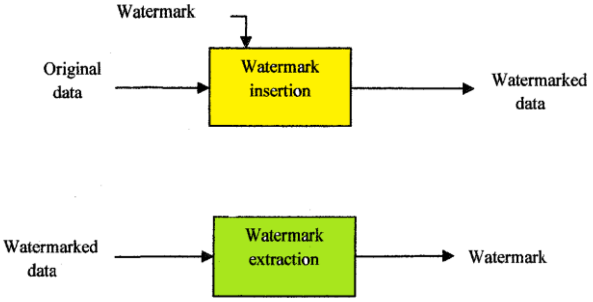

Figure1. Digital Watermarking System

Digital watermarking systems are designed depending on the following requirements: [7, 8]

- ❖ Robustness (resistance): the watermark should be able to resist different attacks and manipulation operations.
- ❖ Capacity: the amount of the digital data (payload) which can be embedded.
- ❖ Security: the watermarked data shouldn't affect the carrier object or work if it is being changed or extracted.
- ❖ Efficiency: the speed of extraction and placement of the digital watermark.
- ❖ Imperceptibility (undetectability): the watermark shouldn't affect the content of the carrying object if it is used.

A digital watermarking system consists of the digital mark (information to be embedded), embedding algorithm, and extraction algorithm. [9]

### 2.1 Watermarking classifications

Digital watermarking technology is classified using different criteria such as visibility, robustness, and domain [6]

- Classifications depending on visibility.
  1. Visible watermarking: A visible watermark is a mark put inside the carrying object and it is made clear to the user [6].
  2. Invisible watermarking: Invisible water mark is a mark added to the carrying object but cannot be seen and can be can be extracted using watermarking algorithms.[6]

- classifications depending on robustness[1]:
  1. Fragile watermark: fragile watermark cannot resist any attacks on the mark and it may be manipulated before reaching to the receiver.
  2. Semi-fragile watermark: A semi-fragile watermark can endure certain kind of attacking techniques on the watermark, at the same time it cannot resist other attacking techniques.
  3. Robust watermark: By presumption Robust watermarks resist all kinds of attacking techniques on the mark.

### 2.2 Watermarking techniques.

Water marking techniques are classified depending on the domain to the following: Spatial domain water marks, Watermarks belonging to frequency (transform) domain and wavelet domain watermarks. [1]

**1. Spatial domain water marks:**

The spatial domain is the normal image space, this mean any altering in any location in the image is reflected in the corresponding scene which the image is formed by its projection. Examples of spatial domain techniques:

- Least significant bit modification (LSB): LSB is the most familiar technique in hiding a watermark in an image it depends on modifications done to the least significant bits of certain pixels in the image. Some algorithms use a sequence of prime numbers instead of the LSB, or add a sequence of prime number to the LSB, other algorithms embeds check sum of the image data into the LSB. [9] LSB is classified as a spatial domain technique in which the watermark size is very smaller than the cover object, the watermark can be embedded repeatedly in certain places in the cover object, these marks maybe lost during the opponent attacks but part of the marks will resist the attacks [1].
- Information tagging: information tagging is a spatial domain technique in which the watermark is hidden depending on the properties of the cover object which is restricted to be an image .Carnoni [9] manipulates the brightness location in the image While Brassil et al. [9] suggests a watermark hiding technique only for images containing text. According to [9] both methods are easily defeated.

**2. Frequency domain:**

"The frequency domain is a space in which each image value at image (I) position F represents the amount that the intensity values in image I vary over a specific distance related to F" [12].The most common frequency domain is discrete cosine domain (DCT) . The DCT divides the image into different frequency groups; the watermark is hidden in the frequency groups that are in the middle .these groups are selected so that they are not visually important [1]. Frequency Spectrum-Based Methods are examples of frequency domain techniques presented in [9].

3. **Wavelet domain:**

Wavelets are 'Functions that provide succinct and accurate representations of time series and arrays of spatial data' [13], wavelets transforms are the components of the wavelet domain .these transforms make a powerful tool that help analyzing the original domain[14]. In this technique the water mark is embedded using discrete wavelet transform DWT which breaks up the image into three different resolutions, and for each part this process can be repeated to generate multiple-scale decompositions then the watermark is embedded in high resolution areas which adds strength and resistance to the watermark.

### 2.3 Privacy Principles for Digital Watermarking [10]

- Privacy by design: When a digital watermark is developed the privacy conditions must be considered in the designing phase.
- Avoid embedding independently useful identifying information directly in watermark: the watermark must not hold data that gives personal information and if it does for some exceptions it must not hold the same code repeatedly.
- Provide notice to end users: End users must be notified that their files including a digital watermark and what kind of data is hidden.
- Control access to reading capability: The companies that develop the watermarks should consider the availability of reading machines and techniques and control their usage to the end users.
- Respond appropriately when algorithms are compromised: If the watermark is compromised by a third party all users must be notified so if the water mark is forged or altered the users can take the right action.
- Provide security and access controls for back end databases: The back-end database must be protected and secured from any un authorized usage by the watermarking companies.
- Limit uses for secondary purposes: When the purpose of the watermark is achieved the watermark must not be used again for other purposes.
- Provide reasonable access and correction procedures for personally identifiable information: watermarks applications that implement individual data about the users must permit reasonable access by the users so they can correct any errors in their records.

### 2.4 Applications of digital watermarking [7, 8, 9]

Digital watermarking is used in several applications; the following is the most important applications.

1. Digital copyright protection.
2. Transaction tracing and fingerprinting.
3. Digital content management.
4. Copy control.
5. Digital content authentication and verification.
6. Broadcasting Synchronization System.
7. Forgery prevention.
8. Lyric sync services.

Digital Copyrights Protection [7, 8, 9]: Copyright protection is a technique used to embed the ownership rights in a multimedia work by its creators. This technique guarantees the owners rights in their works if these works were misused by other users.

Broadcast Monitoring: It’s a technique used by advertisers in television in order to make sure that their ads were broadcasted in the previously indicated time; watermarking techniques could be used to solve this problem by watermarking the ads. The advertisers use watermarks detectors to make sure that their ads were broadcasted at the indicated time.

Lyric Sync Service: Lyric sync service is a watermarking technique that embeds letters information such as the lyrics of a song in an audio file. When the audio file is played the watermarked information can be detected by the lyric sync service and broadcasted in a monitoring screen.

## 3. ATTACKS ON DIGITAL WATERMARKS [11]

Attacks on digital watermarks are classified to either state-of-the-art watermarking attacks or watermark estimation attacks.

### 3.1 State of the art watermarking attacks

This category of attacks includes four types of attacks that are removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

- Removal attacks: Removal attacks remove the watermark information completely from the watermarked data without affecting the security of the used algorithm in masking the information in the digital watermark This type of attacks includes' denoising, quantization (e.g., for compression), demodulation, and collusion attacks'. These attacks if it didn’t success in the removal of the watermark completely; it destroys the watermark.
- Geometric attacks: Geometric attacks is not interested in the removal of the watermark but rather that they distort the watermark detector that is embedded with the information .this detector could be used to reveil the contents of the digital water mark ,but this process is very expensive and very complex.
- Cryptographic attacks: This type attacks the security algorithm used to embed the watermark, by this the watermark can be easily extracted. An example of this type is the brute_force attack other example of this type is Oracle attack which is used to generate a non watermarked signal.
- 6.1.4 Protocol attacks: The main goal of Protocol attacks is to harm the watermark application entirely. An attack based on invertible watermarking is An example of this type. In this case the attacker extracts the watermark from the watermarked data claiming the ownership of this watermarked data.

### 3.2 Estimation based attacks

These attacks require a well knowledge in watermarking technology and the characteristics of the data. The main concept of these attacks is that the original data or the watermark can be estimated by the attacker because the attacker has previous knowledge of the watermark signal statistics. The estimation based attacks can be classified into removal attacks, protocol attacks, or de-synchronization attacks.

- Estimate of the original data: The watermark is an addition to the original data; the attacker can design an extraction technique to get the un watermarked data. The extraction technique depends on both denoising and compression of the watermarked signals. The denoising and compression attacks are classified as removal attacks.
- Remodulation attacks: Demodulation attacks modifies the watermark by using an opposite technique of the embedding algorithm used with the original data, if an approximate estimation is made to the real watermark then the estimated watermark can be subtracted from the original watermarked data which may affect the original data quality.
- Copy attack: The estimated watermark can be used in a copy attack implementation. The attacker adds the estimated watermark to a target data claiming the ownership of the falsely watermarked data.
- Synchronization removal: The synchronization removal attack depends on detection of the synchronization mechanisms used with the original data then removing the synchronization and applying de-synchronization techniques. By this important characteristics of the original data is extracted, which make it easy to get the original data.

## 4. WATERMARK AGENCY [16]

The successful use of digital watermarking technology depends on using efficient detection techniques that detects watermarks in all types of digital objects. a digital watermark agent could be used to provide this service.

A digital watermark agency have a group of agent each of them get information and report to the agency .the agents go through networks to get the required information, then the agency collects all agents reports and analyzes to form its knowledge base.

The agency takes an action upon requests of its clients In order to protect their digital objects.

The major function of digital watermark agency is summarized in the following steps:

1. The agency prepares a package for each agent contains secret watermark keys, objective, action polices and termination condition.
2. Sending agents to their meant destination which as a specific host.
3. Getting information from all agents and analyzing their reports.
4. Guiding agents by providing them with update information.

The agent finishes its mission by taking the appropriate action that protects the specified digital object. After that it clones it self and travel to other host. The water agency scheme represents a useful mean that can be applied to gain digital copyright protection.

## 5. WATERMARKS IN 3D OBJECTS [17, 18]

The increase use of Virtual reality applications make it necessity to have protection mechanisms for these applications .digital watermarking proved its reliability as a protection technique.

Recently many algorithms proposed hiding watermarks in the 3D mesh of the 3D object. The main goal of these algorithms is that the watermark mustn't be perceptible by the human eye in the 3D mesh of the object. And if other senses used to touch the object virtually by special devices any hidden data in the object

Must also be unpredictable .such algorithms represent a revolution in the digital watermarking technology world.

## 6. CONCLUSION

Digital watermarking technology represents a data hiding technique that is used to embed useful information in multimedia object or other work. The proposed technique is classified on different criteria mainly on the domain to spatial domain watermarks, frequency domain watermarks and wavelet domain watermarks .the digital watermarks suffer from different types of attacks that is categorized to state of the art attacks or to estimation based attacks. To detect such attacks a digital watermark agency scheme can be used .the digital watermark technology proved its robustness as protection technique used in many applications such as digital copy right protection .the future of this technology is promising. Recently many proposed algorithms searches the use of digital watermarking for 3D objects.

## 7. REFERENCES

[1] Bing Ouyang WATERMARKING BASED ON UNIFIED PATTERN RECOGNITION FRAMEWORK UMI UMI Number 3336693

[2] Digital Water Marking Injemar J.Cox ,L Miller ,A Bloom Morgan Kaufman Publishers Isbn 1-55860-7145

[3] Image Water Marking In The Time Frequency Domain Mahmood Al Khasaweneh .Proquest Umi Number 3282051

[4] Ongoing Innovation In Digital Water Marking Rajan Samtani,Digimarc Corp, IEEE 0018-9162/09

[5] Rst Invariance Of Image Water Marking Algorithms And The Frame Work Of Mathematical Analysis Dong Zheng Library And Archeives Canada Isbn 978-0-494-50758-2

[6] Digital Water Marking For Compressed Images YAZEED ALRASHED Proquest LLC. UMI 1459036.

[7] Digital Rights And Digital Television ,Bill Rosenblatt ,Giant Steps ,Www.Giantstepsmts.Com Accessed On 10 -12-2009

[8] Content Identification Technologies , Bill Rosenblatt ,Giant Steps ,Www.Giantstepsmts.Com Accessed On 10 -12-2009

[9] Audio Watermarking Technology To Protect Digital Audio Copyrights Last Updated March 1, 2009 By Johnston Yoon Markany, Inc

[10] A Short Summary Of Digital Watermarking Techniques For Multimedia Data. F.Y.DYAN ,I.KING Research Paper ,The Chinese University Of Hong Kong .

[11] CENTER FOR DEMOCRACY & TECHNOLOGY Privacy Principles For Digital Watermarkingmay 2008 – Version 1.0

[12] Attacks On Digital Watermarks: Classification,Estimation-Based Attacks And Benchmarks Voloshynovskiy And Others University Of Erlangen-Nuremberg

[13] Http://Homepages.Inf.Ed.Ac. Uk/Rbf /HIPR2/Hipr_Top.Htm Accessed On 2010-01-15

[14] Answers.Com Accessed On 2010 -01-15

[15] Bayesian Modeling In The Wavelet Domain Fabrizio Ruggeri And Brani Vidakovic NSA Grant E-24-60R At The Georgia Institute Of Technology.

[16] Digital Watermark Mobile Agents Jian Zhao ,Chenghui Luo Fraunhofer Center For Research In Computer Graphics,Inc.

[17] Perceptibility Of Digital Watermarking In Haptically Enabled 3D Meshes A. Formaglio And Others Department Of Information Engineering, University Of Siena, Italy

[18] Robust Mesh Watermarking Emil Praun Hugues Hoppe Adam Finkelstein Princeton University Microsoft Research