

# Digital Watermarking

# Table of Contents

01

## Introduction

Digital Piracy  
Digital Watermarking

02

## Types of Digital Watermarking

visible, invisible, fragile,  
robust, private, public

03

## How does it work

Three Steps of  
Watermarking

04

## Real-life example

"X-Men Origins: Wolverine"  
Leak



# 01

## Introduction

What is digital piracy ?  
What is digital watermarking?

# Piracy

**Digital piracy** refers to the unauthorized use, reproduction, or distribution of copyrighted material. This includes everything from movies and music to software and eBooks. It's a global issue that has significant economic and creative implications.

Combating digital piracy is challenging due to its global scale, the ease of accessing pirated content, and the constant evolution of technology. These factors make it difficult to protect digital content effectively.



# Examples of Piracy



## Movies & TV Shows

Torrent websites, illegal online platforms



## Video Games

Pirated copies of video games, modding gaming consoles.



## E-Books

Unauthorized downloading, sharing without the author's permission



## Music

Unauthorized downloading, P2P networks





## Software

Cracked versions, sharing software licenses illegally



## Art

Reproducing digital art, Using copyrighted images without obtaining a license



So, how do we protect digital content in this scenario?


One effective solution is digital watermarking.



# Digital Watermarking



Digital watermarking refers to the process of embedding information into digital media, like images, videos, or audio files. This information, or 'watermark', can be used for various purposes such as tracking, copyright protection, and authentication.



The primary purposes of digital watermarking are to protect copyright, verify data authenticity, and ensure content authentication. It's a **digital signature** that helps in safeguarding intellectual property and verifying content integrity.

# Applications



## Copyright protection

Torrent websites, illegal online platforms



## Source tracking

Different recipients get differently watermarked content



## Broadcast monitoring

Television news often contains watermarked video from international agencies



## Video editing software programs

To encourage users to purchase the full version to remove it



## ID card security

Verifies authenticity, prevents duplication.



## Fraud and Tamper detection

Reveals alterations, ensures integrity.



# 02

## Types of digital watermarking

# Visible watermarks

These are perceptible watermarks that can be readily seen by the human eye. They are typically in the form of brand logos, images, copyrighted text, personal signatures, and more.



# Invisible watermarks

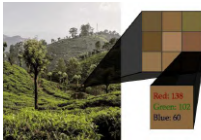
As its name suggests, invisible digital watermarks can't be seen by the human eye. When it comes to audio content, the embedded watermark is inaudible.

An invisible watermark's primary purpose is to provide copyright protection and content identification without altering the visual appearance of the original content. It serves as a hidden signature or fingerprint that can be used to track the origin of the digital file and prove its ownership.

Invisible watermarks are typically applied using specialized software that utilizes advanced algorithms to hide the data within the pixels of the image or video. These watermarks are robust and resistant to various forms of manipulation, making them a valuable tool for ensuring the integrity and security of digital content.

# Invisible watermarks

Depending on its size, photographs will have thousands to millions or even billions of “pixels”. Pixels are tiny squares of one color. Each pixel is composed of three “channels” of red, green, and blue. By mixing various shades of red, green, and blue, we can actually get every color that a computer can render. Perhaps surprisingly, mixing only red, green, and blue also allows us to render every shade of white, black, and gray.



# Invisible watermarks

On a basic level, invisible watermarks work by rounding these channel values to the nearest even or odd number to embed a “code” into the photograph. Odd numbers mean “the underlying watermark pixel is white” and even numbers mean “the underlying watermark pixel is black”. Rounding these values to even or odd numbers actually changes the underlying image but in an imperceivable way. It is very difficult for the human eye to tell the difference between a red shade of 177/255 and 178/255.

Photograph Pixels	Red: 138 Even = Black	Red: 121 Odd = White	Red: 106 Even = Black	Red: 166 Even = Black	Red: 155 Odd = White
Invisible Watermark Pixels					



# Fragile Watermarks



Fragile watermarks are designed to be easily destroyed if the content is altered, making them ideal for tamper detection.

## Legal Documents

These watermarks are designed to be altered or destroyed if the document is tampered with. For example, if a legal PDF document with a fragile watermark is edited or modified, the watermark will break, indicating that the document's integrity has been compromised.



## Digital Photography

If the photo is edited, cropped, or manipulated in any way, the fragile watermark becomes detectable, or it disappears, indicating that the image is no longer in its original state. This is crucial in contexts where authenticity is paramount, like in journalistic or legal settings.



# Robust Watermarks



Robust watermarks, in contrast, are designed to withstand manipulation, such as compression, cropping, or format conversion, ensuring that the watermark persists even if the content is modified.

## Film studios and TV networks

These watermarks can survive alterations like compression, changes in resolution, or even camcording in theaters. The watermark remains detectable, allowing the studio to track and identify unauthorized copies.



## Music Industry

These watermarks can withstand audio compression, equalization changes, and speed alterations. The music industry uses these watermarks to monitor where their music is being played, for instance, on radio stations worldwide, and ensure proper royalty distribution.




## Public vs. Private Watermarks



**Public watermarks** can be decoded without any secret information, often used for visible watermarking.

Example: TV channels often use public watermarks, usually their logos, on the screen during broadcasts. They serve as a constant reminder of the channel's brand and ownership of the content.



**Private watermarks** require a secret key to be decoded, providing an additional layer of security. This type is commonly used in invisible watermarking for sensitive or proprietary content, but they can also be visible.



# 03

**How digital  
watermarking  
works**




## How does it work



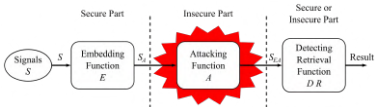
In **embedding**, an algorithm puts the watermark into the host signal without changing how the picture looks or the song sounds.

Then the watermarked digital signal is transmitted to another person. If this person makes a modification, this is called an **attack**. The term attack arises from copyright protection applications, where third parties may attempt to remove the digital watermark through modification.



**Detection** (often called extraction) is an algorithm that is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it may be extracted.

# How does it work



host signal = original file (before watermarking)

## Three Steps of Watermarking

- Embedding
- Attack
- Detection

# 04

## Real-life example

## Case: "X-Men Origins: Wolverine" Leak (2009)

A nearly complete version of "X-Men Origins: Wolverine" was leaked online about a month before its official release date. This unfinished copy of the movie, missing many special effects, appeared on various file-sharing websites. The leak was downloaded millions of times.

The leaked copy contained digital watermarking, which 20th Century Fox, the studio behind the film, used to investigate the source of the leak. The watermark helped trace the leak back to an individual who had access to the copy. It was found that the copy had been intended for internal use, possibly for review or post-production purposes.

The individual identified was an employee of a company contracted by the studio named Gilberto Sanchez. He was arrested and charged with copyright infringement.



05

**Bibliography**



# Bibliography

[1] [https://en.wikipedia.org/wiki/Digital\\_watermarking](https://en.wikipedia.org/wiki/Digital_watermarking)

[2] <https://www.digitalguardian.com/blog/digital-watermarking#:~:text=Digital%20watermarking%20is%20a%20po tent,and%20ownership%20of%20copyrighted%20material.>

[3] <https://invisiblewatermark.net/how-invisible-watermarks-work.html>

[4] <https://www.nytimes.com/2010/01/13/nyregion/13wolverine.html#:~:text=An%20article%20on%20Wednesday%20about,a%20represe ntative%20called%20him%20back.>

THANK  
YOU

...

**Gherghel  
Vlad-Zeno**

...

**Hincu Alice-Ramona**

...

**Herlea Ștefan-  
Alexandru**

