DIGITAL WATERMARKING

Raj Jain, Aditya Balooni, Harshit Jain

Abstract
Digital watermarking technology is a frontier research field and it serves an important role in information security. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. In view of the importance of digital images copyright protection, based on the analysis of the main digital watermarking algorithms, the digital watermarking technology can be applied to the image copyright protection. The two dimension discrete cosine transform is encoded on the Windows platform by using Visual C++ program language. The experiment result shows that the digital watermark is non-perceptible; the watermark information can be extracted even if it has been attacked, and the expected effect can be achieved. Everyday tons of data is embedded on digital media or distributed over the internet. The data so distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of the same concept. There are two types of watermarks: visible watermark and invisible watermark.

Introduction of Digital Watermarking
The history of watermark dates back to the 13th century. Watermarks were used to indicate the paper brand and the mill that produced it in Italy. By the 18th century watermarks began to be used as anti-counterfeiting measures on money and other documents and in 1995 interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark. For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker.

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, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

**Watermarking**

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system.

The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1.

Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it; therefore it inevitably affects the image’s quality. We want to keep this degradation of the image’s quality to a minimum, so no obvious difference in the image’s fidelity can be noticed.

The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded.

The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

**Definition of Watermarking**

Embedding a digital signal (audio, video or image) with information which cannot be removed easily is called digital watermarking.

**Principle of Watermarking**

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. The original image and the desired watermark are embedded using one of the various schemes that are
The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark.

The different techniques differ in the way in which it embeds the watermark onto the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

**Watermarking applications**

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection.

One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier.

Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself.

Transaction tracking is another interesting application of watermarking. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work. For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked
to the Internet, the movie producers could identify which recipient of the movie was the source of the leak.

Finally, copy control is a very promising application for watermarking. In this application, watermarking can be used to prevent the illegal copying of songs, images of movies, by embedding a watermark in them that would instruct a watermarking-compatible DVD or CD writer to not write the song or movie because it is an illegal copy.

**Watermarking models**

There are several ways in which we can model a watermarking process. These can be broadly classified in one of two groups. The first group contains models which are based on a communication-based view of watermarking and the second group contains models based on a geometric view of watermarking.

**Communication-based models**

Communication-based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedded to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process.

**Geometric models**

It is often useful to think of watermarking in geometric terms. In this type of model, images, watermarked and unwatermarked, can be viewed as high-dimensional vectors, in what is called the media space. This is also a high-dimensional space that contains all possible images of all dimensions.

Geometric models can be very useful to better visualize the watermarking process using a number of regions based on the desirable properties of watermarking. One of these regions is the embedding region, which is the region that contains all the possible images resulting from the embedding of a message inside an unwatermarked image using some watermark embedding algorithm. Another very important region is the detection region, which is the region containing all the possible images from which a watermark can be successfully extracted using a watermark detection algorithm.

**Requirements**

The major requirements of digital watermarking are:

**Transparency**

The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life easier for the attacker. It also degrades the commercial value of the image.

**Robustness**
This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

Applications

Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

Broadcast Monitoring: As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

Content Labeling: Watermarks can be used to give more information about the cover object. This process is named content labeling.

Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

Classifications of Watermarking

Visible

The watermark is visible which can be a text or a logo used to identify the owner.
Any text or logo to verify or hide content
Fw= (1-α) F+ α*W [6]
Fw = Watermarked Image
α =constant; 0<=α<=1, IF α=0 No watermark, if α=1 watermark present
F =original image

Invisible

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied.
Invisible watermark can be further divided into three types,
Robust Watermarks

Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

Fragile Watermarks They are designed with very low robustness. They are used to check the integrity of objects. Digital Watermarking.

Public and Private Watermark They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.

Techniques or Schemes of Watermarking

Spatial Domain Techniques
Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression [7]

Least Significant Bit Coding (LSB) LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

Predictive Coding Schemes
Predictive coding scheme was proposed by Matsui and Tanaka in [8] for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.

Correlation-Based Techniques
In this method a pseudo random noise (PN) with a pattern \( W(x, y) \) is added to an image [4] [11], according to the equation
\[
Iw(x,y) = Watermarked \text{ image.}
\]
\[ I(x, y) = \text{Original image} \]
\[ K = \text{original factor} \]

**DIGITAL WATERMARKING:**

The tool used for the execution of this algorithm was ‘Matlab’. The aim of the program is to replace the LSB of the base image with the MSB of the watermark. First, the program asks the user for the images to be read. The user will then enter the name of the images, both the base and the watermark, with their extension. Both these images will be read and stored by the tool, which is ‘Matlab’ in our case. The tool will also display these images to the user with their respective titles. The program will then change the image size to double. This is done so as inform the tool to provide double data-type space for the images. The reason for doing so, is to provide decimal storage for the subsequent additional operations which will be performed on the base and watermark image. The next step is to assign the number of most significant bits of the watermark which will be used to overwrite on the least significant bit spaces of the base signal. Once the user provides this, the watermark signal bits are shifted to the right by the specified bits.

**Results**

- **Base Image ‘A’**
- **Watermark Image ‘B’**
Watermarked Image, using bits=1. Since it is an invisible watermarking scheme, only the base image is visible.

Watermarked Image ‘C’, using bits=5. This is a visible watermarking scheme, both base and watermark images are seen in the watermarked image.

**Conclusion**

Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. These can be described by many different models. Two broad categories for these models were described in this essay. These are communication-based models and geometric models. Communication-based models can be further divided into those which use side-information and those that don’t. One example system was used to illustrate non-side-information models, and two example systems were used to illustrate side-information models. Each of these systems has its advantages and disadvantages, and each one trades some important watermarking property for another. The choice of which to use relies on the underlying application’s requirements.