A SCHEME FOR ROBUST AND IMPERCEPTIBLE VIDEO WATERMARKING

SANAA ADANA ABBAS
Yildiz Technical University , Department of Computer Engineering

E-mail: Sanaalasadi2000@yahoo.com

ABSTRACT

The prevalent growing of the Internet has made the digital media available to everyone. Various digital watermarking techniques have been provided to find solutions to protect the digital media. In the most of these techniques, the digital media that include the watermark are distorted and the robustness in extracting the watermark is unacceptable. The utilization of a scheme for finding secure and preferable locations to embed the watermark inside the media with little distortion and an acceptable robustness is an appropriate solution to solve these problems. In this paper, a robust and imperceptible video watermarking scheme is proposed to overcome a wide range of attacks like frame noise attacks and frame cropping etc. by utilizing the preferable positions in the wavelet transform of the video frames.

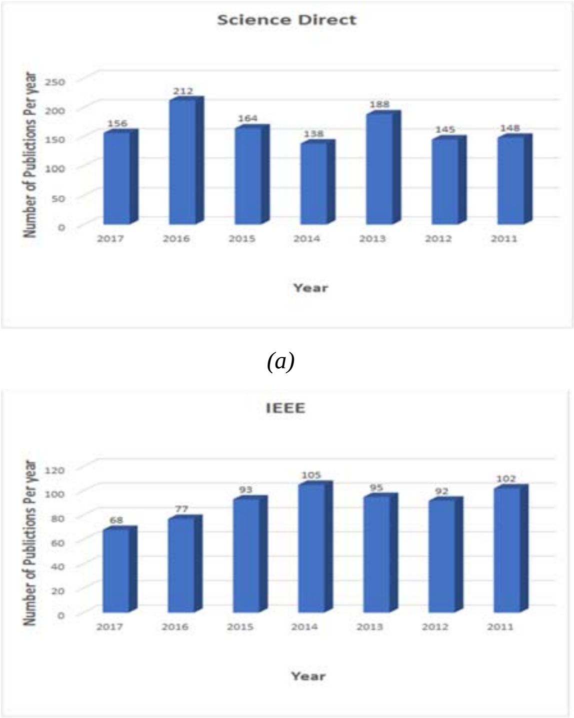
Keywords: *Video Watermarking, Wavelet Transform, Watermarked video frame, Watermark inclusion, Watermark extraction.*

1. INTRODUCTION

Digital video watermarking schemes supply a suitable framework to protect the copyrighted digital videos from illegitimate modifications and non-desirable distributions. The core defiance which is notable by the researchers of digital video watermarking is to sufficiently embed a robust watermark for resisting various kinds of attacks with keep on the imperceptibility of the host video.

Formerly, the digital video watermarking schemes were depending on the spatial domain methods which are easy but influenced by the attacks. Latterly, the transform domain methods are widely used to embed the watermark in the transform domain of the digital video in a robust way [1]. Figure 1 demonstrates the number of publications in the field of video watermarking at "Science Direct website", and "IEEE Explore website" between the years 2011-2017.

Various schemes based on transform domain have been proposed for improving the digital video watermarking. Most of these improved schemes are working with the discrete wavelet transform, singular value decomposition and etcetera.



(a)

(b)

Figure 1: The publications distribution data between the years 2011-2017 have been retrieved from (a) "Science Direct website "; (b) "IEEE Explore website ".

Sanjana Sinha et al. [2] presents a hybrid scheme based on discrete wavelet transform with the help of principal component analysis method to decrease the correlation among coefficients through the wavelet decomposition process. This scheme selects the Low-frequency sub-bands of all the video frames for watermark inclusion, therefore the perceptual quality of the video is not good, and since the scheme is not well designed, the values of extracted watermarks under attacks are low. Also, the same concept of the hybrid scheme but with the selection of Low-frequency and High-frequency sub-bands is utilized by Mohan A. Chimanna et al. [3] in which the results are also still not good. Bhavna Goel et al. [4] presented a video watermarking scheme depending on discrete wavelet transform and singular value decomposition in which the watermark inclusion is done on the singular values of the Low-frequency sub-band. The selection of this sub-band led to increase the robustness of the extracted watermark, while the perceptible quality of the watermarked video is relatively good since the scene change detection technique is used. Pragya Agarwal et al. [5] presented a scheme depensing on lifting wavelet transform and singular value decomposition. This scheme presents results approximate to the results in work [4]. The authors in work [6] presents a relatively robust and imperceptible hybrid scheme based on non-subsampled contourlet transform and singular value decomposition. Another hybrid scheme depending on biorthogonal wavelet transform and singular value decomposition is presented by Anjaneyulu S. et al. [7]. The experimental results of this scheme indicate a good values of extracted watermarks under attacks, and the use of optimization technique to generate random video frames to the watermark inclusion process led to a good video perceptual quality.

This support medium can be almost anything, the most commonly used being images, but also videos, texts, audio files or softwares are perfectly viable candidates for embedding. The relations between watermarking in those media are displays in Figure 2.

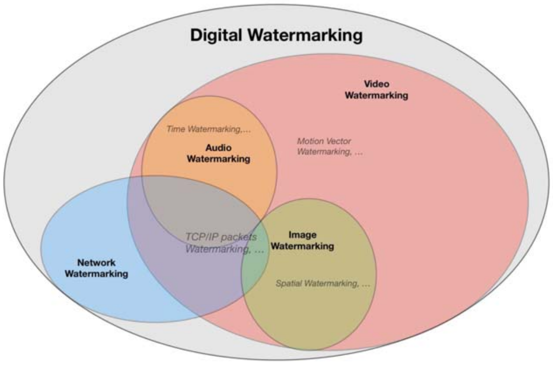


Figure 2: Venn Diagram of main media able to support digital watermarking

This survey however, focuses on watermarks applied to video streams as carrier signals. Video streams can be viewed from many different perspectives that bear various watermarking techniques. We will here consider the following ones:

• First, one can see it as a sequence of bits. Watermarking being useful mainly when the medium is transmitted between entities of a network, we can also view this sequence as packets of data. Hence, this sequence (or those packets) follows a range of protocols that will integrate some redundancies that can be exploited for watermark embedding ([6]).

• Another view of videos is as a sequence of frames displayed one after the other at a high rate. Therefore, any static image watermarking technique can also be applied to videos by applying it independently to the frames of the video. The redundancies used for watermark embedding in image processing are spatial: two pixels in the same region will usually have a higher correlation than two unrelated pixels coming from two completely different parts of an image ([7]). Those techniques are still perfectly efficient and irreplaceable for some cases of video processing like Real-Time Communications where the following frames are not yet known by the system in charge of embedding the watermark.

• As long as the scene change occurs, one could also see a video as one initial static image and a multitude of infinitesimal accumulated changes between the first frame and all the following ones. This view of video sequence induce temporal redundancies that can be used for watermark embedding too ([8]). Indeed, as for the pixels with image watermarking, two consecutive frames will be highly correlated images.

• Finally, a video usually contains some audio data, which imply that all audio watermarking techniques can also be applied to video watermarking ([9]).

In this paper, a blind, robust and imperceptible scheme of digital video watermarking is proposed in which the wavelet transform is used and the process of watermark embedding is done in the middle and high frequency sub-bands of the selected video scenes. The experimental results have been undergone for checking the imperceptibility and robustness under applying various attacks. The construction of the paper is as follows; The next section encompasses a brief explanation for the wavelet transform based scheme; The proposed digital video watermarking scheme, watermark inclusion, and extraction procedures are presented in section three; Section four explains the experiential analysis. The conclusion is given in the last section.

2. WAVELET TRANSFORM BASED SCHEME

The wavelet transform is a time domain localized analysis technique; It differentiates time in a high-frequency area and the frequency in low-frequency areas of signals. The discrete wavelet transform is a multi-resolution mathematical tool to decompose a video frame into four components; Low-frequency, vertical and horizontal high frequency (middle-frequency), and high-frequency. This transform can further be utilized for multiple-scale wavelet decomposition [8]. For the purpose of increasing the watermark robustness with a little effect on video quality, the watermarks should be embedded in areas which are less sensitive to the human visual system, like middle and high frequency sub-bands.

3. WATERMARKING GENERALITIES

We model a video signal as send by a user (end-point) to servers that will then redistribute it to some users. Iacovazzi et al. [10] extract four different watermark lifecycles from this model. Those are presented in Figure 2. We detail Iacovazzi's model by differentiating three possible signal states that can be reached during these watermark lifecycles. Note that the state "Watermark embedded but unused" can be replaced by the state "No watermark" in schemes that allows complete extraction of the watermark and not only detection.

3.1 Global Scheme

Since we defined watermarking as embedding extra information into a signal, we model the scheme followed by any watermarking, physical or digital, in five steps as shown in Figure 3. The two first phases are mandatory for any watermarking process: the context setting phase as to embed information in a signal one needs to choose which information and what signal, then the embedding of the watermark phase as it is the modification made to the signal that create the watermark. Those two steps are followed by three phases that only happen under certain conditions: for the transmission phase the embedded data needs to be shared, and the two last phases, the watermark extraction and its utilization are executed only when the watermark is exploited. Indeed, one could use the watermarked media by just ignoring the watermark. The first and last phases mostly depend on the application of the watermarking whereas the three other ones define which properties (see Section 2.2) the watermarking will have. In general, the designer of a watermark technique only has access to the embedding and extraction process to ensure the behavior the signal should follow during the transmission phase whereas the person using the technique will have to set the context and treat the extracted data to solve his problem.

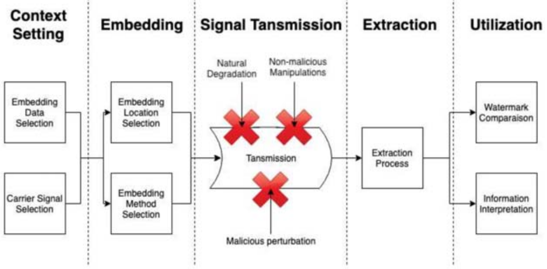


Figure 3: Flow chart describing the general scheme of any watermarking process

Context Setting This step is about observing the application aimed by the watermarking and deducing for it the best way to design the process. The two most important decisions to take are the selection of the medium that will carry the watermark and what data need to be embedded to fulfill the goal. Even though the medium might seem quite obvious, there can be several possibilities for the same application. Video watermarking is a perfect example to demonstrate this, as we could embed the watermark either in the audio channel or in the visual channel as in [11] where both visual and audio channels are watermarked. Concerning the choice of the embedded data, it also directly depends on the application. It could be for example an image, an audio signal, a text or some raw bits. Those two components are the most important inputs of the embedding process that can work as a black box to the user. One might also need to encrypt (or scramble) the watermark before embedding it as [12] that uses the Arnold transform to do so. This need can come from two facts. First, the user might not want anyone that can extract the watermark to be able to interpret it. Second, to make the watermark invisible as encryption can make it appear as a white noise with zero mean and unit variance. The encryption can be done either by the user of the watermark scheme or by its designer during the embedding process. In the first case the designer simply treats the extra data as raw bits.

Watermark Embedding The embedding phase can be seen as a black box, the main inputs being the signal carrier and the data to be embedded (as previously mentioned) and output being the watermarked signal. Depending on the technique used to embed the data, it might also output information needed for the extraction ([13] output a location map to identify which part of the image was watermarked). We split this process in two parts: the decision of the location where extra data are to be embedded and the choice of the method used to add this data to the chosen location. Another possible input is a key that can be generated at random or decided by the user to secure the watermark. As the embedding step is the one responsible for the behavior of the signal during transmission and the one that defines how the extracting process will have to work in order to retrieve the correct information, one can consider it as the most important step of the all scheme.

Signal Transmission During the transmission, the signal can be altered unintentionally by natural noise or by users editing it or relaying it. Later on, we will refer to this as natural alteration. The signal can also be modified intentionally by malicious attackers. For those reasons, the scheme should be designed to minimize nature’s and malicious attackers effects, and possibly users effects depending on the goal of the watermark.

Information Extraction In this step, the watermark is extracted from the carrier signal. However, we consider two different meanings to information extraction:

- Retrieving a single bit information describing watermark presence or absence in the carrier signal. The extractor will be called binary ([14]).
- Retrieving the complete watermark extracted from the signal carrier ([15]). We define such extractor as complete.

To achieve information extraction, one can insert additional information apart from the watermarked signal itself such as the logo of the company claiming ownership of the data. This additional information defines the blindness of the watermark and is generally either the original watermark, the original carrier signal before embedding, a key used for embedding or other kind of data such as the location map mentioned in the watermark embedding paragraph. The extraction, if executed, can be processed at least at three different stages of the watermark lifecycle: at a middle point of the transmission (either by an attacker or by a point relaying the signal), on-the-fly by the receiving end-point, or a posteriori. A posteriori extractions can be processed by two entities: a user trying to remove the watermark (either illegally as an removal attack or legally as part of an access control mechanism), or the owner trying to prove ownership of the product. We observe that in the two first locations the actors are active as their doing might modify the behavior of the receiver’s client side, while the last one is passive as it cannot directly influence the way the application will work.

Extracted Data Utilization Finally, the needed information has been retrieved and the last stage of our watermark processing model is starting. If the extractor is binary, then this step is quite straightforward: the user gets a "yes" or "no" answer to one of the those two questions: "Is there a watermark in this signal?" or "Is this watermark present in this signal?". If the extractor is complete, then more possibilities will be available. First, the user can look at the watermark and use it to prove ownership by comparing it to one belonging to the real owner of the signal. This utilization is the same as when using a binary extractor. Second, the user can compare the retrieved watermark to another one in order to determine the transformation that have been operated on the signal. It can be useful to identify tampering of the signal for example. Third, the user can read the watermark as new information on the users that relayed the signal, which is the technique used for network analysis. Finally, the user can use the extracted watermark to retrieve the original carrier signal by simply computing the difference between the two signals. This is referred as "reversible watermarking" and is the preferred approach for Access Control application of watermarking.

Another relevant technique to mention as it is a usual watermarking scheme, is dual-watermarking ([16, 17]). It consists in embedding two watermarks using two different methods and in two different locations. This sort of scheme can be particularly stronger than simple watermarking, but usually at the cost of increasing drastically the computational complexity. We will later see examples of such scheme.

3.2 Properties and Evaluations

As previously mentioned, watermark system can be viewed as a black box. This black box returns some outputs given a set of inputs. The outputs vary depending on the design of the system that can be described by its properties ([18, 19, 20]). Those properties are the how-to of the usage of this black box. The need for one property directly depends on the use case of the watermark. The designer's decision of which properties his/her scheme will fulfill can be difficult, as all of them are linked together, making this decision an optimization problem of the trade-offs between these properties.

3.2.1 Medium Fidelity (or Distortion)

We define the medium fidelity of the watermark as how noticeable the distortion on the carrier signal after the embedding of the watermark is. In the specific case of image processing, this property is often called invisibility whereas for other signals it is usually called undetectability. There are many measures that can be used to quantify the medium fidelity of a watermark. Most of those measures are detailed in [21]. We here detail the most common ones:

• The Hamming Distance: it compares the raw bit streams of the original image and the watermarked image and is defined as the number of bits that differ between them. Also defined the Hamming distortion of sequences in [22]:

$$dist(X,\hat{X}) = \sum_{i} |X_i - \hat{X}_i|$$

Where X_i is the i^{th} bit of the original signal and $\hat{X}_i$ is the i^{th} bit of the watermarked signal. The higher the distance, the more distorted the signal.

• The Bit-Error-Rate is related to the Hamming Distance. It is given by

$$BER = \frac{dist(X,\hat{X})}{len(X)}$$

and is the ratio of bits that differs by the total number of bits contained in the signal.

•The Mean Square Error is also commonly used to describe quality of predictors especially in Machine Learning models as in [23], and is given by the following formula:

$$MSE = \frac{1}{n}\sum_{i=0}^{n}(X_i - \hat{X}_i)^2$$

The MSE is generally used to assess the quality of a predictor, but can give a first idea of the “error” induced by the watermark in the signal carrier. The higher he MSE, the more distorted the signal.

• The Peak Signal to Noise Ratio is the most common measure to quantify watermark visibility. It is directly defined by the MSE of the signal:

$$PSNR = 10.log_{10}(\frac{MAX^2}{MSE})$$

In this formula, MAX is the maximum possible value of the signal. The PSNR's unit is the decibel. The lower the PSNR, the more distorted the signal.

• The Correlation Coefficient will be the last quantification described here. It represents the similarity between the original and the watermarked images and is given by [24] as

$$C(X,\hat{X}) = \frac{cov(X,\hat{X})}{\sqrt{var(X).var(\hat{X})}}$$

where cov is the covariance between the two signals and var is the variance of the given signal. The higher the correlation is, the more distorted the signal is.

There are a lot of other measures that can be used for distortion measurement, but those are the most commonly used ones in the watermarking field. It is important to note that a watermark user might want a high distortion when the watermark is embedded in order to create an Access Control system for example using reversible watermarking.

3.2.2 Watermark Fidelity (or Distortion)

The name of this property is indeed similar to the previous one, as we use it to describe how the embedded information has been preserved during the transmission phase of the communication process. Its importance depends primarily on whether you need to know the watermarked information for the watermark detection or not. As it deals with distortion, all measurements of medium fidelity also allow to quantify watermark distortion. Another property linked to this one is the recognizability, that our model as well as [21] use to quantify the ability of a binary extractor to output a correct result bit. To measure recognizability, [25] uses four primitives:

• True Positives: number of signal decided as containing a watermark that did contain a watermark.

• True Negatives: number of signal decided as not containing a watermark that did not contain a watermark. • False Positives: number of signal decided as containing a watermark that did not contain a watermark.

• False Negatives: number of signal decided as not containing a watermark that did contain a watermark.

From those primitives, a significant number of values that give information on the recognizability can be computed such as the True Positive/Negative Rate, the Positive/Negative Predictive Rate, the False Positive/Negative Rate, the False Discovery Rate, the False Omission Rate, and the Accuracy. The main way to represent those is using the Receiver Operating Characteristics curve obtained by plotting the TPR (or Sensitivity) against the FPR (or Specificity) as shown in Figure 4. The recognizability is observed by considering the area under the curve as explained in [26]. The closer to the top and left borders the curve is, the more accurate the decider is, the more recognizable the watermarking scheme is.

3.2.3 Blindness

We call blindness of a watermark the property defined by the prior information needed by the detector to retrieve the wanted data from the carrier channel. [21] differentiate four main possibilities regarding the blindness of a watermark.

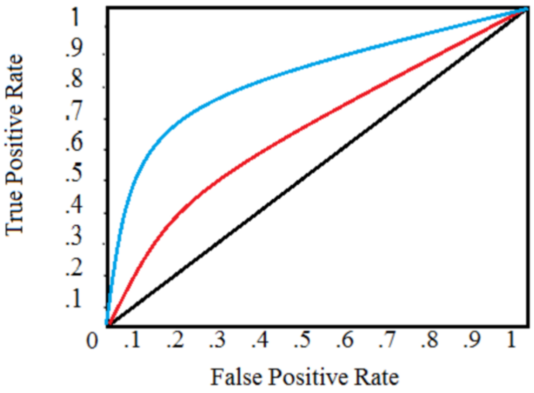


Figure 4: Receiver Operating Characteristics, the diagonal being a completely random decider, and the blue having a better recognizability than the red

Private Watermarking This type requires at least the original signal to be recognized as in [27]. In the case of Network Watermarking, to determine whether a packet has been embedded by a watermark or not, the original encapsulation and headers of the packets would be needed. This extraction mode can for example compute the difference between the original and potentially watermarked object which should result in an estimation of the watermark (encrypted or not). The watermark itself may or may not be needed depending on the embedding process. So the total inputs of a private extracting process are the watermarked signal, the original signal, potentially the watermark and potentially an encryption key. These watermarking schemes are usually quite robust. Indeed, the more information we have about what we are looking at and for during the extraction phase, the easier it is to determine the watermark's presence.

Semi-private Watermarking More often called semi-blind, in such scheme the original signal is not mandatory, but the original watermark is required ([28]). The knowledge given up decrease the robustness of the global system following the same principle as the robustness given by a private watermarking scheme. In [29], a scheme was designed based on spread spectrum techniques and uses two secret keys to embed the information. Both keys are needed for the detection, but not the original bit stream.

Public Watermarking Also called Blind Watermarking, it only uses the received/watermarked signal and an information key to detect and/or extract the watermarked signal. For example, [20] describe a scheme that uses only a location map to retrieve the embedded information. This kind of technique requires a high level of security to transmit the information key between the embedder and the detector as it is sufficient to extract the data.

Asymmetric Watermarking This last kind of extraction also known as Public Key Watermarking describes a system where anyone with access to the watermarked signal can observe the embedded information, but only one person could have embedded it and no one can remove it. It is by nature computationally more expensive as it usually relies on heavier cryptographic primitives. Schyndel et al. describe a watermarking scheme based on Legendre sequences in[30], their invariance under Fourier Transform allows the author of creating such system. Other schemes can be based on RSA cryptography such as [31] to achieve asymmetry.

Others Some other schemes exist, but they usually define themselves as a combination of some of the four previous watermarkings such as the dual-watermarking method presented in [32], where a first asymmetric watermark is embedded, followed by a second symmetric one.

3.2.4 Robustness

The robustness property can be defined by how difficult it is to remove the watermark from the embedded signal, whether it is by a malicious attacker, by a non-malicious one, or by natural degradation of the signal. Three kinds of robustness levels are usually distinguished ([18]). They all have different characteristics and can be linked to various specific applications. In many of the currently existing techniques, watermarking security is ensured by obscurity, which is completely against Kerckhoff's principle ([33]). For example watermarks using techniques such as Least-Significant-Bit embedding can be easily detected, extracted and removed if the adversary is aware of how the watermark has been embedded. This is a really important design flaw, therefore fewer and fewer schemes use this kind of insecure methods. Robustness deals more about general signal manipulations.

Fragile Watermarking This level of security is the weakest of all, meaning that the embedded information can be removed very easily. Indeed, almost any manipulation applied on the media would destroy the watermark. The goal is to make sure that absolutely nothing altered the integrity of the signal. In [34], the author describes a fragile scheme that allows not only to detect the location where the image has been tampered, but also to reconstruct the original image. This is possible using the concept of self-referenced watermark described in the same article: the embedded information is a description of the carrier image.

Semi-fragile Watermarking Related to fragile watermarking, semi-fragile techniques ensure that the signal was not altered in a significant way such as image forgery on top of it or geometric transformations, but will still resist common light signal modifications such as filtering or compression. If one of those light manipulations is applied, the watermark will suffer very few changes whereas if a heavy editing of the signal is executed, the watermark will be destroyed or significantly damaged. This is particularly important for media as the signal is usually compressed and encoded, sometimes with losses in order to be stored and transmitted using less bandwidth. [35] proposes an example of such watermarking system. Indeed their results show good robustness against re-compression, noise addition and frame dropping attacks. Moreover, malicious attacks (non-content preserving) can be detected and localized in a video frame.

Robust Watermarking Finally, robust watermarking refers to schemes that embed data as securely as possible so that it is hard to remove the watermark. The main use for this level of robustness is copyright protection as the mark embedded by the owner should never be removed. High robustness can be achieved by various means including embedding at low bit-rate, multiple embeddings of the same information or self-referenced watermarks. An example of such robust watermarking scheme is [36], which implements a watermarking solution presenting good result against important cropping, rotation, scaling as well as combined attacks such as rotation, cropping and histogram equalization at the same time.

To evaluate the robustness, the usual strategy is to apply various kinds of attacks on an embedded signal, extract it and evaluate the difference between the originally embedded watermark with the extracted one. A generic tool has been developed for image watermarking since 1997 called Stirmark [37, 38]. It applies a series of random bi-linear geometric distortions to generic images containing a watermark in order to try to damage the embedded data of a given algorithm.

3.2.5 Capacity

Also sometimes called payload, the capacity of a watermark as defined by [18] is the quantity of information that the scheme is able to embed in the carrier signal. It is usually quantified in bits per covert signal unit. If the covert signal is an image or a video, then the capacity is the number of bits that fit per carrier image (or frame). An important trade-off is to be decided between capacity and medium distortion: indeed, the more bits we want to embed, the more visible the distortion induced usually is (at least when using the same embedding technique).

3.2.6 Time Complexity

The time complexity of a watermarking scheme can be divided into two parts: time complexity of the embedding process and time complexity of the extracting process. Their meaning are quite straightforward: the embedding (respectively extracting) complexity is the time that it takes to embed (respectively extract) a signal. When the embedding is executed right before emission (and respectively extraction on reception), time complexity is particularly important as it represents a delay. A common way to quantify the time complexity, especially for the video watermarking, is the Bit Increased Rate (%) as defined in [20]:

$$BIR = \frac{R_{\hat{X}} - R_X}{R_X} * 100$$

where R_X is the bit-rate of the original stream and $R_{\hat{X}}$ is the bit-rate of the watermarked stream.

3.3 Applications

Applications of digital watermarking are as broad as the techniques that can be used to implement it. During our research, five major applications stood out as the most encountered ones. These are copyright protection, tampering identification, traffic analysis, clandestine communication and access control. These applications all use digital watermarking to solve some of the four central concepts of information security as defined by [39]:

- Confidentiality: the information is not disclosed to unauthorized entities.

- Integrity: the information is proven to be complete and accurate as the source emitted it.

- Authentication or Non-Repudiation: the source that emitted the information prove as well as not deny having sent it.

- Availability: the information is available when needed by the authorized entities.

The relationships between the security concepts and the main applications of watermarking are shown in Figure 5.

3.3.1 Copyright Protection

Copyright protection is the most common application of watermarking. Indeed, as seen in the introduction, proving origin was the main reason why paper watermarks where first invented [40]. The basic idea is to embed the information to identify the owner in the product. Then, if a product's origin generates a controversy, the embedded information simply has to be extracted in order to determine who the product belongs to. When the watermark is visible, the extraction process is not necessary as the identifier is directly visible.

The application fields are many, including obviously Art, as the author of a piece, would it be a music [41], a painting or a photography does not want his creation to be claimed by someone else [42], Geographic Information Systems as geographical data are hard and expensive to collect [43]. The identifying information embedded can be used in court in case of issue regarding an object's origin under certain conditions as exposed in [44].

3.3.2 Tampering Identification

To stay in the legal field, one can also use watermarking in order to detect data tampering. For example this can be used to detect forgeries or fake images as they are usually re-assembled parts of images. There are two main ways to identify such tampering on a medium:

- The first one is not specific to watermarking, but is the most common method to ensure integrity: the use of a checksum ([45]). Meaning a string of fixed length that is absolutely specific to a sequence of bits. The slightest modification to the image would change completely the output of the checksum. Linking it to watermarking is quite straightforward: one just has to compute the checksum and embed it robustly into the image. To verify the integrity, the checksum is extracted and compared with the one computed from the original image. If both differs, then the image has been tampered. [46] proposes such method especially applied to the medical field where the checksum of most important zone of the image (Region Of Interest) is embedded in the rest of the image. The positive side of the technique is that it only requires a low watermarking capacity as checksums are digest of the global images, the counterpart is that one can only notice that the image was modified, but not where nor how.

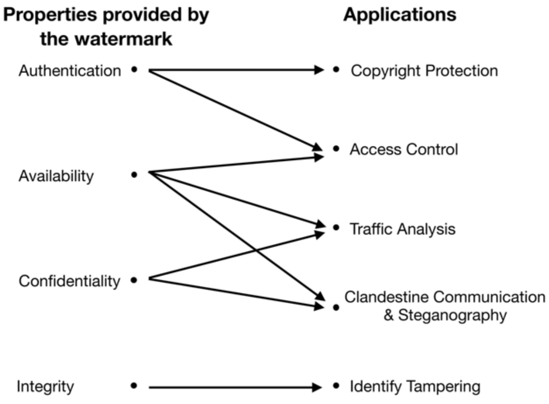


Figure 5: Graph of watermarking applications and the fields they can be applied to

• The second technique specifically uses the properties of watermarking as it relies on a low robustness of the watermark. If the image is modified, so is the watermark. Using this principle, one can not only observe that the image has indeed been modified, but also where it has been tampered. The original carrier signal can then sometimes be recovered. For example if the watermark was a self-referenced one as in [34].

As we saw, tampering identification has applications in the medical domain, but also in justice where the integrity of images used in court is essential, in military as intelligence has to certify that, for example, pictures used for strategic decision have not by compromised. Journalism can also use this application as it is also a reporter's job to ensure the veracity of his images.

3.3.3 Clandestine Communication

Clandestine communication using digital watermarks is known as Steganography. Steganography can be considered as a sub-domain of watermarking, since its goal is to embed a secret message into a covert medium. The goal of steganography is often described by the Prisoner's Problem [47]. This problem describes a situation in which two prisoners must find a way to communicate secretly together in full view of the warden. The main difference with usual watermarking is the importance of the secrecy of message embedded. Steganography usually does not give importance to the covert medium as long as it safely protects the message, we say that steganography is watermark-oriented. The three most relevant properties of a steganographic system are a high capacity, a high undetectability and a low watermark distortion. From this definition, we define watermarking focused on the medium as carrier signal-oriented which relies on a high robustness, blindness of the extraction and a high medium fidelity.

There are many reasons to develop clandestine ways of communicating. In the military and intelligence fields, it is very important to be able to communicate between two points, keeping not only the content of the discussion secret to the enemy, but also the presence and location of the two entities communicating. The same reasons can motivate journalists or whistle-blowers to use clandestine communication in order to avoid censorship control. An example of technology designed specifically to circumvent censorship is [48], where the Message-In-A-Bottle protocol is defined in order to establish first contact between two entities through photos included in blog posts so that they can then start a secure communication.

Another application of watermarking that can be considered as clandestine communication is data exfiltration. A well known cyber-attack model is the Advanced Persistent Threats (APTs) [49]. The model decompose the attack into several stages, the last one being data exfiltration that aims at retrieving the information extracted for the target computer network. Indeed, some security mechanisms are usually in place to prevent such exfiltration, using steganography is a solution to bypass those security mechanisms as in [10].

3.3.4 Traffic Analysis

As a goal of images and videos is to relay information, these data are usually transmitted. Transmitting data generates traffic and flows that can be analyzed in order to monitor and enhance control and security over the resulting network. Watermarking is one of the technology that allows such traffic analysis. For example, to break anonymity on network traffic, a unique identifier can be assigned to each entity of the network. These ids being automatically embedded as watermarks into the transmitted packets. This application is a part of the fingerprinting technology [50]. One can also automatically detect previously embedded watermark to monitor broadcast of a commercial or a movie. The implementation of traffic analysis using watermarking gives access to an extremely wide variety of tools such as unusual traffic detection, geographical prediction, network design decision making and more as detailed in [10].

3.3.5 Access Control

The last presented application of digital watermarking is Access Control. Part of this application is included in the previous description of clandestine communication, as hiding a signal in a radio transmission, for example, restrain access to this information to those unaware of its presence. Access control can also be guaranteed by the implementation of a software client side which blocks a media if it contains (or not) a certain watermark. More information on this application can be found in [9]. The domains where such access control is used include TV broadcasting, access to medical information, or network design.

4. THE PROPOSED DIGITAL VIDEO WATERMARKING SCHEME

The presented scheme encompasses the watermark inclusion and extraction procedures.

4.1 The Procedure of Watermark Inclusion

The specifics of the watermark inclusion procedure are as follows (see Figure 6 which demonstrates the overall structure of this procedure):

First Step: Choose the watermark image of size $m \times m$.

Second Step: Spread out the watermark image n times for decreasing the relationships between pixel spaces by utilizing the Arnold cat map transform.

Third Step: Select an AVI video file as an input and convert it into frames.

Fourth Step: For each video frame, perform the histogram distinction technique for finding the first different scenes.

Fifth Step: For each selected video scene; Apply one level discrete wavelet transform on the selected RGB channel to generate four wavelet areas low-frequency, two middle-frequency, and high-frequency.

Sixth Step: Pick out the middle and high frequency sub-bands; Then, divide those specific sub-bands into non-overlapped blocks of size 8×8 pixels.

Seventh Step: Generate a random key in the length of watermark image size which represents the random locations without repetition (the blocks number) to be used for watermark bits' inclusion.

Eighth Step: For each Bit in the binary watermark image:

- Fetch the non-repeated block depending on the selected random number.
- Determine its first row, the maximum element and the minimum element inside that row.
- If the watermark bit value is one, then replace the first element in the row by maximum element + α.

$$\mathit{First\ element\ in\ the\ Row} \leftarrow \mathit{Maximum\ Element} + \alpha$$

- Else, if the watermark bit value is zero, then replace the first element in the row by minimum element - α;

$$\mathit{First\ element\ in\ the\ Row} \leftarrow \mathit{Minimum\ Element} - \alpha$$

Where α is an estimated strength parameter (α=2).

Ninth Step: Rebuild the blocks that include the embedded bits into middle and high frequency sub-bands, then an inverse discrete wavelet transform should be applied to those modified sub-bands and non-modified high-frequency sub-band for obtaining the watermarked channel; After that, merge this channel with the other channels for making the watermarked video frame.

Tenth Step: At the end, all the watermarked and non-watermarked video frames are integrated to obtain the watermarked video.

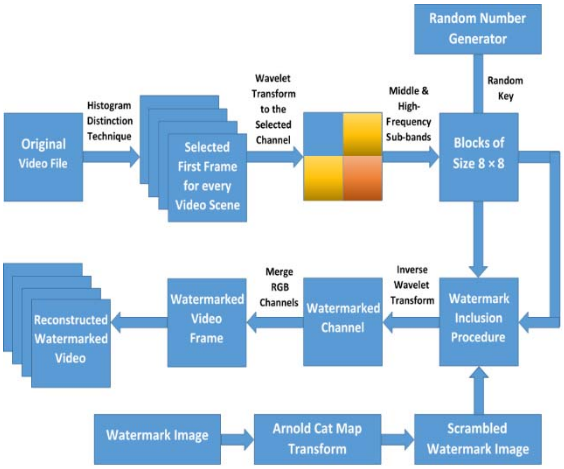

Random Number Generator
Random Key
Original Video File
Histogram Distinction Technique
Selected First Frame for every Video Scene
Wavelet Transform to the Selected Channel
Middle & High-Frequency Sub-bands
Blocks of Size 8 × 8
Reconstructed Watermarked Video
Watermarked Video Frame
Merge RGB Channels
Watermarked Channel
Inverse Wavelet Transform
Watermark Inclusion Procedure
Watermark Image
Arnold Cat Map Transform
Scrambled Watermark Image

Figure 6: The watermark inclusion procedure.

4.2 The Procedure of Watermark Extraction

The specifics of the watermark extraction procedure are as follows (see Figure 7 which demonstrates the overall structure of this procedure):

First Step: Select the watermarked video file as an input and convert it into frames.

Second Step: Finding the first different scenes, and for each one selects the channel and decompose it into one level discrete wavelet transform, then extract the middle and high frequency sub-bands, and divide these sub-bands into non-overlapped blocks of size 8*8 pixels.

Third Step: Use the generated random key at the procedure of watermark inclusion as a secret key for extraction to determine the blocks locations that contain the watermarks bits.

Fourth Step: the procedure of extraction is accomplished by finding the average of the first row to the selected watermarked blocks, and in each block, if the first element in the row is less than the average then the value of the embedded Bit is zero, else, the value of the embedded Bit is one.

$$\mathit{Embedded\ bit} \leftarrow 0, \quad \mathit{If} \quad \mathit{First\ element\ in\ the\ Row} < \mathit{Avarage}$$

$$\mathit{Embedded\ bit} \leftarrow 1, \quad \mathit{If} \quad \mathit{First\ element\ in\ the\ Row} \geq \mathit{Avarage}$$

Fifth Step: Finally, apply an inverse Arnold cat transform on the scrambled extracted watermark image by n times to obtain the extracted watermark image.

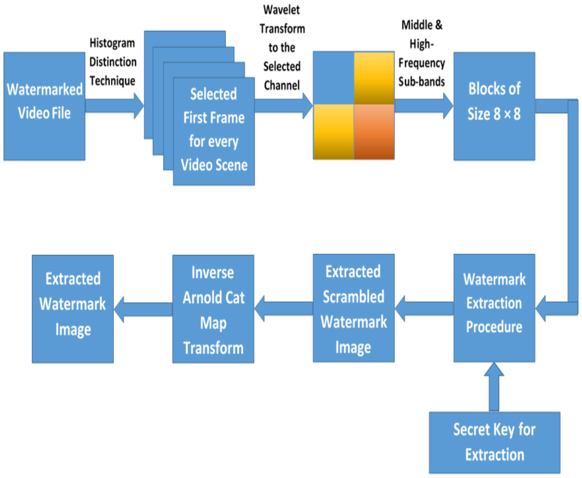
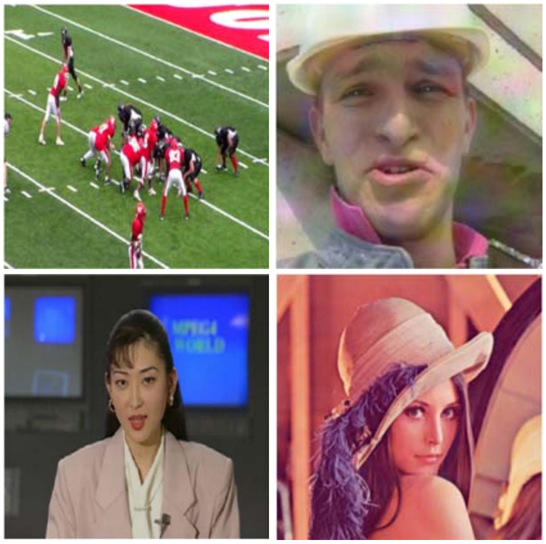

Watermarked Video File
Histogram Distinction Technique
Selected First Frame for every Video Scene
Wavelet Transform to the Selected Channel
Middle & High-Frequency Sub-bands
Blocks of Size 8 × 8
Extracted Watermark Image
Inverse Arnold Cat Map Transform
Extracted Scrambled Watermark Image
Watermark Extraction Procedure
Secret Key for Extraction

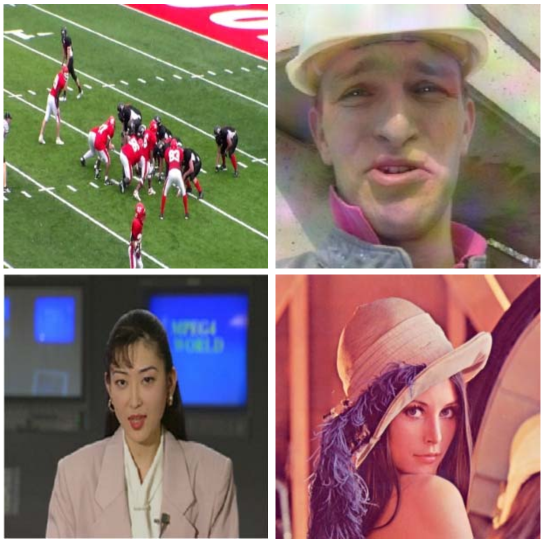
Figure 7: The watermark extraction procedure.

5. THE EXPERIENTIAL ANALYSIS

The proposed scheme is examined with RGB Color Image "Lena.png" and three video files “Football.avi”, “Foremen.avi”, and “Akiyo.avi” encompassing of 140 video frames of size 512 × 512. The binary image "W.bmp" of size 32 × 32 is utilized as a watermark image. Figure 8 demonstrates the original and watermarked samples.



(a) The original video frames, and image.



(b) The watermarked video frames, and image.

Figure 8: The original and watermarked samples.

The performance of the proposed scheme is undergone in term of Peak Signal to Noise Ratio (PSNR) for measuring the perceptual quality for the video frames. The higher PSNR value refers to the higher perceptual quality of video watermarking. The PSNR formula is given in Equation 1:

$$PSNR = 20\log_{10}\left(\frac{Value\ of\ Largest\ pixel\ in\ an\ Image}{\sqrt{Mean\ Square\ Error}}\right) \quad (1)$$

The PSNR values of the video frames samples under different kinds of attacks “Salt and Pepper Noise, Gaussian Noise, Histogram Equalization, Gaussian Low Pass Filter 3*3, Intensity Adjustment, and 25% Cropping” are demonstrated in table 1.

Table 1: The PSNR values of the watermarked samples with and without attacks.

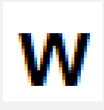
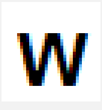
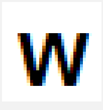
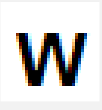
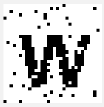
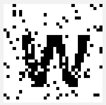
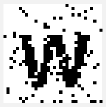
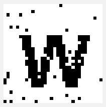
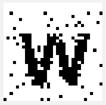
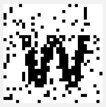
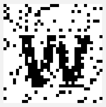
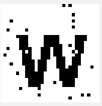
	Football Video Frame	Foreman Video Frame	Akiyo Video Frame	Lena Image
PSNR of Watermarked Frame without Attack	50.9325	60.0233	61.4981	53.0188
PSNR of Watermarked Frame with Salt and Pepper Noise	29.8119	29.9379	29.5417	30.2048
PSNR of Watermarked Frame with Gaussian Noise	34.7494	34.7512	34.9951	34.7014
PSNR of Watermarked Frame with Histogram Equalization	16.9263	22.6842	22.8315	19.2836
PSNR of Watermarked Frame with Gaussian LPF 3*3	41.3345	56.2914	51.1385	43.8366
PSNR of Watermarked Frame with Intensity Adjustment	22.8319	22.5255	23.688	21.9628
PSNR of Watermarked Frame with 25% Cropping	19.1797	16.0825	17.704	19.2711

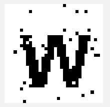
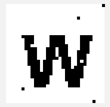
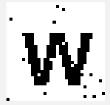
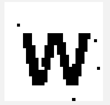
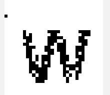
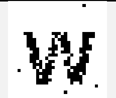
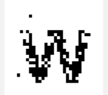
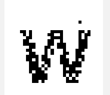
The term of Normalized Cross-Correlation (NCC) is utilized for measuring the watermark robustness, Where the peak value of NCC is equal to One. The NCC formula is given in Equation 2:

$$NCC = \frac{\sum_{x=1}^{x=m-1}\sum_{y=1}^{y=m-1} W(x,y)\cdot W'(x,y)}{\sqrt{\sum_{x=1}^{x=m-1}\sum_{y=1}^{y=m-1}(W(x,y))^2}\cdot\sqrt{\sum_{x=1}^{x=m-1}\sum_{y=1}^{y=m-1}(W'(x,y))^2}} \quad (2)$$

Where $W(x,y)$ is the values of the original watermark image, and $W'(x,y)$ is the values of the extracted watermark image. Table 2 demonstrates the extracted watermark image under different kinds of attacks with the NCC values.

Table 2: The extracted watermark image under different kinds of attacks and the NCC values.

	Football Video Frame	Foreman Video Frame	Akiyo Video Frame	Lena Image
Extracted Watermark without Attack				
NCC	1	1	1	1
Extracted Watermark with Salt & Pepper Noise				
NCC	0.966317	0.93788	0.949143	0.97614
Extracted Watermark with Gaussian Noise				
NCC	0.962455	0.918891	0.911068	0.985354

Extracted Watermark with Histogram Equalization				
NCC	0.982896	0.995143	0.989043	0.99636
Extracted Watermark with Gaussian LPF 3*3				
NCC	1	1	1	1
Extracted Watermark with Intensity Adjustment				
NCC	1	1	1	1
Extracted Watermark with 25% Cropping				
NCC	0.972056	0.97356	0.969763	0.974295

6. CONCLUSION

In this work, a secure, robust and imperceptible "RGB uncompressed AVI" digital video watermarking scheme based on wavelet transform is proposed. The coefficients of the middle and high frequency sub-bands are modified by watermark image bits'. The high degrees of PSNR exhibited that the perceptual quality of the video frames after the inclusion procedure is very good (PSNR values of the samples; Football, Foreman and Akiyo video frames, and Lena image are up to 50.9325, 60.0233, 61.4981, 53.0188 respectively). Also, the high values of the normalized cross-correlation for the extracted watermark under different kinds of attacks exhibit a good watermark recovery. Finally, we concluded that the embedding and inclusion procedures for the proposed scheme are well designed. Accordingly, this scheme is appropriate to be used in the application of real-world digital video watermarking.

REFERENCES:

[1] Divjot Kaur T., Sonika J., “A Semi Blind DWT-SVD Video Watermarking”, Procedia Computer Science, Vol. 46, 2015, PP. 1661-1667.

[2] Sanjana S., Prajnat B., Swarnali P., Ankul J., Dipak K., Aruna C., “Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis”, International Journal of Wisdom Based Computing, Vol. 1, No. 2, 2011, PP. 7-11.

[3] M. A. Chimanna and S. R. Khot, "Robustness of video watermarking against various attacks using Wavelet Transform techniques and Principle Component Analysis," 2013 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2013, pp. 613-618.

[4] Bhavna Goel and C. Agarwal, "An optimized un-compressed video watermarking scheme based on SVD and DWT," 2013 Sixth International Conference on Contemporary Computing (IC3), Noida, 2013, pp. 307-312.

[5] P. Agarwal, A. Kumar and A. Choudhary, "A secure and reliable video watermarking technique," 2015 International Conference on Computer and Computational Sciences (ICCCS), Noida, 2015, pp. 151-156.

[6] C. V. Narasimhulu, "A robust hybrid video watermarking algorithm using NSCT and SVD," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1495-1501.

[7] Anjaneyulu Sake, and Ramashri Tirumala, “Bi-orthogonal Wavelet Transform Based Video Watermarking Using Optimization Techniques”, Materials Today: Proceedings, Vol. 5, 2018, pp. 1470-1477.

[8] Osama S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain”, AEU - International Journal of Electronics and Communications, Vol. 67, No. 3, March 2013, PP. 189-196.

[9] Rade Petrovic and Venkatraman Atti. Watermark based access control to copyrighted content. In 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), volume 1, pages 315–322. IEEE, 2013.

[10] Alfonso Iacovazzi, Sanat Sarda, Daniel Frassinelli, and Yuval Elovici. Dropwat: an invisible network flow watermark for data exfiltration traceback. IEEE Transactions on Information Forensics and Security, 13(5):1139–1154, 2018.

[11] Jana Dittmann, Anirban Mukherjee, and Martin Steinebach. Media-independent watermarking classification and the need for combining digital video and audio watermarking for media authentication. In Proceedings International Conference on Information Technology: Coding and Computing (Cat. No. PR00540), pages 62–67. IEEE, 2000.

[12] Ma Zhaofeng, Huang Weihua, and Gao Hongmin. A new blockchain-based trusted drm scheme for built-in content protection.

EURASIP Journal on Image and Video Processing, 2018(1):91, 2018.

[13] Sibaji Gaj, Shuvendu Rana, Arijit Sur, and Prabin Kumar Bora. A drift compensated reversible watermarking scheme for h. 265/hevc. In 2016 IEEE 18th International Workshop on Multimedia Signal Processing (MMSP), pages 1–6. IEEE, 2016.

[14] Ton Kalker et al. A security risk for publicly available watermark detectors. In SYMPOSIUM ON INFORMATION THEORY IN THE BENELUX, pages 119–126. Citeseer, 1998.

[15] Dan Yu, Farook Sattar, and Kai-Kuang Ma. Watermark detection and extraction using independent component analysis method. EURASIP Journal on Advances in Signal Processing, 2002(1):523219, 2002.

[16] Saraju P Mohanty, KR Ramakrishnan, and Mohan Kankanhalli. A dual watermarking technique for images. In Proceedings of the seventh ACM international conference on Multimedia (Part 2), pages 49–51. Citeseer, 1999.

[17] Xiao-LongLiu,Chia-ChenLin,andShyan-MingYuan.Blinddualwatermarkingforcolorimages'authentication and copyright protection. IEEE Transactions on Circuits and Systems for Video Technology, 28(5):1047–1055, 2018.

[18] Mohammad Abdullatif, Akram M Zeki, Jalel Chebil, and Teddy Surya Gunawan. Properties of digital image watermarking. In 2013 IEEE 9th international colloquium on signal processing and its applications, pages 235–240. IEEE, 2013.

[19] Arezou Soltani Panah, Ron Van Schyndel, Timos Sellis, and Elisa Bertino. On the properties of non-media digital watermarking: a review of state of the art techniques. IEEE Access, 4:2670–2704, 2016.

[20] Tanima Dutta and Hari Prabhat Gupta. An efficient framework for compressed domain watermarking in p frames of high-efficiency video coding (hevc)–encoded video. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 13(1):12, 2017.

[21] Martin Kutter and Fabien AP Petitcolas. Fair benchmark for image watermarking systems. In Security and Watermarking of Multimedia Contents, volume 3657, pages 226–240. International Society for Optics and Photonics, 1999.

[22] Thomas M Cover. Elements of information theory, second edition.

[23] Kalyan Das, Jiming Jiang, JNK Rao, et al. Mean squared error of empirical predictor. The Annals of Statistics, 32(2):818–840, 2004.

[24] AG Asuero, A Sayago, and AG Gonzalez. The correlation coefficient: An overview. Critical reviews in analytical chemistry, 36(1):41–59, 2006.

[25] Muhammad Bilal Zafar, Isabel Valera, Manuel Gomez Rodriguez, and Krishna P Gummadi. Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment. In Proceedings of the 26th International Conference on World Wide Web, pages 1171–1180. International World Wide Web Conferences Steering Committee, 2017.

[26] Margaret Sullivan Pepe, Tianxi Cai, and Gary Longton. Combining predictors for classification using the area under the receiver operating characteristic curve. Biometrics, 62(1):221–229, 2006.

[27] Ming Sun Fu and Oscar C Au. A robust public watermark for halftone images. In 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353), volume 3, pages III–III. IEEE, 2002.

[28] Wei-Lun Chao. Comparison of video copy detection techniques: The robustness against distortion and attacking. Technical Paper, Graduate Institute of Communication Engineering, National Taiwan University, 2009.

[29] P. H. W. Wong and O. C. Au. A novel semi-private watermarking technique. In 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), volume 3, pages III–III, May 2002.

[30] Ron G Van Schyndel, Andrew Z Tirkel, and Imants D Svalbe. Key independent watermark detection. In Proceedings IEEE International Conference on Multimedia Computing and Systems, volume 1, pages 580–585. ieee, 1999.

[31] Yunxia Liu, Shuyang Liu, Hongguo Zhao, and Si Liu. A new data hiding method for h.265/hevc video streams without intra-frame distortion drift. Multimedia Tools and Applications, Jul 2018.

[32] F. Ahmed and S. My. A hybrid- watermarking scheme for asymmetric and symmetric watermark extraction. In 2005 Pakistan Section Multitopic Conference, pages 1–6, Dec 2005.

[33] Fabien A. P. Petitcolas. Kerckhoffs' Principle, pages 675–675. Springer US, Boston, MA, 2011.

[34] Chuan Qin, Ping Ji, Xinpeng Zhang, Jing Dong, and Jinwei Wang. Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Processing, 138:280–293, 2017.

[35] Gagandeep Kaur, Singara Singh Kasana, and M. K. Sharma. An efficient authentication scheme for high efficiency video coding/h.265. Multimedia Tools and Applications, Mar 2019.

[36] Shabir A Parah, Javaid A Sheikh, Nazir A Loan, and Ghulam M Bhat. Robust and blind watermarking technique in dct domain using inter-block coefficient differencing. Digital Signal Processing, 53:11–24, 2016.

[37] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. Attacks on copyright marking systems. Information Hiding Lecture Notes in Computer Science, page 218–238, 1998.

[38] F.a.p. Petitcolas. Watermarking schemes evaluation. IEEE Signal Processing Magazine, 17(5):58–64, 2000.

[39] Michael E Whitman and Herbert J Mattord. Principles of information security. Cengage Learning, 2011.

[40] Frank Hartung and Martin Kutter. Multimedia watermarking techniques. Proceedings of the IEEE, 87(7):1079– 1107, 1999.

[41] Steve Czerwinski, Richard Fromm, and Todd Hodes. Digital music distribution and audio watermarking. UCB IS, 219, 2007.

[42] P Lipin´ski. Watermarking software in practical applications. Bulletin of the Polish Academy of Sciences: Technical Sciences, 59(1):21–25, 2011.

[43] Michael Voigt and Christoph Busch. Watermarking 2d-vector data for geographical information systems. In Security and Watermarking of Multimedia Contents IV, volume 4675, pages 621–629. International Society for Optics and Photonics, 2002.

[44] M H. M. Schellekens. Digital watermarks as legal evidence. Digital Evidence and Electronic Signature Law Review, 8, 01 2014.

[45] Fred Cohen. A cryptographic checksum for integrity protection. Computers & Security, 6(6):505–510, 1987.

[46] R Sreejith and S Senthil. A novel tree based method for data hiding and integrity in medical images. In 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), pages 1–4. IEEE, 2017.

[47] Gustavus J Simmons. The prisoners' problem and the subliminal channel. In Advances in Cryptology, pages 51–67. Springer, 1984.

[48] Luca Invernizzi, Christopher Kruegel, and Giovanni Vigna. Message in a bottle: Sailing past censorship. In Proceedings of the 29th Annual Computer Security Applications Conference, pages 39–48. ACM, 2013.

[49] Colin Tankard. Advanced persistent threats and how to monitor and deter them. Network security, 2011(8):16–19, 2011.

[50] Ingemar J Cox, Matthew L Miller, Jeffrey Adam Bloom, and Chris Honsinger. Digital watermarking, volume 53. Springer, 2002.