Investigating the Viability of Digital Watermarking Strategies for Enhanced Intellectual Property Protection.

Dr. Aliyah R. Thompson and Dr. Ethan T. Patel

Dr. Aliyah R. Thompson is affiliated with the School of Electrical and Computer Engineering, University of California, San Diego, CA, USA..

ABSTRACT: *In recent years, the significant growth of computer networks has facilitated the publication of multimedia data such as images, video, audio, etc. Digital images can be easily copied and published in the internet without the owner's consent. There are several ways to prevent these problems; one of these methods is digital watermarking. In these methods, a watermark that can be trade mark, digital signature, and so on is inserted into the image, and the watermarked image is obtained. This image can then be published. Therefore, the image's owner can prove a suspicious image by retrieving the watermark from watermarked image. The main objective of watermarking of digital images is to insert the watermark information in digital content as invisible and usually robust. Digital watermarking consists of two watermark insertion and extraction stages. In insertion stage, watermark is embedded in the host image and the watermarked image is obtained. In the extraction stage, watermark is extracted from the image. There are different classifications for different methods of digital watermarking. This paper studies the basic concepts of watermarking and its classifications, and at the end, common uses of watermarking are discussed.*

KEYWORDS: Steganography, Robust, Fragile, Watermarking System, Watermarking Applications.

INTRODUCTION

People have always been interested in putting up their names on the works they create, to cause people who see the work find a sign of its creator. Some cases of this desire and interest may even be found in ancient paintings and pottery that have signs of their creators as seals or abbreviations. Today, with the advancement of technology and entry of all field to the digital domain, this interest still continues, and in addition the financial incentives and rights have intensified it.

Potential unlimited copying of digital products such as digital images, audios and videos easily and without loss of quality has put material rights of producers at serious risk, and there would be no way to differentiate and distinguish between the producer and its unauthorized copier. One of the primary methods used to protect the rights of the owners of these products was encryption, so that the product was encrypted by the sender (producer), and then the receiver (consumer), knowing the encryption key and method, decrypted and used the data. However, still after the decrypting by authorized users, the

data could be copied illegally, and no measures were taken to protect the data after decryption. Watermarking can be considered as one of the solutions presented in this field independently, or as a complementary method of encryption to protect the rights of digital products and their producers [1].

With the development of digital technologies and their increasingly entrance into the everyday life of people, the need to create such systems to protect the rights of digital products and their producers is more clear. Therefore, in the last decade, watermarking is considered as one of the important research areas in the field of image and signal processing. The amount of papers presented at international conferences and journals in the field of watermarking and its growth in recent years is a proof to this claim [1,2].

In summary, digital watermarking can be defined as hiding a signal that is called watermark, in data such as audio, video and digital video for a variety of purposes and applications. Today, digital watermarking is widely used, and different applications are proposed for it, so as it seems that in the near future, the majority of digital products will be equipped with hidden information which includes information to protect the rights of producers or means to prevent unauthorized copying.

BASIC DEFINITIONS AND CONCEPTS OF WATERMARKIN

With the increased interest of businesses and research institutions in data hiding in recent years in both contexts of steganography and watermarking, different terms have been used in this field. At the beginning of this section, it is tried to express the common and widely used terms in these areas. Then, more specifically, the applications and classification methods of watermarking is discussed from different perspectives[2,3]. It is necessary to note that although all concepts of watermarking can be applied to all digital multimedia products including audio, video, and image, since the purpose of this paper was to protect digital images, in most cases, instead of studying the general conditions for digital products, only requirements for digital images have been studied.

Data Hiding

Data hidden in the digital domain means hiding data in digital products, so that people do not have the ability to understand such data easily. Different branches of data hiding in the digital domain are shown in Figure 1, and will be briefly discussed in the following.

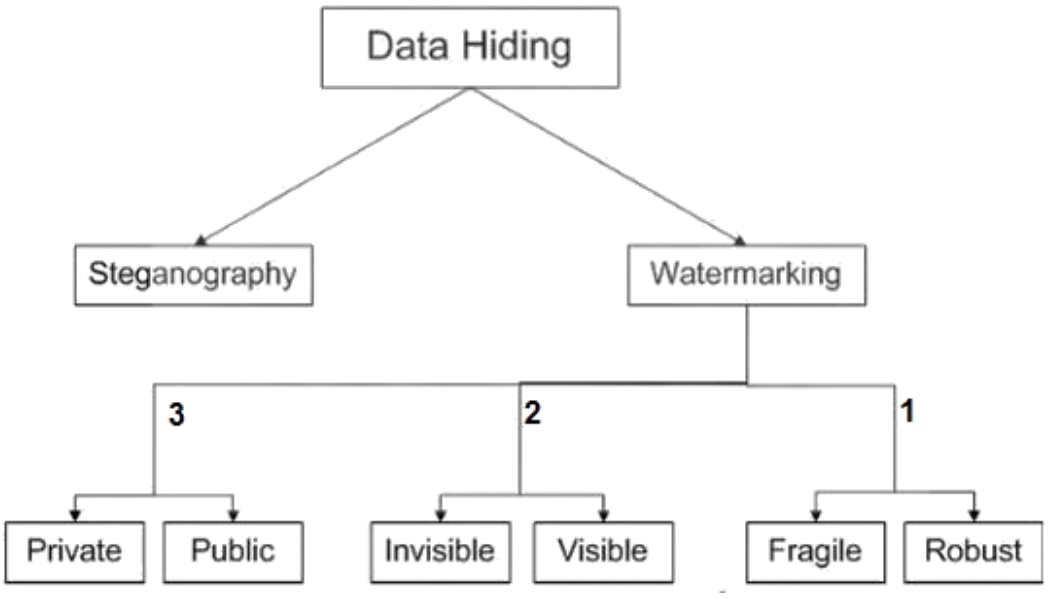

FIGURE 1: Different categories of data hiding.

Steganography

While cryptography encrypts a message so as the enemy cannot understand the content of the message, steganography tries to hide messages in a cover, so as the enemy cannot know about existence of such a message. The roots of steganography is a Greek word meaning "covered writing", and usually refers to methods that are trying to hide a message in other data. Steganography has long been used in the non-digital world, for instance using special characters in a text and using invisible inks are the old methods of steganography [4].

In the digital domain, steganography is one of the categories of data hiding, where the message is hidden in digital data and is sent to the recipient. The purpose of steganography is having a secret connection between the sender and recipient, so that this connection is fully hidden from an enemy. The implementation of a successful attack on these systems requires finding such a connection in the first step, and revealing the hidden messages in the next step. In these systems, the four concepts and terms of Embedded Data, Cover Object, Stego Object and Stego Key are used, which will be discussed in the following[4,5]:

- **Embedded Data:** A message that sender wants to send to the recipient in secret.
- **Cover Object:** Data is used as the cover of main message, i.e. the Embedded Data, and depending on its type, is called Cover Txt, Cover Audio, Cover Image, or Cover Video.
- **Stego Object:** A product that is resulted from the combination of Embedded Data and Cover Object. Depending on the type of the cover data

that is similar to the final production, Stego Object is called Stego Text, Stego Image, Stego Audio and Stego Video.

- **Stego Key:** Steganography Key is a key that limits the possibility of revealing a message from the cover data only to those who know the key or its production parameters.

Watermarking

Watermarking can be general defined as adding data to digital a product (such as audio, video, or digital video) for various applications and purposes, and in particular, hiding data in a digital product in order to maintain the product from unauthorized applications, and in some cases, to prevent tampering and change. Digital watermark signal is an amount of information that is added directly to digital products, so that it is understandable for vision or hearing system in men, but can be detected by the computer. Here, unlike steganography, the objective is not to maintain the hidden message, but to maintain digital products.

GENERAL FRAMEWORK OF WATERMARKING SYSTEMS

Figure2 shows the overall model of a watermarking system. Here, watermarking is considered as the process of combining two pieces of information, that is the original signal (S) and the watermark signal (w), and finally reaching the watermarked signal (Sw), and on the other side, the combined information that were probably under distortion (* SW) pass two filters of human or machine sensory tools and the detector. Ideally, human or machine sensory tools can only understand and receive a piece of information that is similar to the original non-watermarked signal (S*). It can be audio, image or video, and the watermark detector reveals a piece of information that is related to the watermark (w*), that is not necessarily the original watermark signal and depends on the watermarking method robust, so as the greater the watermark robust, the higher the similarity of the detected watermark and original watermark. The general equation (1) can be written for each watermarking system:

$$S_W = S + f(w, s, k) \quad (1)$$

And specifically, equation (2) can be written for digital images watermarking:

$$I_W = I + f(W, I, K) \quad (2)$$

Where I is the original image and Iw is the watermarked image. moreover, K is the watermarking key which in most cases can be attributed to the input parameters of watermarking algorithm, and the detector cannot detect the watermark without knowing them and just with the method used for watermarking, since strong coupling between the original signal and the watermarked signal while watermark in

the original signal is imperceptible is one of the most important common features of watermarking algorithm. The mathematical foundation of more watermarking algorithms is similar to spread spectrum techniques. In this algorithm, by hiding watermark information in important and certain sections of the image, it is tried to meet these two features in the best way[6]. In addition, to make the coupling as robust as possible, while the watermark is invisible and the image quality is maintained, most of these methods are designed so that the properties of human visual system (HVS) are used, while the applied watermark is compatible with the image properties. These goals will be well realized by choosing an appropriate function f (W, I, K). For decision on confirming or rejecting a specific watermark in the image, the usual approach is that first the watermark is detected by the detector, and then the correlation coefficient between the original watermark (w) and detector watermark (w*) is calculated. Depending on one-dimensionality or twodimensionality of the watermark signal, the correlation coefficient can be calculated from equation (3) or (4).

$$Coor(w,w^*) = \frac{\sum_n (w_i - \bar{w})\,(w_i^* - \overline{w^*})}{\sqrt{\left[\sum_n (w_i - \bar{w})^2\right]\left[\sum_n \left(w_i^* - \overline{w^*}\right)^2\right]}} \quad (3)$$

$$Coor(w,w^*) = \frac{\sum_m \sum_n (w_{i,j} - \bar{w})\,(w_{i,j}^* - \overline{w^*})}{\sqrt{\left[\sum_m \sum_n (w_{i,j} - \bar{w})^2\right]\left[\sum_m \sum_n \left(w_{i,j}^* - \overline{w^*}\right)^2\right]}} \quad (4)$$

The correlation coefficient obtained from the equations (3) and (4) is then calculated with a threshold level τ, and if higher, the detector verifies existence of watermark in the image, otherwise the received image is detected without watermark. Different criteria are provided for determining the threshold level τ. however, based on the type of watermarking, the quality of the received images, and the required system security, this threshold can be empirically set with appropriate accuracy. However, it should be noted that in some applications of watermarking, the only objective is to detect the watermark completely, and correlation criteria is not used in these systems [6].

Thus, the general framework of watermarking systems in hiding and detecting the watermark and the final decision making I mentioned. However, the accurate design of these algorithms requires deeper understanding of their features and indicators. The correlation coefficient obtained from the equations (3) and (4) is then calculated with a threshold level τ, and if higher, the detector verifies existence of watermark in the image, otherwise the received image is detected without watermark. Different criteria are provided for determining the threshold level τ. however, based on the type of watermarking, the

quality of the received images, and the required system security, this threshold can be empirically set with appropriate accuracy. However, it should be noted that in some applications of watermarking, the only objective is to detect the watermark completely, and correlation criteria is not used in these systems [6].
Thus, the general framework of watermarking systems in hiding and detecting the watermark and the final decision making I mentioned. However, the accurate design of these algorithms requires deeper understanding of their features and indicators.

CLASSIFICATION OF WATERMARKING METHODS

There are different classifications for different methods of digital watermarking. In this section, three of the classifications will be discussed [1,2,6].

Classification of watermarking methods in terms of watermark resistance

In terms of robust against distortion and manipulation of images, as well as attacks against watermarking systems, watermarking methods can be divided into the following categories:

- **Robust Watermarking:** In these systems, watermarking is performed in such a way that it is not possible to separate watermark and image, and if possible, quality of the product decreases dramatically. In such systems, the objective is that if the product is distorted intentionally or unintentionally, watermark can be detected in the product. It is clear that the watermark in such systems should be placed in important parts of the image.
- **Fragile Watermarking:** In such systems, the watermark is placed in the product in such a way that in case of any change in the image, the watermark will also change. In these systems, by comparing the detected watermark and original watermark, the extent and location of the product changes can be found, and if the watermark is not changed, it can be stated definitely that the product is not changed.
- **Semi Fragile Watermarking:** In some of these systems, algorithm is designed in such a way that watermark is robust to many of the unintentional distortions, and only changes against intentional manipulation. The operation of such systems is called a semi-fragile watermarking. Today, using fragile and semi-fragile watermarking systems, some solutions are provided for digital invoked in courts.

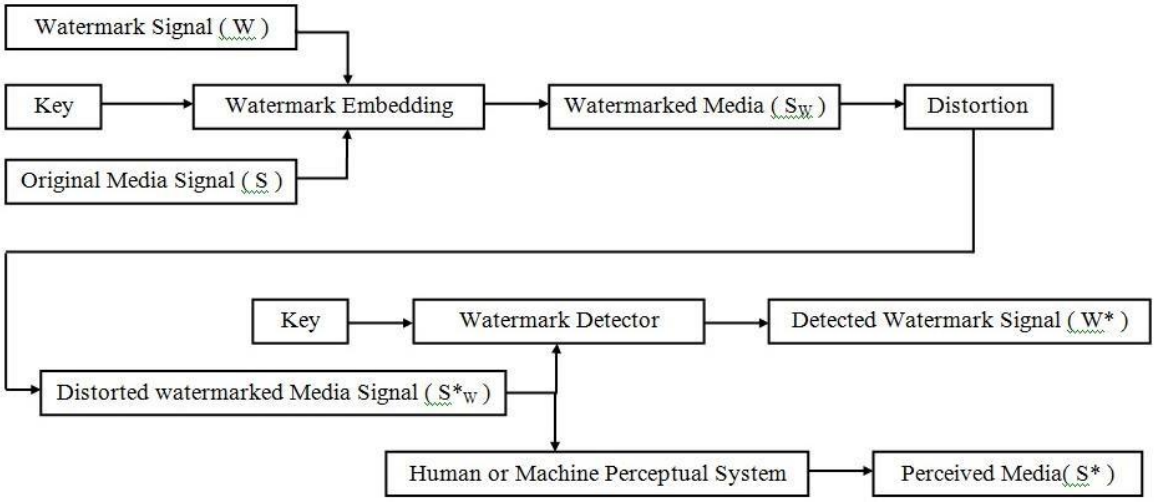

FIGURE 2: The general model of a watermarking system.

Classification of watermarking methods in terms of the type of watermark in image
Watermark in digital products can be visible or invisible. In this term, watermarking methods can be divided into the following categories:

- **Visible Watermarking:** In some applications of watermarking, there is no interest in the full hiding of the added section, and the added digital image or message is visible to all people, such as brands and so on. Such systems are called visible watermarking.
- **Invisible Watermarking:** Most systems used today are trying to hide watermark in digital products in an invisible way. The operation of these systems is called invisible watermarking. The watermark should be placed in the image so as it is invisible to the observer. Also watermark insertion should not result in visible loss of image quality. In most basic watermarking methods, invisibility was considered as an absolute concept, but this ideal state is neither necessary nor desirable in many applications. In fact, given the fact that in majority of cases, the original and watermarked image are not both available to the observer, and only the watermarked images are available, invisibility should not be necessarily ideal, and the only important thing is that the observer be satisfied with the watermarked image quality. Also, it is necessary to note that since in advanced image compression methods, all information that is not detectable by the human eye is discarded, if the watermark added to the image is quite invisible, it may be removed by these compression methods, and not be detectable any longer.

Classification of watermarking methods in terms of the information required to detect the watermark

Watermark in digital products can be visible or invisible. In this term, watermarking methods can be divided into the following categories:

- **Public Watermarking:** This watermarking method which is also called blind watermarking, only need the watermarked image to detect the watermark.
- **Private Watermarking:** This watermarking method which is also called non-blind watermarking, in addition to the watermarked image, need the original non-watermarked image to detect the watermark. Generally, private watermarking methods are more robust against attacks than public watermarking methods, but need more information in the detector.

Classification of watermarking methods in terms of how to insert watermark on an image watermark

Sometimes, different watermarking methods use a fixed way to insert watermark in the image for all cases. However, sometimes parameters of watermark insertion method re changed based on the image specifications. According to this, watermarking methods are divided into the following categories:

- **Non Adaptive Watermarking:** This category of methods use a particular constant way to insert a watermark; that means they use a similar method with fixed parameters to insert a watermark in the image regardless of the image content and its statistical specifications and characteristics.
- **Adaptive Watermarking:** This category of methods that are more intelligent than previous methods analyze the image and some statistical characteristics to create changes in watermark insertion method, and sometimes these changes are fundamental. It is clear that these methods are more robust than previous methods against attacks.

WATERMARKING APPLICATIONS

What is presented in this paper and other articles as watermarking is widely applied in today's digital images and videos. In this section, a brief description of some of these applications is presented [7,8].

Ownership Assertion and Copyright Protection

In this feature, watermarking is used to prove ownership of the product, so that any natural or legal producer of digital product puts his/her own specific watermark in the product. Therefore, copyright for the product can be given to persons that according to the watermark in the product, are its owners, or authorized by the owners of a product.

Fingerprinting for Pirate Tracing

In this feature, watermarking is used to specify receiver or buyer of the products, so as the main owner puts a watermark in any sold product that is specified to a certain customer. The watermark can be a recorded number such as UPC in a compact disc, a text message, or a unique pattern such as a person's DNA. In this case, if any unauthorized copy of the product were discovered, the source of unauthorized copies can be identified, and the violator can be prosecuted.

Image Authentication and Image Integrity Verification

In this feature, watermark is used to verify the authenticity of the image or digital information. Today, digital images are increasingly used as documentary evidence. Furthermore, the increasing development of digital image editing software's and increased expertise of their users prevent detection of forgery or manipulation of images using the human visual system.

In this application, first the sender puts a specific watermark in the image, and the recipient is informed of the content of the watermark. The recipient compares the watermark in the detected product with the original watermark. Then, based on the changes of detected watermark compared to the original one, the extent and location of changes and manipulation in image can be found. This type of watermarking should be performed so that the watermark be robust against unintentional distortion such as compression, low-range filtering, addition of noise, etc. but change rapidly with any change in the image against deliberate manipulation, which, as mentioned earlier, is called semi fragile watermarking.

Usage Control and Copy Protection

Watermark in a product can include information about the application rules, authorized number of copies, and the application location. For example, display location of some digital videos can be restricted to specific areas of the world, or the number of copies a buyer is permitted to make can be limited to a specific number. This application of watermarking requires written rules, standardization, and widespread use in the related industries.

Security in Medical Documents & Content Protection

Insertion of data and medical information about the patient in x-ray images increases medical documentation security. Watermarking has found a good position in this application. Also, if a company intends to distribute free copies of its products, and does not want the product be used by profiteers, it can use visible watermarking and inform the audience about this issue using a special watermark.

CONCLUSIONS

As can be seen, the features listed in this article are all somehow connected. For example, if changes made in the original signal were high, a high-strength algorithm is obtained, but on the other hand, it is most likely to lose image quality. Or as mentioned in the robustness of the algorithm, public watermarking algorithms, in which it is allowed to use the original image on the detector, are generally more robust, since using the original image, they can detect lots of processing, including geometric transformations and reverse them. Or non-robust algorithms are certainly insecure, and will not be robust to distortion and fraud. Thus, according to the interconnection of the different features, algorithm for each application should be designed specific to the needs and characteristics of that application to make a balance between all these features.

REFERENCES

[1] Fridrich, Jessica; M. Goljan and D. Soukal. Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 5306: 70–82, 2004
[2] Ali Akansu and Richard Haddad, Multiresolution Signal Decomposition: Transforms, Subbands, Wavelets, Academic Press, 1992, ISBN 0-12-047140-X
[3] Xie G, Shen H. Toward improved wavelet-based watermarking using the pixel-wise masking model. In: IEEE international conference on image processing (ICIP'05), vol. 1, 2005.
[4] Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008
[5] Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008
[6] Cox I, Miller M, Bloom J. Digital watermarking: principles and practice. Morgan Kaufman; 2001.
[7] Podilchuk C, Delp E. Digital watermarking: algorithms and applications. IEEE Signal Proc Mag 2001;18:33–46.
[8] Tsai J-S, Huang W-B, Kuo Y-H. On the selection of optimal feature region set for robust digital image watermarking. IEEE Trans Image Process 2011;20:735–43