International Journal of Applied Research 2017; 3(4): 128-131

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(4): 128-131
www.allresearchjournal.com
Received: 23-02-2017
Accepted: 25-03-2017

Poonam
Assistant Prof., Maharaja Surajmal Institute of Technology, New Delhi, India

Dr. Shaifali M Arora
Associate Prof., Maharaja Surajmal Institute of Technology, New Delhi, India

Correspondence
Poonam
Assistant Prof., Maharaja Surajmal Institute of Technology, New Delhi, India

Digital watermarking: An introduction

Poonam and Dr. Shaifali M Arora

Abstract
Watermarks are valuable tools for protecting audio, video and data from being copied and distributed with no cost to people across the world over digital network system. This paper provides knowledge of principle, a brief history, importance, and various applications of watermarking. The different key issues like effectiveness, fidelity, payload size and robustness are also discussed in brief.

Keywords: Watermarking, fidelity, watermarking models, blind embedding, informed embedding

Introduction
Digital watermarking is the process of hiding a message, text, logo or signature into any work of media like an image, audio video etc. [1, 2]. Watermarking can be either visible or invisible. Watermarking can be provided to physical objects as well as to electronic signals. Audio, video and images are the most common electronic signals that can be watermarked.
The structure of watermarking constitute two main parts: one is the embedding part and other is detector part. In the embedding part there are two types of inputs, the message we want to encode as a watermark and other is the host in which we want to embed the watermark. The watermark is extracted with the help of detector unit which determines that whether the watermark is present or not. The existence of watermark provides the authenticity of data.
Watermarking techniques may use logos, text information, random numbers [2] etc. The random numbers are often generated by PRN generator.

Brief History
In year 1282, first paper watermark appeared. However, the meaning and purpose of that watermark are uncertain till now [1]. The word watermark was first used at the end of eighteenth century. In 1779, the first bank note forgery was attempted [1]. Counterfeiting prompted advances in watermarking technology. William Congreve, invented a technique for making colour watermarks. Later the banks found that technique difficult to implement. A more practical technology was invented by William Henry Smith. In this a shallow relief sculpture was pressed onto the paper. The resulting variation on the surface of pattern produced watermarks with varying shades of grey.
Digital watermarking gradually evolved until it was accepted. In 1979, Szepanski [1] described a machine detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, researchers described the method of embedding a code in audio signal. In 1988, researchers first used the term digital watermark. By 1990s watermarked products became openly available.

Importance of digital watermarking
Easy access to internet and availability of personal computers has lead to a significant increase in downloading of digital media files like: images, videos, data or any other document. Therefore copying and modifying these media files have become very popular. The illegal copying of some type of media has been a subject of concern form past. As a result, an urgent solution for copyright protection and authentication is needed [1]. Digital watermarking is an effective solution to provide safety to copyright and authentication.
Using digital devices and connecting them over internet, people can record and distribute copyright protected material without return to the legal content owners, nor pay them for their efforts.

Owners of such legitimate property started seeking a method to protect their rights. Cryptography is probably the most common method of protecting digital content. In cryptography products are encrypted before their sale. The person who purchases the product will get a decryption key to access the full product. Once the original product is sold, a pirate can purchase the product, use the decryption key and then can reproduce multiple copies for illegal distribution [8]. So protection of content is required even if it is decrypted.

In digital watermarking, the information is hidden inside the contents. Digital watermarking can survive different kinds of attacks e.g. compression, analog to digital conversion, and file format change etc.

Applications

The various applications of digital watermarking are [3]:

1. **Copyright Protection:** Digital watermarking is used for copyright protection [2]. The watermark information denotes the owner of original product (media).
2. **Copyright Authentication:** Authentication is the process of attemptin to verify the digital identitty of the original document [3]. A dgital watermark can be used to prove that the document content has not been changed. This is achieved by hiding the watermarking information in content that can be retrieved to verify the original data.
3. **Fingerprints and digital signatures:** For monitoring or tracing of illegaly produced copies of data, watermark will record the recipient in each legal sale [3]. The owner or producer of data will place a different watermark in each copy. If it is misused, the owner can discover who created that illegal copy.
4. **Copy protection and device control:** Copy control is intended to protect digital data from illegal copying. This can be achieved by telling recording equipment wahat type of content not to be recorded. Similarly, a digital watermark can be used to enable copy control device.
5. **Broadcast Monitoring:** It is important for broadcast companies to prevent illegal rebroadcasting activities. Digital watermarks can be used to automatically monitor broadcasting streams at satellite nodes all over the world and identify any illegal broadcast material.

Key Issues

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are forced to accept some tradeoffs between these properties depending upon the application of the watermarking system. Some of the key issues related to watermarking system are as listed below [9, 10]:

1. **Effectiveness:** this is perhaps the most important property. This is the probability that the message in a watermarked image will be correctly detected. Ideally this probability is desired to be 1.
2. **Image Fidelity:** Watermarking is a process that alters an original image by adding message to original image. Therefore it affects the image quality. This degradation of image quality must be kept low.
3. **Payload Size:** Every watermarked work is used to carry a message. The size of this message is very important as many systems require a relatively big payload to be embedded in a cover book. There are also many applications that only need a single bit to be embedded.
4. **Robustness:** Robustness is crucial for watermarking system. There are many cases in which watermarked work is altered during its lifespan. A robust watermark should be able to withstand additive Guassian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

Watermarking Models

A watermarking process can be modeled in several ways.

These can be classified broadly in two categories. The first category contains models that are based on communication view of watermarking and the second category contains models based on geometric view of watermarking [4].

A: Communication Based Models

Communication based models describe watermarking in the same way traditional models of a communication system. Watermarking can be seen as a process of communicating a message from the watermarking embedder (transmitter) to the watermarking receiver. Therefore it makes sense to use the models of secure communication to model this process. The communication based watermarking models can further be divided into two sub categories. The first category uses the side information to enhance the process of watermarking and the second does not use any side information.

B: Geometric Models

In this type of watermarking model data, watermarked or unwatermarked, can be viewed as high dimensional vectors. These vectors are termed as media space. For example a 512x512 image would be described as a 262144 elements vector in a 262144 dimensional space.

Geometric models gives better visualization of watermarking process by using a number of regions based on the desirable properties of watermarking. There are mainly two regions of interest. One is the embedding region, which is the region that contains all the possible images resulting from the embedding of a message into the unwatermarked image using some watermark embedding algorithm. The other region is the detection region, which is the region containing all possible images from which a watermark can be successfully extracted using a watermark detection algorithm. The embedding region for a given watermarking system should ideally lie inside the intersection of the detection region and the region of acceptable fidelity, in order to produce successfully detected watermarks that do not alter the image quality very much.

Watermarking without side information

Some communication based models don't take advantage of the channel side information. In this type of models the image is considered as another form of channel noise that distorts the message during its transmission. A standard model for watermarking with no side information is shown in fig.1 [7].

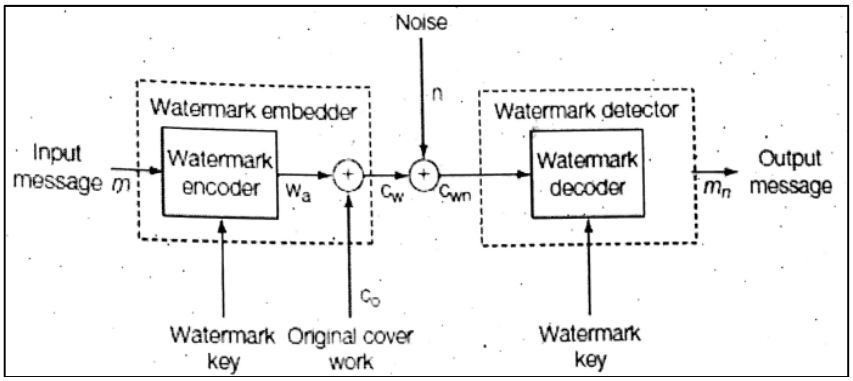

Fig 1: Watermarking model with no side information

The watermark embedder encodes a message using a watermark encoder and a key. This is then added to the original image and transmitted over the communication channel which adds some noise. The watermark detector at the other end receives the noisy watermarked image and tries to decode the original image using the key. Blind embedding is an example of such method. In blind embedding method the original image statistics are not exploited to embed message in the image. The detection is done using linear correlation. This systems embeds only one bit (a 0 or 1) so this is also called a 1-bit watermarking system. The algorithm for embedder and detector is as follows [6]:

Choose a random reference pattern. This is simply an array with the same dimensions as the original image, whose elements are drawn from a random Guassian distribution in the interval $[-1, 1]$. The watermarking key is the seed that is used to initiate the pseudo-random number generator that creates the random reference pattern.

Embedder

1. Calculate a message pattern depending on whether we are embedding a 1 or a 0. Leave the random reference pattern as it is. For a 0 take its negative to get the message pattern.
2. Scale the message pattern by a constant α which is used to control the embedding strength. For higher values of α we have more robust embedding, at the expense of loosing image quality.
3. Add the scaled message patterns to the original image to get watermarked image.

Detector

1. Calculate the linear correlation between the watermarked image that was received and the initial reference pattern that can be recreated using the initial seed which acted as watermark key.
2. Decide what the watermark message was, according to the result of correlation. If the correlation values was above a threshold, we say that the message was 1. If the values are below thresholdwe say that message was 0.

Watermarking with side information

Some limitations in terms of robustness and effectiveness were observed in watermarking systems without any side information system. However these limitations can be overcome with the use of watermarking system that exploits the side information. The general form of watermarking models that uses side information is given in fig.2.

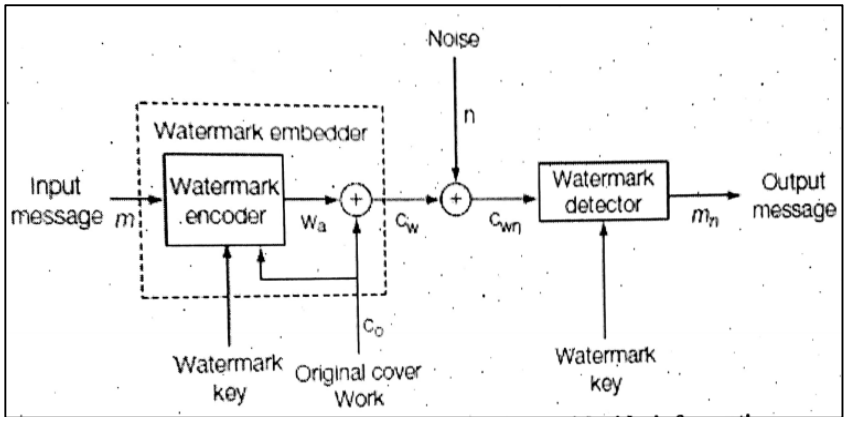

Fig 2: Standard model for watermarking with side information.

The difference between this model and the model described in previous section is the use of the original image. In this method the encoder encodes not only using a key but it also uses the information provided by the original image. The resultant encoded message is then added to the original image as in the case of no side information model. The noisy channel further adds some noise, and then the watermarking detector tries to get the original message back using the original key and a detection algorithm. The algorithm for embedder and detector for this method is as follows [6]:

Embedder

1. Choose a random reference pattern. This is simply an array with the same dimensions as the original image, whose elements are drawn from a random Guaussian distribution in the interval $[1, 1]$. Watermarking key is the seed that is used to initiate the pseudo-random number generator that creates the random reference pattern.
2. Calculate a message pattern depending on whether we are embedding a 1 or a 0. For a 1, leave the random reference pattern as it is. For a 0, take its negative to get the message pattern.
3. Calculate α constant using the linear correlation between the watermarked image and the message pattern. The goal is to ensure that the linear correlation value used for the watermark detection is always some constant, greater than the detection threshold. We substitute this value in the left hand side of the linear correlation equation and solve for α. In this way we get a different value for α for every image.
4. Scale the message pattern by α which is used to control the embedding strength.
5. Add the scaled message pattern to the original image to get the watermarked image.

Detector

1. Calculate the linear correlation between the watermarked image that was received and the initial reference pattern that can be recreated using the initial seed which acted as the watermarking key.
2. Decide what the watermark message was, according to the result of the correlation. If the linear correlation value was above a threshold, we say that the message was a 1. If the linear correlation was below the negative of the threshold we say that the message was a 0. If the linear correlation was between the negative and the positive threshold we say that no message was embedded.

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 paper. Each of these systems has its advantages and disadvantages, and each one trades some important watermarking property for other. The choice of model selection depends on the underlying application's requirements.

References

1. Swanson MD, Zhu B, Tewfik AH. Multiresolution Scene-Based Video Watermarking Using Perceptual Models, IEEE Journal on Selected Areas in Communication. 1998; 16(4):540-550.
2. Cox IJ, Kilian J, Leighton T, Shamoon T. Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institute, Technical Report, 95-10.
3. Xia XG, Boncelet CG, Arce GR. A Multiresolution Watermark for Digital Images, in Proc. of IEEE Int. Conf. Image Processing. 1997; 1:548-511.
4. O'Ruanaidh J, Pun T. Rotation, Scale and Translation Invariant Digital Image Watermarking, in Proc. of IEEE Int. Conf. Image Processing, 1997; 1:536-538.
5. Langelaar GC, Lagendijk RL, Biemond J. Watermarking by DCT Coefficient Removal: A Statistical Approach to Optimal Parameter Settings, in Proc. of SPIE Sym. of Security and Watermarking of Multimedia Contents, 1999, 2-13.
6. Hartung F, Girod B. Fast Public-Key Water-marking of Compressed Video, in Proc. of IEEE Int. Conf. Image Processing, 1997; 1:528-531.
7. Wong PHW, Au OC, Wong JWC. Image Watermarking Using Spread Spectrum Technique in Log-2-Spatio Domain, in Proc. of 2000 IEEE Int. Sym. on Circuits & Systems (ISCAS), 2001; 1:224-227.
8. Lin ET, Delp EJ. A Review of Data Hiding in Digital Images, in Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), 1999, 274-278.
9. Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital Watermarking and Steganography Second Edition. Elsevier, 2008.
10. Costa M. Writing on dirty paper. IEEE Transactions in Information Theory, 1983; 29:439-441.