International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

SURVEY OF DIGITAL WATERMARKING TECHNIQUES AND ITS APPLICATION

Komal M. Lande

Department of MCA SEM VI, YMT College of Management, Institutional Area, Sector -4, Kharghar, Navi Mumbai

---

Abstract:- Digital watermarking hides a digital signal message, such as image, video within the signal itself, in different ways. In this paper, we present a review of Digital Watermarking, different factors used in digital watermarking, properties and their area of application where water and technology must be used. Digital media technology has grown in need of protection when the necessary protection is transferred via the internet or other media.

Proposed based on the wavelet transformation of the embedding and extraction algorithm of the digital image watermark based on the algorithm designed and implemented with the intuitive visual meaning of the binary image, extracting the hidden watermark and filtering, noise algorithm. Use Peak Signal-to-Noise Ratio to evaluate the difference between the original watermark image to quantitatively validate the robustness of the algorithm using standardized cross-correlation to check the similarity of the extracted watermark to the original watermark. The main reason for digital watermarking research development is to protect the digital world's intellectual properties.

Keywords: Digital watermarking, marking, assessment, metric quality, robustness.

INTRODUCTION

Digital marking describes techniques and methods the digital media, such as images, videos or audio, which conceal information such as a number or text. The embedding is done by manipulating digital data conte nt, which mean A information in the data frame is not embedded. The hiding process must be such that changes in media are imperceptible. This means that changes must be invisible for images to the pixel values. Furthermore, depending on the application, Either fragile robust or must be the watermark. By "rugged" means that the watermark's ability to resist media manipulations, such as loss compression (where data is compressed and then decompressed, retrieves data that may well differ from media manipulation). Original, but close enough to be useful in some ways), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering or resist only to a certain degree.

LITERATURE REVIEW

[1] This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a digital watermarking methodology that can be generalized to audio, video, and multimedia data. We introduce new classes of embedding methods, called quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM), and develop convenient modulation realizations. Over the past few years, multimedia watermarking technology has evolved very rapidly. A digital watermark is information that can not be removed imperceptibly and robustly embedded in the host data. We will see how previously proposed methods such as spread-spectrum watermarking has been applied to the wavelet transform domain in a variety of ways and how new concepts such as the wavelet image decomposition's multi-resolution property can be used.

[2] There are two major issues that need to be addressed by watermarking algorithms. First, watermarking schemes are required to provide reliable evidence to protect legitimate ownership. Improvement of performance regarding existing algorithms is achieved through a new approach to masking the watermark according to the characteristics of the human visual system (HVS). It consists of adding an invisible, statistically unobtrusive, and robust, pseudo-noise signal to the video against manipulation.

[3] A digital watermark is an invisible mark embedded in a digital image that can be used for a variety of purposes including image captioning and copyright protection It allows a code for identifying the data creator, owner, authorized consumer, etc. to be closely associated with a digital document. Many electronic watermarks are sensitive to geometric distortions for still images and video content. Simple rotation, scaling, and/or translation (RST) of an image, for example, may prevent a public watermark from blind detection. As an alternative to embedding the location map, we propose a histogram shifting technique. The proposed technique improves the performance of distortion at low capacity of embedding and

mitigates the problem of capacity control. In the context of watermarking, we show the weaknesses of standard image quality measures and propose a new measure adapted to the human visual system

PROPERTIES OF DIGITAL WATERMARKING

1. **Fidelity:**

   The watermark should not be visible to the viewer and the watermark should not degrade the content's quality. We used the term "imperceptible" in earlier work, and this is certainly the ideal. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal.

2. **Robustness:**

   Many types of distortions can occur in music, images and video signals. Lossy compression has been mentioned already, but there are also many other signal transformations. For example, an image may be enhanced by contrast, colours may be somewhat altered or the bass frequencies of the audio signal may be enhanced. In general, transformations involving common signal distortions as well as digital-to-analog and analog-to-digital conversion and loss compression must be robust to a watermark. In addition, it is important that the watermark survives geometric distortions such as translation, scaling and cropping for images and video.

3. **Tamper-resistance:**

   In addition to being robust against the signal distortions that occur in normal processing, watermarks are often required to be resistant to signal processing intended solely to remove them. We refer to this property as being resistant to manipulation. An analytical statement on watermark tamper resistance is desirable. However, due to our limited understanding of human perception, this is extremely difficult, even more so than in cryptography. A successful attack on a watermark must remove the watermark from a signal without altering the signal's perceptual quality. If we had perfect knowledge of how the relevant perceptual process behaved and the computational complexity of such models would be tractable, we could make precise statements about the computational complexity of watermark manipulation. Our present understanding of perception, however, is imperfect, so it is not yet possible to make such precise statements about tamper-resistance.

4. **Key restrictions:**

   The level of restriction placed on the ability to read a watermark is an important distinguishing feature. We describe watermarks in which the key is available, as explained in the previous sections. A very large number of detectors as "unrestricted-key" watermarks and those where keys are kept secret by one or a small number of detectors as watermarks "restricted-key."

5. **Modification and multiple watermarks:**

   It is desirable to change the watermark after insertion in some circumstances. For example, a disk may be watermarked for digital video disks to allow only one copy. Once this copy is made, the watermark on the original disk must be changed in order to prohibit further copies. Changing a watermark can be done by either removing the rst watermark and then adding a new one or inserting a second watermark so that both can be read, but one overrides the other. The first alternative does not interfere with a watermark

6. **Data payload:**

   Basically, a watermark's data payload is the amount of information that it contains. This can be expressed as a number of bits, as with any data storage method, which indicates the number of separate watermarks that could be inserted into a signal. If the watermark carries N bits, different possible watermarks are available for 2N. However, it should be noted that a watermark detector actually returns 2N + 1 possible value, as there is always the possibility that there is no watermark.

7. **Computational cost:**

   The computational costs of inserting and detecting watermarks, as with any technology intended for commercial use, are important. This is especially true if you have to insert or detect watermarks in real-time video or audio

CLASSIFICATION OF DIGITAL WATERMARKING

Depending on different parameters, digital watermarking techniques can be classified in a number of ways. There are different types of watermarking techniques-

Robust & Fragile Watermarking

Robust watermarking is a technique that does not affect the watermark by modifying the watermarked content. Fragile watermarking is a technique where watermark is destroyed by modifying or manipulating watermarked content.

Visible & Transparent Watermarking

Visible watermarks are those that are embedded in visual content in such a way that they are visible when viewing c ontent. Transparent watermarks are imperceptible and ca n not be detected simply by viewing digital content.

Public & Private Watermarking

Users of the content are authorized to detect the watermark in public watermarking while users are not allowed to detect the watermark in private watermarking

Asymmetric & Symmetric Watermarking

Asymmetric watermarking is a technique in which the watermark is used or embedded and detected by different keys. The same keys are used in symmetric watermarking, or watermarks are embeded and detected.

Steganographic & Non–Stenographic watermarking

Stenographic watermarking is used in fingerprinting, whereas non-Stenographic watermarking techniques can be used to deter piracy. Users are aware of the presence of non-stenographic watermarking

WORKING OF DIGITAL WATERMARKING

Typical Digital watermarking system structure consists of three main parts viz. Insertion watermark unit, extraction unit for watermarks and detection unit for watermarks. Thus, the digital watermarking process comprises three processes, i.eInsertion of watermarks, process of extraction of watermarks and process of detection of watermarks. The watermark insertion unit provides the generic approach to watermarking any digital media. Generic approach consists of watermark and watermark detector. There are two inputs to the watermark embedder, i.e. cover work and watermark message, and its output is watermarked work that is input to watermark detector. Then after performing some detector operations, the watermark message will be detected. Insertion unit inputs are the original image (i.e. any digital content), the watermark and the key for obtaining watermarked image. The insertion unit output is an object watermarked. The input to the extraction unit consists of watermarked image and key used during the insertion unit If, since it has been marked and correct key is used, the output of the extraction unit is watermark.[1]

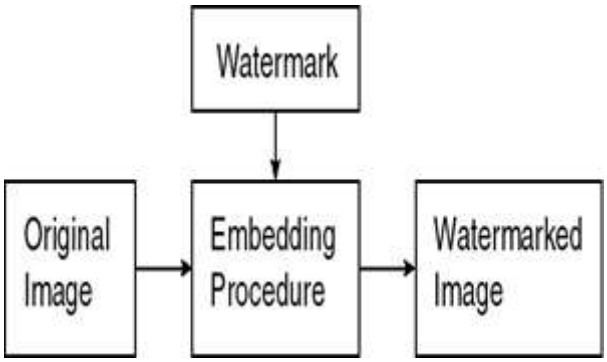

Figure1: Embedding process of image watermarking [1]

METHODOLOGY

The majority of researchers proposed the first LSB (Least Significant Bit) but the proposed watermarking algorithm reverses the watermark text and embeds it in different order in the traditional LSB. First, we select the image that is a gray-scale image and after typing it we will transfer the watermark to binary value. Then we use the proposed algorithm to embed the watermark into the image.

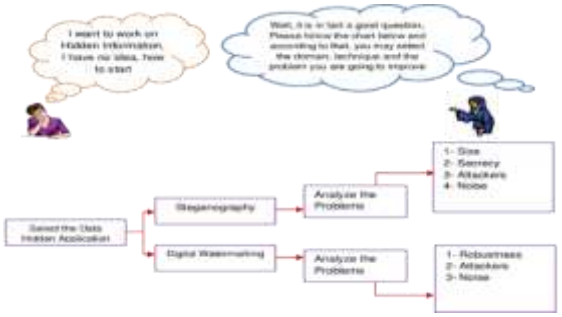

Figure2. Research methodology of doing research in steganography and digital watermarking.[2]

Embedding Algorithm

After we select the image and type the watermark text, we transfer the watermark text to binary values and determine the image coordinates in which the watermark will be embedded. First, we will embed the length of the watermark text in sixteen pixels starting from the first coordinate we select until we embed it in the first LSB in the sixteen pixels. Based on the length of the watermark text, we can know how many copies it will be embedded and if we are going to embed it into the 2nd LSB. Before the watermark is embedded in the 1st LSB image, it will be reversed and we will change the order of embedding. So, if the X coordinate is even, it will subtract 1 from X and if X is odd, it will add 1 to X.

Input:
1- Cover Image
2- Watermark text.

Output:
Watermarked Image

Begin
1- Check the length of the watermark text to know how many copies will be embedded in the first LSB and if it will embed in the second LSB.
2- Embedding the length of the watermark text in the first LSB.
3- convert the watermark text from characters to bits.
4- Inverse the watermark bit.
5- Check the coordinate of X, if it is odd, the algorithm will add 1 to X, and if it is even, the algorithm will subtract 1 from X.
6- Embed the watermark bit in the first LSB.
7- Go to 4 until finishing all the watermark.
8- Go to 4 if we need to embed another copy of the watermark text.
9- Save the Image as bitmap image

End

Figure3- Then, watermarked image will be produced and it will be saved embedding algorithm.[3]

WATERMARKS AND WATERMARK DETECTION

Two types of watermarks can be embedded in an image.

a) Gaussian watermark sequence is a sequence of numbers that contains 1 and-1 and is denoted as a watermark with the same number of 1's and-1's. It is considered a zero-mean and one-variation watermark. Such watermarks are used with a correlation measure to detect original data

b) Binary Image or Grey Scale Image Watermarks: Instead of a pseudo-random Gaussian sequence, some watermarking algorithms embed meaningful data such as logo image. Such watermarks are regarded as watermarks of binary image or watermarks of gray scale. Such watermarks are used to detect original data. A suitable decoder should be used to detect the existing watermark based on the type of watermark embedded.[2]

WATERMARKING APPLICATIONS

The main applications of digital watermarking are presented as:

1. **Copyright Protection***:* Watermarking can be used to protect the redistribution of copyrighted material across untrusted networks such as Internet or peer-to-peer (P2P) networks. Networks with knowledge of content (p2p) might incorporate watermarking technologies to report or filter copyrighted material from such networks.
2. **Content Archiving***:* To help archive digital content such as images, audio or video, watermarking can be used to insert digital object identification or serial number. It can also be used for digital content classification and organization. Their file names normally identify digital contents; however, this is a technique that can easily change file names. The integration of the object identifier into the object itself reduces the possibility of manipulation and can therefore be used effectively in archiving systems.

3. **Meta-data Insertion:** Meta-data is the data describing the data. Images with their content can be labeled and used in search engines. Audio files can contain the singer's lyrics or name. Journalists could insert the cover story of the respective news using photographs of an incident. Medical X-rays can store records of patients.

4. **Broadcast Monitoring:** Write down anything you want. Then press the Quill It button on the right to paraphrase it. Broadcast Monitoring refers to the cross-checking technique of whether or not the content that was supposed to be broadcast (on TV or Radio) was actually broadcast. It is also possible to use watermarking for broadcast monitoring. This has a major application in commercial advertising broadcasting where the advertising entity wishes to monitor whether its advertising was actually broadcast at the right time and for the right duration..

5. **Tamper Detection:** By embedding fragile watermarks, digital content can be detected for manipulation. If the fragile watermark is destroyed or degraded, it indicates the presence of manipulation and therefore can not be trusted in the digital content. For some applications involving highly sensitive data such as satellite imagery or medical imaging, detection of malfunctions is very important. Detection of manipulation is also useful in court where digital images can be used as a

forensic tool to prove whether or not the image is manipulated.

6. **Digital Fingerprinting**: Digital fingerprinting is a technique used to detect digital content ownership. Fingerprints are unique to the digital data owner. A single digital content may therefore have different fingerprints because it relates to different users.[3]

CONCLUSION

There are many ways to hide the protection of data and copyright. Digital watermarking is found to be more intelligible and easier to hide data from the survey. This is also more robust and more capable than the other hiding techniques because of its efficiency. Watermarking focuses on safety by using the method's secret key. Due to cyber crime, the demand for security is increasing day by day. It provides security for images as well as video, text and audio as well. Secure watermarking makes digital data easy and efficient.

REFERENCES

[1] A survey of digital watermarking techiques and its application Lalit Kumar Saini1 , Vishal Shrivastava2

[2] A review of audio-based steganography and digital watermarking M. L. Mat Kiah1, B.B. Zaiden 2,3,4, A.A. Zaidan2,3,4*, A. Mohammed Ahmed1 and Sameer Hasan Al-bakri1

[3] Chen, B., & Wornell, G. W. (2001). Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, *47*(4), 1423-1443.

[4] Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998). A DCT-domain system for robust image watermarking. *Signal processing*, *66*(3), 357-372.

[5] Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L., & Lui, Y. M. (2001). Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on image processing*, *10*(5), 767-782.

[6] Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE transactions on image processing*, *16*(3), 721-730.

[7] Kutter, M., & Petitcolas, F. A. (1999). Fair benchmark for image watermarking systems. *Security and Watermarking of Multimedia Contents*, *3657*, 226-239.