Digital Watermarks for Copyright Protection

Alen Joseph[1], Ambily Sajan[2] , Dr. Dhanya Job[3]

[1,2] PG. Scholar
Department Of Computer Science
Santhigiri College Of Computer Science, Vazhithala
[1]mca2022_alenjoseph@santhigiricollege.com
[2]mca2022_ambilysajan@santhigiricollege.com

[2]Head Of Department
Department Of Computer Science
Santhigiri College Of Computer Science, Vazhithala
dhanyajob@santhigiricollege.com

Abstract: ***Digital watermarking is the process of embedding data to identify its owner or originator. It track the use of digital media and identifies the unauthorized use or access. Digital watermarking is embedding data's in the form of text, video, audio, or images. There are two types of watermark classification- invisible watermark and visible watermark. In invisible watermarking, information is added as digital data to audio, video, and images whose information that are not visible. While visible watermarking, the embedded information is visible in the form of a text or a logo. The data contained in the watermark includes the recipients of each copy so that any information that gets leaked can be traced back very easily. This tracing can be identified with the help of algorithms. Nowadays organizations are developing new digital watermark types in the form of noise. These noises are a type of digital watermark that assigns random data to exist electronic data. We have discussed digital watermarking and its detection towards copyright protection in more detail through this paper.***

Keywords: watermark, detection, algorithm, techniques

1. Introduction

In this current era of technological advancement, the demand for multimedia resources through internet are rapidly increasing. This creates a threat of unauthorized access to these resources. To avoid such unauthorized access the usage of watermarking is necessary. Watermarking is a type of technique where one message is embedded in another. It is mainly used to identify ownership of the copyright and process of hiding digital information. watermark is more or less transparent. The watermarking is represented by a logo or text in any side of an image or video etc. that for protecting the original image from the unauthorized access. We can see the water marks in currency notes, photos, bank checks, videos, bond papers etc. Through this paper we are discussing how this digital watermarking works for copyright protection.

2. Digital Watermarking

Digital watermarking is the process of embedding data called watermark. It can be extracted for ownership verification. Digital watermarking is the insertion of imperceptible and inseparable information into data for data integrity. It actually describes the methods and technologies for hiding the information. The hiding process should take place in the manner that their modifications are imperceptible. They are characterizing patterns, of varying visibility, added to the digital media as a guarantee of authenticity, quality, ownership, and source. Digital Watermarking is a form of steganography which means the message is hidden along with the contents without any public authorities or typical citizens noticing its presence. In digital watermarking the hidden data are visible only with the help of certain electronic devices. These electronic devices can retrieve the embedded message to identify its code.

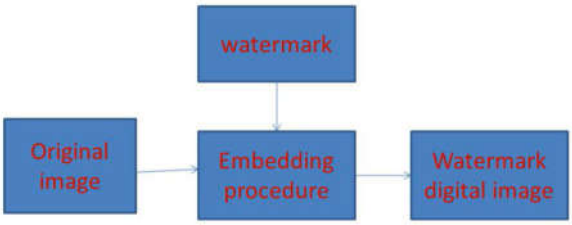


Figure 1: Digital watermarking of an image

2.1 Characteristics of digital watermarking

The basic characteristics of digital watermarking are as follows:

2.1.1 Capacity

It is the optimum amount of data that can be embedded in the given signal.

2.1.2 Robustness

It is the one of the major characteristics of digital watermarking. We embed and retrieve data such that it would survive malicious or accidental attacks.

2.1.3 Security

We ensure that the information embedded has not tampered, forged or even removed.

2.1.4 Transparency

The watermark is not visible under typical viewing conditions. The quality of an image can be measured by using PSNR ratio. This ratio is used as the measurement for quality between the original and compressed image. The higher the PSNR ratio, better will be image quality.

3. Related Works

Brassil et al. [1] have explored various techniques for checking text inside archives with an exceptional paired codeword which serves to distinguish genuine clients of the archive. The codeword is implanted in an archive by making inconspicuous alterations to the construction of the archive, for example, tweak of line width and interword separating just as alteration of character text styles. The presence of the codeword doesn't obviously corrupt the archive yet can be promptly recognized by making a correlation with the first. Standard record giving tasks, for example, copying and filtering don't eliminate the imprint. A similar thought may be reached out to incorporate the insurance of pictures.

Kurak and McHugh [2] have thought about the conceivable use of excess highlights in computerized pictures to the transmission of data. Their anxiety was the transmission of hazardous infections (or 'deception programs') at all critical pieces of an information stream.

They note that just review a picture isn't adequate for distinguishing the presence of some type of defilement. Contingent upon the surface of the picture and the nature of a PC screen, it is conceivable to abuse the restricted unique scope of the natural eye to cover up inferior quality pictures inside different pictures.

Zhao and Koch [3] have explored a methodology to watermarking pictures dependent on the JPEG [lo] picture compression calculation. Their methodology is to divide the picture into single 8 x 8 squares. Here eight coefficients occupy specific positions in the 8 x 8 block. Here square of DCT coefficients can be stamped. These include the low recurrence parts of the picture block, however reject the mean worth coefficient (at facilitate (0, O)) just as the low frequencies at organizes (0, l) and (1, O). Three of the leftover DCT coefficients are chosen utilizing a pseudorandom number generator to pass on data. The likeness of this strategy to recurrence jump spread range interchanges is referenced by the writers [3]. Zhao furthermore, Koch additionally avoid potential risk of setting the impedes aimlessly positions in the picture to make a successful attack from an enemy.

4. History of Watermarking

Watermarking was introduced by Andrew Tirkel and Charley Osborne in December 1992 and the term “water mark” introduced in the end of the 18th century. The first success in water marking is steganographic spread spectrum watermark in 1993 with the help of Gerand Rankin. The watermarks appeared in Italy (paper brand) during the 13th century, but their use rapidly spread on Europe. In 18th century water marking is used as anti-counterfeiting measures on money and other documents to protect copyright. Watermarks on paper in Europe and America has been used for their trademarks in 18th century but now a days we can see the water marks are used in different areas like photos videos audio etc.

5. Digital Watermarking techniques

Watermarking techniques are classified by 4 criteria’s:

1. According to working domain
2. According to the type of document
3. According to the human perception
4. According to application

5.1 According to working domain

5.1.1 Spatial domain

Spatial domain involves direct usage of data to embed and extract Watermark. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colors are separated for printing.

5.1.2 Frequency Domain

This technique is motivated by both perceptual transparency and watermark robustness. This technique is very effective both in terms transparency, robustness to signal processing.

5.2 According to the type of document

According to the type of document it is classified as:

a) Image Watermarking
b) Video Watermarking
c) Audio Watermarking
d) Text Watermarking

5.3 According to the human perception

5.3.1 Visible watermark

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media.

5.3.2 Invisible-Robust watermark

Information is added as digital data to audio, picture, or video, but it cannot be perceived.

5.3.3 Invisible-Fragile watermark

A fragile marking system should be able to detect any changes made in a marked image after marking. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal.

5.4 According to application

5.4.1 source based

Source-based watermark are desirable for ownership identification or authentication where a unique watermark

identifying the owner is introduced to all the copies of a particular image being distributed.

5.4.2 Destination based

In case of destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination-based watermark could be used to trace the buyer in the case of illegal reselling. (EX- FINACLE SOFTWARE BY INFOSYS)
When we talk about the techniques used for digital watermarking, here are the some of the commonly used techniques i.e.; the messages can embed in following domains:

a) Spatial Domain Watermarking

1)LSBs

It is used for confidentiality, authentication and copy right protection. In this paper watermarking is done with the help of least significant bit technique (LSB). As LSB technique is used as it has less effect on image. This new algorithm is using LSB of original image and doing '&&' operation with MSB of watermark image, and same watermarked image is then extracted from host image by replacing its LSB with MSB and making its LSB zeroes, so then watermark is extracted from host image [4].

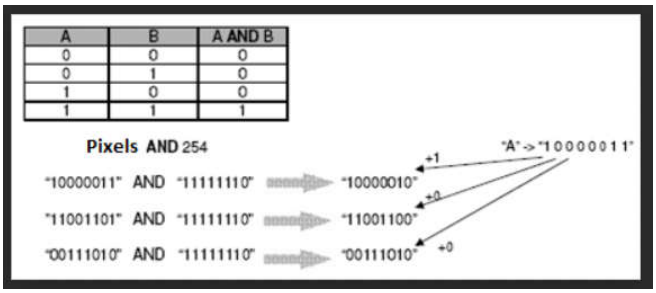


Figure 2: LSB Technique for watermarking

Advantages of LSB includes: Simple and quick Vulnerable to compression, cropping, and some image processing. Can be used for Invisible Fragile Watermark (spatial domain watermarks is that picture cropping (a common operation of image editors) can be used to eliminate the watermark.)

b) Transform Domain Watermarking

Transform domain watermarking techniques are more robust in comparison to spatial domain methods. Transform domain is also called as frequency domain. The watermark message is inserted in the transform domain. Different transforms behave differently to different attacks.
Some of the transform domain watermarking are:

1) DWT
2) DFT
3) DCT
4) FFT

1) DWT (Discrete Wavelet Transform)

Among the transform domain watermarking techniques discrete wavelet transform (DWT) based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform such as progressive and low bit-rate transmission, quality scalability. Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It decomposes a signal into a set of basic functions, called wavelets. Its multi-resolution analysis (MRA) analyzes the signal at different frequencies giving different resolutions. The DWT splits the signal into high and low frequency parts. The low frequency part contains coarse information of signal while high frequency part contains information about the edge components [5]. Watermarking in the DWT domain is composed of two parts: encoding and decoding. In the encoding part, we first decompose an image into several bands with a pyramid structure as shown in Fig:3 and then add a pseudo-random sequence (Gaussian noise) to the largest coefficients which are not located in the lowest resolution, i.e., the corner at the left and top, as follows.

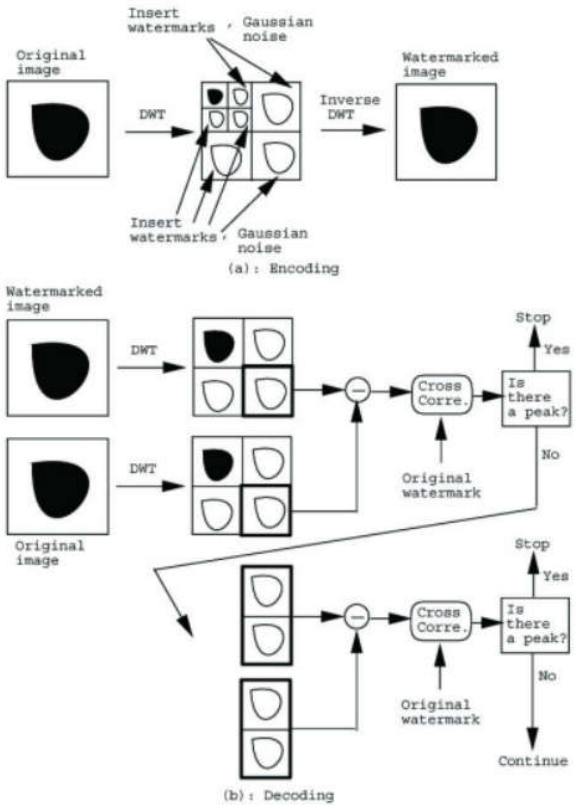


Figure 3: DWT Technique for watermarking

In decoding, we first decompose a received image and the original image (it is assumed that the original image is known) with the DWT into four bands, i.e., low-low (LL 1) band, low-high (LH 1) band, high-low (HL 1) band, and high-high (HH 1) band, respectively. We then compare the signature added in the HH 1 band and the difference of the DWT coefficients in HH 1 bands of the received and the original images by calculating their cross correlations. If there is a peak in the cross correlations, the signature is called detected. Otherwise, compare the signature added in the HH 1 and LH 1 bands with the difference of the DWT coefficients in the HH 1 and LH 1 bands, respectively. If there is a peak, the signature is detected. Otherwise, we consider the signature added in the HL 1, LH 1, and HH 1

bands. If there is still no peak in the cross correlations, we continue to decompose the original and the received signals in the LL 1 band into four additional sub bands LL 2, LH 2, HL 2 and HH 2 and so on until a peak appears in the cross correlations. Otherwise, the signature cannot be detected [6].

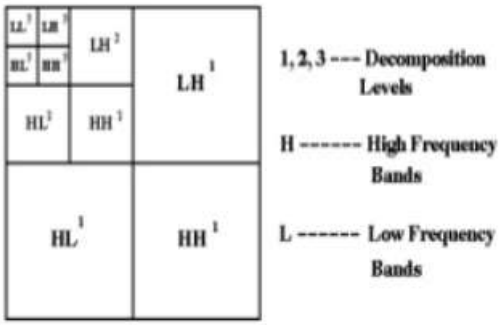


Figure 4: decomposition using DWT Technique

2) DFT (Discrete Fourier Transform)

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients.

3) DCT (Discrete Cosine Transform)

Discrete Cosine Transform is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong energy compaction property and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images [7].

4) FFT (Fast Fourier Transform)

The DFT tool is the primary tool of digital signal processing. The foundation of the signal processing toolbox is the Fast Fourier Transform, a method to compute the DFT with faster execution time. The FFT operates by decomposing an *N* point time domain signal into *N* time domain signals each composed of a single point. The second step is to calculate the *N* frequency spectra corresponding to these *N* time domain signals. Lastly, the *N* spectra are synthesized into a single frequency spectrum.

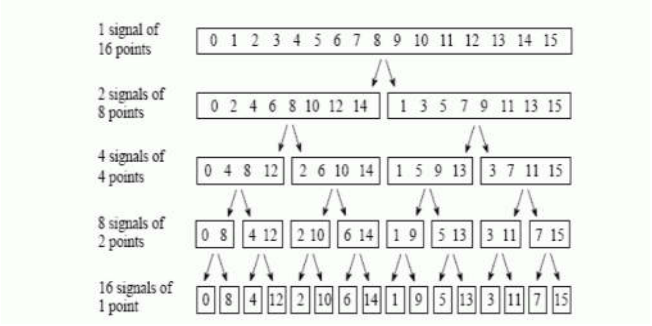
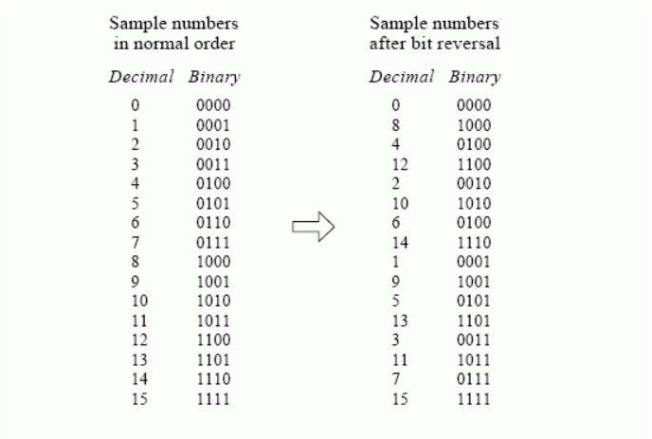


Figure 5: FFT Decomposition

In FFT method, each N signal is decomposed to odd and even samples. A method of interlace decomposition is used to separate odd and even sample signals. Later on it is used for bit reversal order as shown below:



Sample numbers in normal order		Sample numbers after bit reversal	
Decimal	*Binary*	*Decimal*	*Binary*
0	0000	0	0000
1	0001	8	1000
2	0010	4	0100
3	0011	12	1100
4	0100	2	0010
5	0101	10	1010
6	0110	6	0100
7	0111	14	1110
8	1000	1	0001
9	1001	9	1001
10	1010	5	0101
11	1011	13	1101
12	1100	3	0011
13	1101	11	1011
14	1110	7	0111
15	1111	15	1111

Figure 6: FFT bit reversal sorting

5.5 Applications of digital watermarking

Digital watermarking may be used for a wide range of applications, such as:

1) Copyright protection

2) Source tracking (different recipients get differently watermarked content)

3) Broadcast monitoring (television news often contains watermarked video from international agencies)

4) Video authentication

5) Software crippling on screen casting and video editing software programs, to encourage users to purchase the full version to remove it.

6) ID card security

7) Fraud and Tamper detection.

8) Content management on social networks

6. Watermarks for copyright protection

6.1 General Steps in watermarking

The copyright is mainly occurred by taking any information from others information, it may be an image, video, music etc. like this type of issues there is a copy right protection to protect the information. The copyright protection is working like a text or logo representing in any side of image or video.

There is visible and invisible copy right protection. Visible that we can see the logo or text but in the invisible we can't see the logo or text; it is added as digital data. The copywrite is mainly occurring in YouTube, Instagram etc. by taking the photos and videos of others and putting that in another account without the permission of the owner. For example, A and B are 2 different persons A is taking a photo from B's account and putting the photo in A without the permission of B. To prevent this type of problems we can use the digital watermarking. For every watermarking, the original image is firstly encrypted with a sort of encryption algorithm and later watermark is added to the original image using some watermarking algorithm or techniques. And finally, it is identified whether there happened a change in the original image by certain type of attacks like cropping, resizing etc. This could help in someway to protect from copyright.
Normally the basic principle of watermarking goes through the three stages: Generation and embedding, attacks, retrieval/detection. The detailed process is clearly shown in below figure:

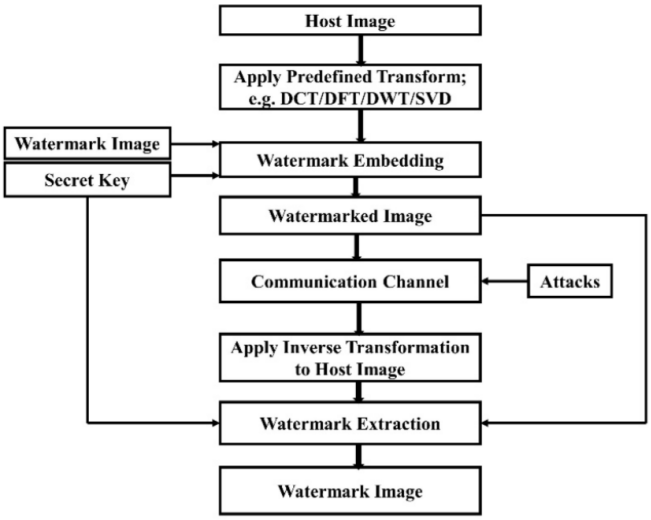


Figure 7: Steps of Watermarking detection

6.2 Digimarc Corporation's ImageBridge Solution

Copyright protection appears to be one of the first applications for which digital watermarking were targeted. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content. An example of one commercial application created for that purpose is Digimarc Corporation's ImageBridge Solution. The ImageBridge watermark detector is made available in a form of plug-ins for many popular image processing solutions such as Adobe PhotoShop or Corel PhotoPaint. When a user opens an image using a Digimark-enabled application, Digimarc's watermark detector will recognize a watermark. It will then contact a remote database using the watermark as a key to find a copyright owner and his contact information. An honest user can use that information to contact the copyright owner to request permission to use the image.

7. Future Scope

Digital watermark is not a complete solution for the copyright protection. There is still security is a concern factor. The challenging problems include the Modeling watermark security, measuring watermark security, Building secure watermark systems. The proposed watermarking scheme can be further improved in many ways and has enormous scope for expansion. Some of the directions for future work are:
1) Development of Hybrid Approaches: Hybrid approaches can be used to enhance the security of watermark against forgery attacks. A dual watermarking scheme based on the combination of geometrically invariant approach with feature-based or block-based approach can be explored for this purpose.
2) Realization of High-Capacity Watermarking Applications: High capacity is required for watermarking applications used for secure media distribution, thumbnail embedding and medical imaging. Therefore, the usability of proposed watermarking system for high-capacity data embedding applications can be further investigated.
3) Rotation Invariant Transforms for Real-time Watermarking Applications: Transforms provide speed advantage, but offer poor reconstruction capabilities. Another research direction can be to explore rotation invariant transforms for real-time watermarking applications.
4)Extensions to Other Digital Media: Although our work mainly focused on gray scale images with possible extensions to color images and video frames as they have similar data representations. Further, through proper transformation 1-D audio signal can also be mapped to 2-D image like signal thus making proposed technique extendible for audio watermarking. But the effects on robustness and visual imperceptibility on different digital contents need further investigation.

8. Conclusion

Digital watermarking is being used in many Industries such as the Digital Multimedia. More enhancements are being under research around the World to provide us with higher information security in the near future. Digital watermarking is a young but rapidly growing technology. Currently watermarking are not robust enough against altering transforms. Whether all the theoretical approach in this field will lead to robust, practical watermarking schemes remains to be seen. This paper is very well-written and easy to understand. The authors made considerable effort to show the landscape of current digital watermarking.

References

[1]BRASSIL, J.? LOW,,& MAXEMCHUK, N., and O'GORMAN,L.: 'Electronic marking and identification techniques to discourage document copying'. Proceedings of INFOCOM 94, 1994
[2]KURAK, C., and McHUGH, J.: 'A cautionary note on image downgrading'. Proceedings 8th Annual Computer Security Applications Conference, San Antonio, 1992 .
[3] ZHAO, J., and KOCH, E.: 'Embedding robust labels into images for copyright protection'. Technical report,

Fraunhofer Institute for Computer Graphics, Darmstadt, Germany, 1994
[4]Anum Javeed Zargar.:Digital Image Watermarking using LSB Technique,'International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014 202 ISSN 2229-5518
[5]DWT-SVD Based Efficient Watermarking Algorithm To Achieve High Robustness and Perceptual Quality Image by Rahul Kodali,Rohan Kamila,Sentu Paul,Supriya Monda,Surit Datta ,Siddhartha Kar
[6]Xiang-Gen Xia, Charles G. Boncelet, Gonzalo R. Arce, "Wavelet transform based watermark for digital images," Opt. Express 3, 497-511 (1998); https://www.osapublishing.org/oe/abstract.cfm?URI=oe-3-12-497

[7]Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform Bhupendra Ram, Member, IEEE, International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 19 ISSN 2278-7763

Author Profile

Alen Joseph completed Bachelor of Computer Application from SSR College, Bangalore in 2017-2020. Currently pursuing Master of Computer Application from Santhigiri college of Computer sciences, Vazhithala in 2020-2022.

Ambily Sajan completed Bachelor of Computer Application from Santhigiri College of computer sciences, Vazhithala during 2017-2020. Currently pursuing Master of Computer Application from Santhigiri college of Computer sciences, Vazhithala in 2020-2022.

Dhanya Job received the M.sc. professional degree and Ph.D in Computer Science. Currently working as HOD of Computer Science Department in Santhigiri College of Computer Sciences, Vazhithala.