



Ministry of Higher Education
And Scientific Research
University of Qadisiyah
College of Computer Science
And Information Technology
Computer Department

Watermark On Integer Wavelet Transform

A project Report Submitted to the college computer science and
information technology – university of Qadisiyah

It is part of the requirement of the BSc degree in computer
science

students ■

Zahraa Sahel Abed ○

Amna Abdullah Wanas ○

Noor Rahy Abed ○

Under the supervision of ○

Dr. Rana Juma ■

—

يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا قِيلَ لَكُمْ
تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا
يَفْسَحَ اللَّهُ لَكُمْ^ط وَإِذَا قِيلَ انشُرُوا
فَانشُرُوا يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا
مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ^ج
وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ (١١)

"صدق الله العلي العظيم"

الآية المجادلة (١١)

الإهداء

- إلى من تمنيته شمساً اقتربت بإشراقها
.... أمامي صاحب العصر والزمان
- إلى كل من علمني حرفاً والقوة في هذه الدنيا الفانية ومن زلل الصعاب أمامي
..... أبي الغالي-
- إلى من علمتني الصمود مهما تبدلت الظروف وأحسنّت تربيتي وسهرت
الليل من أجلي
..... الحنونة
- إلى النور الذي يضيئ حياتي والسند القوي ومن شاركني حنان أمي
.... إلى أخواني وأخوتي
- إلى الذي مبتسم لحين الشهادة في الحروب ودافع عن الأرض بدون مقابل
.....أبن مرجعتي الغيور
- إلى من كان لي وطناً من بعد أسرتي ومن شاركني حزني وأفراحي
- زملائي وزميلاتي

شكر والتقدير

تتناثر الكلمات حبرا وحبا على صفائح الأوراق ...

لكل من علمني....

ومن أزال غيمة الجهل مرت بها برياح العلم الطيبة ...

ولكل من عاد رسم ملاحمي وتصيح عثراتي ...

(أساتذتي الأفاضل ...)

ما أجمل العيش بين أناس احتضنوا العلم، وعشقوا الحياة...

وتغلبوا على مصائب العلم

(رئيس القسم الدكتور محمد عباس)

كتبت في الأخلاق أحلى عنوان..

واتخذت لك في القلب مكان..

فأكثر الله من أمثالك ...

وأحسن فيما يرضيه أمالك....

(مشرقتي الدكتورة رنا جمعه)

List of Contents

Subject	Page
List of Contents	1
Abstract	2
Chapter ONE :-Introduction	3
1.1-Introduction	4
Chapter Two : Watermarking Basics	6
2.1 Classification of Watermarking	7
2.2 Watermarking Properties	9
2.3Purpose of Watermark	12
2.4 Image Watermarking Algorithms	15
References	17

Abstract :-

The field of digital watermarking has recently seen vast interests cover theoretical study, new technique, attack and analysis. This is due to the fact that over the previous 15 years, the watermarking community has focused on developing and introduce new techniques for watermark embed and detection. Analysis of these techniques leads to methods for trouble and development of countermeasures which then used to discover faults and limitations in applications, encouraging the development of better ones. In this paper, comprehensive overview of digital watermarking are discussed. This includes watermarking properties , algorithms , general model, types, applications and future trends of current implementations. Also introducing a robust multi-resolution watermarking algorithm for copyright protection of digital images. By adapting the watermark signal to the wavelet coefficients, the proposed algorithm is very image adaptive and the watermark signal can be strengthen in the most significant parts of the image . The proposed technique is described and analyzed. The document concludes with future plans of the chosen method in digital watermarking

Chapter One

Introduction

Introduction

1.1-Introduction :-

Multimedia services have witnessed a spectacular progress and growth in recent years. This progress has created an ever increasing need for techniques that can be used to support security issues such as copyright protection, fingerprinting and authentication. So this progress in digital media and digital distribution systems, like Internet and cellular phones, has enabled us to easily access, copy, and modify digital content, like documents, images, audio, and video. Under these circumstances, techniques to protect the copyrights of digital data and to prevent unauthorized duplication or tampering of these data are strongly desired.

Digital watermarking (DW) is a promising method for the copyright protection of digital data , In digital watermarking, an imperceptible signal, referred to as a watermark, it is embedded into multimedia data for various purposes, such as copyright protection, fingerprinting, authentication, etc. The embedding of the watermark usually introduces irreversible distortion, although it may be quite small, in the original data. For applications where the availability of original data are essential, Examples of such applications include multimedia archives, military image processing, and medical image processing for electronic patient records (EPRs) [1][2][3].

Integer Wavelet Transform(IWT): Is an invertible integer _to_ integer wavelet analysis algorithm. too can use the IWT in the application that you want to produce integer, coefficients for integer _encoded signals. Compared with the incessant wavelet transform (CWT) and the discrete wavelet transform (DWT). The IWT in not only computationally faster and more memory _ efficient but too more suitable in loss less data _ compression application . The IWT ability you to reconstruct an integer signal perfectly from the computed integer coefficients.[4]

Chapter Two

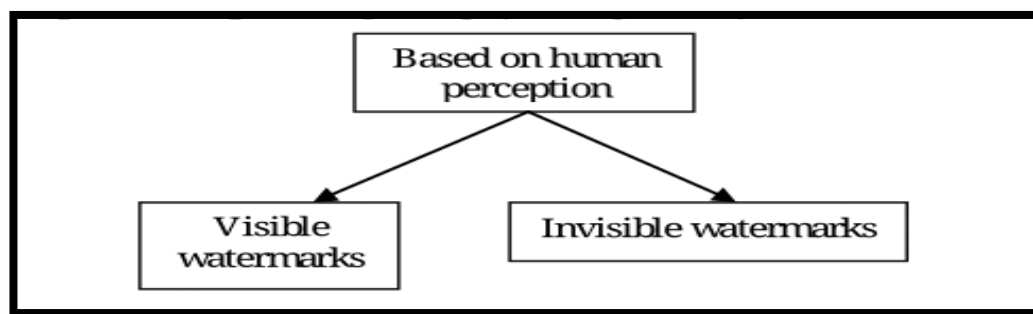
Watermarking Basics

Watermarking Basics

2.1 Classification of Watermarking :

2.1.1 Division Based on Human Perception

This is subdivided into visible watermarks and invisible watermarks.



1. Visible Watermarks :

These watermarks can be seen clearly by the watcher and can also identify the longer or the owner . Visible watermarking technique changes the original single .The watermarked signal is different from the original signal. Visible watermark embedding algorithms are less computationally complex. The watermarked image cannot with exist the signal processing attacks, like the watermark can be cropped from the watermarked image . Spreading the watermark throughout the image is a best option, but the quality of the image is degraded which prevents the image from being used in medical applications.[5]

2. Invisible Watermarks :

These watermarks cannot be seen by the watcher. The output signal does not change much when compared to the original signal.



Figure (1) : shows invisible watermarked image.

The watermarked signal is almost similar to the original signal . As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As the quality of the image does not suffer much, it can be used in almost all the applications .

2.1.2 Division Based on Applications :

- **Fragile Watermarks :**

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked one.

2.1.3 Division Based On Level Of Information Required To Detect The Embedded Data :

based on the level of required information all watermarks are sub-divided into blind watermarks, semi-blind watermarks and non-blind watermarks.

1. Blind Watermarks .

2. Semi-Blind Watermarks :

These watermarks require some special information to detect the embedded data in the watermarked signal.

3. Non-Blind Watermarks :

These watermark require the original signal to detect the embed information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

2.1.4 Based On User's Authorization To Detect The Watermark :

This is sub-divided into public watermarks and private watermarks.

1. Public Watermarks :

In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

2. Private Watermarks :

In this watermarking, the user is not authorized to detect the watermark embed in the original signal.

2.1.5 Division Based on Knowledge of the User on the Presence of the Watermark :

1. Stenographic Watermarking :

The user is not aware of the presence of the watermark.

2. Non-Stenographic Watermarking :

The user is aware of the presence of the watermark.

2.2 Watermarking Properties :-

Defining the properties of watermarking plays an important role in the systematic development of various schemes. For example, in developing a new scheme, the watermarking objectives determine a set of criteria .Each criterion can be expressed in terms of the minimum requirements for a relevant watermarking property. In the design phase, those requirements help characterize the scheme (e.g., by setting constraints for the construction of watermarking functions). In the evaluation phase, measuring (with a suite of tests) how those requirements are fulfilled gives merit to the scheme. The relative importance of each property, thus, can be determined based on the application requirements. This also means that the interpretation and significance of watermarking properties can vary with the application. These properties, in practice, can be interpreted in terms of the inputs and outputs of watermarking components, use of keys, etc. They can also be mutually dependent, which requires a trade-off among the improvements in the properties for an application[6].

In the image watermarking context, a number of defining properties (considering their relative importance) are studied below , They are

**"perceptual similarity, visibility, blindness, ,
, robustness,.**

In the following sections, we formally define these properties using the developed watermarking model and show how they can be interpreted and used in a real application scenario. To simplify reading, from now on, the notations are used without explicitly giving their domains.

For example, ‘for all $a,b,c,\dots$ ’ will be used to mean ‘for all $(a,b,c,\dots) \in A \times B \times C \dots$ ’.

2.2.1 Perceptual similarity :-

The *perceptual similarity* (or *imperceptibility*) is one of the most important properties for the image applications. Since embedding distortion is inevitable, E exploits the (relatively) redundant information of an image intelligently for a minimum of visual artifacts. In almost any image application, therefore, keeping a watermarked image perceptually similar to the original image becomes an important criterion. Perceptual similarity means the perceptual contents of the two images are ‘sufficiently’ similar to each other, (and thus it is mainly studied for the *invisible* watermarking schemes; the ‘visibility’ property is discussed below). The requirements for this property may vary with the application scenario. In order to ease the problem of dealing with these varying requirements, we now define the perceptual similarity property using a quantitative approach.

2.2.2 Visibility :-

A *visible* watermarking scheme deliberately inserts a watermark such that it appears noticeably on the watermarked image to show some necessary information such as company logo, icon, or courtesy. However, in order that the watermark does not become so strongly pronounced that it takes over the main image, the level of visibility can be controlled, for example, by a parameter α . Visible watermarks are important in recognition and support of possessing a digital image. In contrast, an *invisible* watermark is embedded by keeping the perceptual content of the watermarked images similar to that of the original images to address security problems in different application scenarios. Therefore, there are

schemes which are either *visible* or *invisible* based on the appearance of watermark on the watermarked images [7][8][9][10][11].

2.2.3 Blindness :-

Another important watermarking property is *blindness* that helps characterize a scheme to be *blind*, *non-blind*, or *semi-blind*. The term *blindness* (or *oblivious*) is generally used in cryptography to define a detection process independent of any side information. More specifically, blindness is used to define a computational property of information retrieval (e.g., to define the computational independence on the original information or its derivatives to retrieve the required information). Similarly, blindness defines the detection and extraction process in digital watermarking, although there is no complete definition for a watermarking scheme to be *blind* or *non-blind*.

As a requirement for blindness, some schemes consider that no original input image and the information derived from the input image should be required, whereas other schemes consider only avoiding the original input requirement during the detection.

2.2.4 Robustness :-

Robustness in watermarking is often confused with its meaning from cryptography . A main reason is probably that watermarking has to consider some spatial or perceptual properties (e.g., perceptual similarity, visibility). Several attempts have been made to informally define the robustness property of watermarking. For example, Piper and Safavi-Naini considered a watermarking scheme as robust if it can successfully detect the watermark in the ‘processed’ images. The strength of this definition depends on how the ‘processed’ image is defined. In contrast, Cox et al. referred to robustness as the ability to detect the watermark after common signal processing techniques. More specifically, robustness can be defined as the degree of resistance of a watermarking scheme to modifications of the host signal due to either common signal processing techniques or operations devised specifically in order to render the watermark undetectable [12]

2.3 Purpose of Watermark :

A watermark protects digital intellectual possessions, such as photos and artwork, from unauthorized use. It identifies the rightful dishearten own. It is a visible cover of copyright in order (usually in the form of text or an image logo) added to photos or other digital documents. Image processing software programs, such as Photoshop, Paint.Net and Paint Shop Pro make it easy to design and add custom watermarks to photos. Watermarks are, however, not a infallible way of protecting photos or artwork from not permitted use; some people still publish watermarked photos on their websites. While it's hard to stop people from doing so, having a well-placed watermark containing a copyright sign, name and URL of the owner can go a long way to discourage this[13].

digital watermarking is being used in numerous applications , The various types of watermarks can be better described by going through some of the most common (purposes or benefits) of watermarking photos, such as the following :-

1. **Copyright protection** : Digital watermarking can be used to identify and keep copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.
2. **Owner Identification** : The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attacker. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed.
3. **Copy protection** : Digital content can be watermarked to indicate that the digital content cannot be unlawfully replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.
4. **Digital right management** : Digital right management (DRM) can be deified as —the description, identification, trade, protection, monitoring, and tracking of every forms of usages over tangible and intangible assets|. It concerns the management of digital rights and the enforcement of human rights digitally.

5. **Tamper proofing** : Digital watermarks which are fragile in natural world, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.
6. **Broadcast monitoring** : Over the previous few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragment and fast change market, knowing the real broadcast realism has become critical for content owners, copyright holder, distributors and broadcasters.
7. **Access control** : Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some system to have a copy and use control mechanism to prevent illegal copy of the content or limit the number of times of copying. A strong watermark can be used for such purpose.
8. **Medical application** : Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [14].
9. **Image and content authentication** : In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be on lend from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera [15] .
10. **Annotation and privacy control** : Multi-bit watermarking can be use to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other uses of annotation watermarking are electronic ` document indexing and automated information recovery.

11. Media forensics : Forensic watermark applications enhance content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

12. Communication enhancement : Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.

13. Content protection for audio and video subject: Modern digital formats employed for sale or rental of commercial audio and video content to consumers—such as DVD, Blue-Ray Disc, and iTunes—incorporate content protection technology that control access to and use of the content and limit its unauthorized copying and redistribution. Parties looking for to connect in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to get a decrypted copy of the content.

14. Locating content online : The volume of content be uploaded near the web content to produce as we depend more and more on the Internet for information exchange, clients engagement, research and communication. It has also well become a primary selling tool and selling environment, providing an opportunity to showcase our products or services and attract buyer from about the world.

15. Sense of satisfaction : It is so easy to share, copy, and save anything that is published on the Internet. As well, photo sharing websites are as popular as ever. If you plan to post your photos on the Internet, having a watermark on it will give you a sense of satisfaction when you see your photo published for the world to see, branding your name

2.4 Image Watermarking Algorithms :-

The rapidly growing field of digitized images, has urged the need of copyright protection, which can be used to produce evidence against any illegal attempt to either reproduce or manipulate them in order to change their identity. Digital watermarking is a technique providing embedded copyright information in images through using several algorithms . In recently many watermarking algorithms were proposed , the following algorithms are the most common of them :

1. Integer Wavelet Transform (IWT) :

In general wavelet domain allow us to hide facts in regions that the human visual system (HVS) is fewer sensitive to, such as the high restriction detail bands (HL, LH and HH), Hiding data in these area allow us to increase the robustness while maintaining good visual quality. IWT maps an integer data set into another integer data set. In discrete wavelet transform, use wavelet felting contain floating point coefficients can we hide data in their coefficients any truncations of the floating point values of the pixels that must be integers may cause the loss of the hidden information which can lead to the failure of the data hiding system . To avoid problems of floating point correctness of the wavelet filter when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image and in this case there will be no loss of information through forward and converse transform .Due on the mention difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub Band in the folder of IWT paper to be a close copy with smaller size of the original image while in the folder of DWT the resultant LL sub band is distorted. Lifting scheme is one of many techniques that can be used to perform integer wavelet transform it is also the scheme used in this paper. The following is an example showing how we can use lifting scheme to get integer wavelet transform by using simple truncation and without losing inevitability [16][17].

2. Least Significant Bit (LSB) algorithm :

Using Least Significant Bit manipulation, a huge amount of information can be hidden with very little impact to image quality. This technique is performed in the spatial domain. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. Extraction of the watermark is performed by extracting the least significant bit of each of the selected image pixels.

3. Watermarking Based on DFT Amplitude Modulation

In the spatial domain, if the image is shifted a little bit, the watermark extraction process will be disturbed greatly because the pixels will now be translated to different locations. Embedding the watermark in the DFT amplitude of the image overcomes this problem. Due to the periodicity of the image implied by DFT, cyclic translations of the image in the spatial domain do not affect the DFT amplitude. A watermark embedded in this domain is therefore translation invariant. The embedding process consists of selecting which amplitudes to modify to embed the watermark and modifying them in such a way that image quality doesn't degrade.

4. Watermarking Based on DCT Coefficient Modulation

None of the previously mentioned techniques are resilient enough to JPEG compression. This technique embeds the watermark in the DCT domain to increase the robustness of the watermarking scheme against JPEG compression. The idea in this algorithm is very similar to DFT amplitude modulation. The watermark bits are embedded in each 8x8 DCT block of the image.

References

1. R. B. Wolfgang, C. I. Podilchuk, E. J. Help, "Perceptual watermarks for digital images and video," in Proc.of the IEEE, Special Issue Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1108 - 1126, July 1999.
2. X. Xiang-Gen, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital images," in Proc. Of1997 Int. Conf. on Image Processing (ICIP'97), vol. 1, pp. 548-551, 1997.
3. N. Kaewamnerd, K. R. Rao, "Wavelet based image adaptive watermarking scheme," IEE Electronics Letters, vol. 36, no. 4, pp. 312-313, Feb. 2000.
- 4- LabVIEW2010 Advanced Signal Processing Toolkit Help ,June(2010), part number:371419D-01
- 5-*C.M.R.A, GP,Sanghi,GauravChawla , U.I.E.T,RajkumarYadav I nternational Journal of Computer Applications& Information Technology*,Vol. I, Issue II, September 2012 (ISSN: 2278-7720)
- 6-Fridrich J, Goljan M: Comparing robustness of watermarking techniques. In Proceedings of SPIE. SPIE., Bellingham; 1999:214-225.
- 7.Chen B, Wornell GW: Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans. Inform. Theor 2001, 47(4):1423-1443. 10.1109/18.923725
- 8-Barni M, Bartolini F, Piva A: Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans. Image Process 2001, 10(5):783-791. 10.1109/83.918570
- 9-Lin C-Y, Wu M, Bloom JA, Cox IJ, Miller ML, Lui YM: Rotation, scale, and translation resilient watermarking for images. IEEE Trans. Image Process 2001, 10(5):767-782. 10.1109/83.918569
- 10-P Chassery J-M, Macq B, Bas: Geometrically invariant watermarking using feature points. IEEE Trans. Image Process 2002, 11(9):1014-1028. 10.1109/TIP.2002.801587

11-Luo L, Chen Z, Chen M, Zeng X, Xiong Z: Reversible image watermarking using interpolation technique. IEEE Trans. Inform. Forensics Secur 2010, 5(1):187-193.

12-Tefas A, Nikolaidis N, Pitas I: Image Watermarking: Techniques and, Applications (Chapter 22). Academic Press, Boston; 2009.

13-Mei Jiansheng, Li Sukang, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107 .

14-G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow,IEEE, B. Sankur, Member, IEEE "A Review of digital imagewatermarking in health care".

15-Edin Muharemagic and Borko Furht —A Survey of watermarking techniques and applications 2001.

16-S. Lee, C.D. Yoo and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, Sep. 2007, pp. 321-330.

17-M. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan, "Steganography Using BPCS the Integer Wavelet Transformed Image", UCSNS International Journal of Computer Science and Network Security, VOL. 7 No.7, July 2007.