# Discrete wavelet based image watermarking: An idea leads to security

**Keshav S. Rawat**[1], **Sachin Goyal**[2] **and Roopam Gupta**[3]
[1]School of Information Technology, UTD, RGPV, Bhpal, India, Keshav_79699@yahoo.co.in
[2]Department of Information Technology, UIT, RGPV, Bhopal, India, Sachingoyal@rgtu.net
[3]Department of Information Technology, UIT, RGPV, Bhopal, India, roopam@rgtu.net

**Abstract**- Digital watermarking is a multimedia technique recently developed with the purpose of enhancing copyright protection on multimedia files. Watermarking techniques consider multimedia data as a communication channel transmitting owner identification or content integrity information. This paper presents the literature survey on digital watermark features, its classifications and implementation. Various watermarking techniques have been studied in detail in mainly three domains: spatial, discrete cosine transform (DCT) and wavelet (DWT) domain. The work then proceeds with the implementation of basic algorithms for embedding and extraction of watermark in all the domains. In spatial domain, LSB modification algorithm has been implemented and the results have been produced for gray-scale, RGB and YCbCr color domains. For DCT domain, block based approach and for wavelet domain, multi-level wavelet transformation technique and CDMA based approaches is implemented. Resultant watermarked image and extracted watermark for all the approaches are presented in the paper.

## Introduction

Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the Internet, it may sometimes be desirable to use watermarks. Digital watermarking is the processing of combined information into a digital signal. The signal can be audio, image or video, for example. When the signal is copied, then the information is also carried in this copy.

Watermarking [5] is also a sub-discipline of information hiding. The watermarking process is generally applicable to waveform type of information sources.

A watermark is a secondary image, which is overlaid on the primary image, and provides a means of protecting the image.

## 2. Overview of Watermarking

Digital watermarking is defined as information embedded inside chunks of information. Digital watermarking is a technique, which allows an individual to add hidden copyright notices, or other verification messages to digital audio, video or image signals and documents. Such a messages is group of bits describing information pertaining to the signal or to the author of a signal (name, place, etc). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking can be a form of stenography, in which data is hidden in the message without the end user's knowledge.

The content protection mechanism attempt to protect the right of the content creator, distributor and user. The content owner deposits a unique description of the original to a neutral registration authority. This unique description may be hash value or textual description. Now, the registration authority allots a unique identification number to the content and archives these two for future reference. This unique identification number is also conveyed to the contents owner.

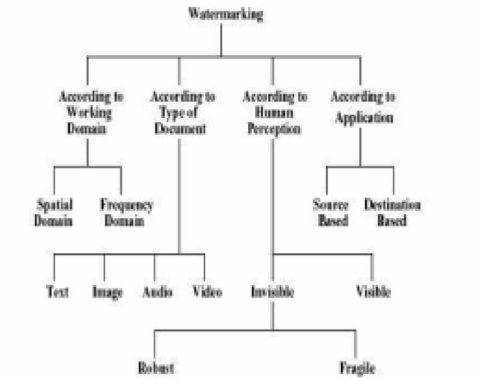

Fig. 1-Types of watermarking.

The content owner derives suitable parameters, usually digital watermarks pertaining to this unique identification number. This digital watermark is securely and secretly merged with original content itself. The digital watermarked content's quality is minimally degraded. As and when required, the content owner can prove the origin of creation by extracting the watermark from the watermarked content.

In addition to secretly embedding a watermark in content, a content owner / distributor can attach a 'label' that is related to a unique identification number. This label is a public notice that informs a user about the intellectual property rights (IPR) of the content.

The second aspect is the secure transportation of copyright protection content over the Internet. This requires a secure channel between two end points for the content transport. Cryptography is an effective solution for secure transport/distribution of copyright protected content. The implementation of a cryptography scheme requires specialized hardware and key management system. Cryptography prevents eavesdropping and manipulation of copyrighted content during transport over the Internet.

## 3. Watermarking classification

Some of the important types of watermarking based on different watermarks [1, 2,5] are given below:

Visible watermarks: Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image. Further, such watermarks are protected against such as statistical analysis.

The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.

**Invisible watermark**: invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and /or author authentication and for detecting unauthorized copier.

**Public watermark**: Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information. They are good alternatives to labels.

**Fragile watermark**: Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made.

**Private watermark**: Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.

**Perceptual watermarks**: A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

There are currently numerous techniques for applying a digital watermark to an image. The techniques can be divided into major categories based on the desired application for the watermark (1) to detect image tampering and (2) to embed copyright information. The classification has shown in figure 1 highlights a number of interesting characteristics of the various watermarking techniques. The techniques used to detect image-tampering tent to be fragile and introduce insignificant data loss. Robust watermark algorithm used to embed copyright data tend to introduce increased visible artifacts, the notable exception are the spread spectrum methods of digital watermarking which are particularly useful for copyright labeling, being both robust and invisible.

## 4. Application

There are various watermarking applications for images, as listed below [2,3,4].

• Copyright protection is probably the most common use of watermarks today. Copyright owner information is embedded in the image in order to prevent others from alleging ownership of the image.

• The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained.

• Prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied. An ironic example in which the use of a watermark might have prevented the wholesale pilfering of an image is in the ubiquitous “Lena” image, which has been used without the original owner’s permission.

• 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.

**• Medical applications**

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.

## 6. Basic Watermarking Principle

The basic idea in watermarking is to add a watermark signal to the host data to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on if the correct cryptographically secure key needed for recovery is used.

There are three main issues in the design of a watermarking system

Design of the watermark signal W to be added to the host signal. Typically, the watermark signal depends on key K and watermark information I.

$W = f_0 (I, K)$

It may also depends on the host data X into which it is embedded

$W = f_0 (I, K, X)$

Design of the embedding method itself that incorporates the watermark signal W into the host data X yielding watermarked data W.

$Y = f_1 (X, W)$

Design of the corresponding extraction method that recovers the watermark information from the signal mixture using the key and with help of the original

$\hat{I} = g (X, Y, K)$

Or without original data

$\hat{I} = g (Y, K)$

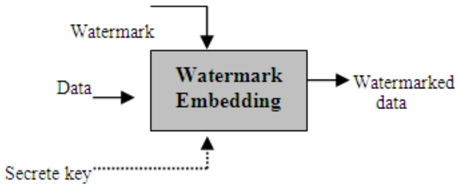

Fig. 2- Watermark embedding scheme.

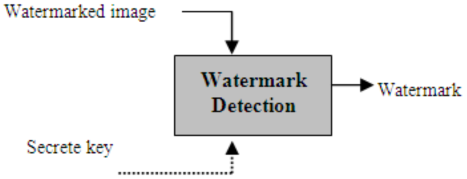

Fig. 3-Watermark detection scheme.

Figure 2 and figure 3 illustrate the concept. Figure 1 shows the generic watermarking scheme for the embedding process. The input to the scheme is the watermark, the host data, and an optional public or secrete key. The host data may depend on the application be uncompressed or compressed, however, most proposed method work on uncovered data. The watermark can be any nature, such as a number, text, or an image.

The secrete or public key is used to enforce security. If the watermark is not to be read by unauthorized parties, a key can be used to protect the watermark. In combination with a secrete or a public key, the watermarking technique are usually referred to as secrete and public watermarking techniques, respectively. The output of the watermarking scheme is the modified, i.e., watermarked data. The generic watermark recovery process is depicted in figure 3. Inputs to the scheme are the watermarked data, the secret or public key and, depending on the original data and the original watermark. The output of the watermark recovery process is either the recovered watermark or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

## 7. Discrete Wavelets Transform

The Discrete Wavelet Transform (DWT)[10] is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [6]. We use the DWT to implement a simple watermarking scheme. The 2-D discrete wavelet transforms (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original; only on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low-pass and high-pass filters of the wavelet transform naturally break a signal into similar (low pass) and discontinuous/rapidly-changing (high-pass) sub-signals. The slow changing aspects of a signal are preserved in the channel with the low-pass filter and the quickly changing parts are kept in the high-pass filter's channel. Therefore we can embed high-energy watermarks in the regions that human vision is less sensitive to, such as the high-resolution detail bands (LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [7]. The fact that the DWT is a multi-scale analysis can be used to the watermarking algorithm's benefit. Multi-resolution is the process of taking a filter's output and putting through another pair of analysis filters. The first approximation will be used as a "seed" image and recursively apply the DWT a second and third time (or however many times it is necessary to perform to find all of the areas of interest)[6]. We can See [9] for more background on wavelets, and [8] for wavelet history.

## 8.Multi-Level Wavelet Transformation Technique

Originating the idea from scalar wavelets, which use only one scaling, and one wavelet, multiwavelets use multiple scaling functions and wavelets. This extends the degree of freedom in constructing wavelets. On contrary to scalar wavelets, properties such as orthogonality, symmetry, vanishing moments, compact support and short support can be gathered in multiwavelets, at the expense of replacing scalars with matrices, scalar functions with vector functions and single matrices with block of matrices [11]-[12]. This technique is based on [13] where the wavelet coefficients of the watermark are embedded to the most significant coefficients at the low and high frequency bands of the discrete wavelet transform of an image.

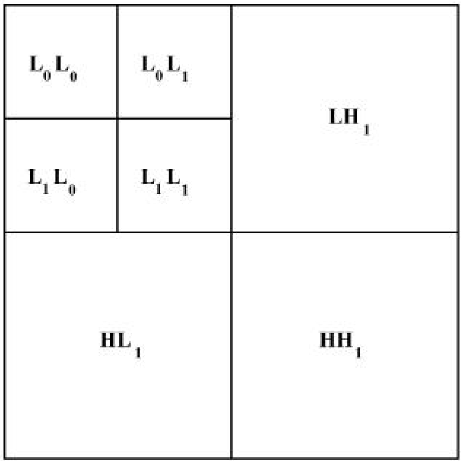

Fig. 4- Multiwavelet sub-bands

### (A) Watermark Embedding Technique

In watermark embedding technique we take an image and resize it into 256X256and then we take a watermark image and resize it into 128X128.now we performing single-level DWT of the original image and performing single-level DWT of the watermark. Then embed the LL1 sub-band of the watermark into LL2 sub-band of the image using the following equation:

$$I'_w = I_w (1+ \alpha *W_w)$$

Where $\alpha$ is a scaling parameter having value between 0 and 1and $I'_w$, $I_w$ and $W_w$ are watermarked, original and watermark images in the wavelet domain. Other three sub-bands HL, LH and HH are embedded using the following equation:

$$I'_w = I_w + \beta* W_w$$

Where $\beta$ is a scaling parameter having value between 0 and 1.Finally we apply 2-level Inverse DWT of the resultant image. This will give us the watermarked image.

### (B) Watermark Extraction Technique

In watermarking extraction technique we take the original image and resize it into 256X256.And take watermarked image. Now we perform two-level DWT of both the images. A coefficient of the LL sub-band of the watermark is extracted by the following equation:

$$W_w = (1/\alpha)(I'_w / I_w - 1)$$

A coefficient of the other three sub-bands of the watermark is extracted by the following equation:

$$W_w = (1/\beta)(I'_w - I_w)$$

These two equations give all the four sub-bands of the watermark image. Finally performing 1-level inverse DWT will give us back the watermark image

## 9. Conclusion

Our study shows that digital watermarking technique is very impressive for image authentication or protection for attacks. Domain technique are good for applications where exact watermark need to be extracted and channel do not consists any noise.

## References

[1] Petitcolas F. A. P., Anderson R.J. and Kuhn M. G. (1999) *Proceedings of the IEEE*, Volume 87, Issue 7, 1062-1078.

[2] Hartung F. and Kutter M. (1999) *Proceedings of the IEEE*, Volume 87, Issue7, 1079-1107.

[3] Hartung F., Kutter M., Stefan Katzenbeisser and Fabien A. P. Petitcolas, (2000) *Information Hiding Techniques for Steganography and Digital watermarking*, Artech House.

[4] Juergen Seitz (2005) *Digital Watermarking for Digital Media*, Information Science Publishing.

[5] http://www.networkmagazineindia.com/200108/security1.htm.

[6] Michael Weeks (2006) *Digital Signal Processing Using MATLAB and Wavelets*, Infinity Science Press.

[7] Langelaar G., Setyawan I. and Lagendijk R. L. (2000) *IEEE Signal Processing Magazine*, Number 17, 20-43.

[8] Stephane Jaffard, Yves Meyer and Robert D. Ryan (2001) *Wavelets Tools for Science and Technology*, Society for Industrial and Applied Mathematics (SIAM).

[9] Stephane Mallat (1989) IEEE Pattern Analysis and Machine Intelligence, Volume 11,Number 7, 674-693.

[10] [10] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University " Watermarking withWavelets: Simplicity Leads to Robustness".

[11] Goudarzi M. M., Taheri A. and Pooyan M. (2004) *Trans. Engin., Computing and Tech.*, vol. 2, pp. 241-244.

[12] Strela V. (1996) Multiwavelets: Theory and Application, Ph.D. Thesis,Massachusetts Institute of Technology, United States.

[13] Taskovski D., Bogdanova S., Bogdanov M. Digital watermarking in weblet Domain ,www.ee.bilkent.edu.tr/~signal/BCSP/taskovski.pdf