Spread spectrum wavelet watermarking system

Michael E. Osadebey and Apostolos A. Georgakis
Dept. Applied Physics and Electronics
Umeå University
SE-90187, Umeå Sweden
e-mail: apostolos.georgakis@tfe.umu.se

ISSN Number: 1652-8441

Report Date: December 26, 2005
Abstract

Lately attention has been focused on wavelet-based watermarking because of its compatibility with the newly developed JPEG 2000 image compression scheme. The major setback associated with wavelet-based watermarking is its vulnerability to geometric distortion caused by the lack of invariance property of wavelet transform. The domain of digital watermarking focused on spread spectrum based technique because of its excellent anti-jamming feature in wireless communication. However existing digital watermarking systems based on spread spectrum technique are yet to replay the anti-jamming feature in wireless communication, hence have not yielded the desired fully robust characteristics. Existing geometric invariant spread spectrum watermarking systems are complex, difficult to implement and unreliable. In our view this is due to inability of researchers to faithfully implement spread spectrum principle. Our investigation showed that most spread spectrum based watermarking faithfully implement the embedding process but fail to despread the signal before detection as required in a typical wireless spread spectrum communication. In this project we propose a simple spread spectrum wavelet watermarking system that is secure, tuneable and fully robust to all known forms and severities of attacks. The novel feature of our watermarking system design is its model as a communication system with the original (host) image representing the communication channel, the watermark represent the message (base band) signal and the legal and malicious attacks represent the noise, interference or jamming of the message signal. Experimental results from our system showed a replay of the excellent anti-jamming feature of spread spectrum communication technique and confirm the superior performance of our system over existing correlation-based spread spectrum wavelet watermarking system.
Contents

1 Introduction .................................................................................. 5
2 Basic watermarking principles .................................................. 8
  2.1 Mathematical formulation ....................................................... 8
3 Review of related work ............................................................... 9
4 Motivation .................................................................................... 10
5 Spread spectrum communication ............................................. 11
  5.1 Spread spectrum communication defined ............................... 11
  5.2 Theory of spread spectrum communication ............................ 11
  5.3 How to spread the spectrum .................................................... 12
  5.4 Random white Gaussian noise ............................................... 12
  5.5 Pseudo-random noise signal ................................................... 13
  5.6 Types of spread spectrum technique ...................................... 13
  5.7 Basic principle of direct sequence spread spectrum - encoding ..... 14
  5.8 Basic principle of direct sequence spread spectrum - synchronized decoding ........................................... 15
  5.9 Basic principle of direct sequence spread spectrum - unsynchronized decoding ........................................ 17
  5.10 Spread spectrum in the presence of interference ...................... 17
  5.11 Why spread the spectrum ..................................................... 18
6 Wavelet transformation ............................................................... 19
  6.1 Wavelet transformation defined .............................................. 19
  6.2 Basis of a vector space, basis vector, basis function and wavelet defined ................................................... 19
  6.3 Wavelet transformation explained ......................................... 19
  6.4 Discrete wavelet transformation ............................................. 21
7 System design: Encoding ............................................................. 23
  7.1 Embedding algorithm introduced ............................................ 23
  7.2 Embedding algorithm ........................................................... 23
  7.3 Simulation of encoding algorithm .......................................... 25
8 System design: Correlator .......................................................... 29
  8.1 Correlation algorithm introduced ......................................... 29
8.2 Uniformly distributed PRN signal or normally distributed PRN signal? ........... 30
9 System design: Comparator ..................................................................................... 32
  9.1 Comparator algorithm introduced ................................................................... 32
  9.2 Comparator algorithm .................................................................................. 33
10 System design: Despreader ................................................................................ 35
  10.1 Simulation of watermarking system ............................................................ 35
  10.2 Analysis of simulation result: First sub bands in first, second and third level .... 35
  10.3 Analysis of simulation result: Second sub bands in second and third level ........ 39
  10.4 Analysis of simulation result: Third sub bands in third level ......................... 39
  10.5 General analysis of simulation result ............................................................ 40
  10.6 The need for a despreader unit ................................................................. 40
11 Test results ........................................................................................................ 43
12 Conclusion ......................................................................................................... 52
# List of Figures

1. Baseband signal before and after spreading ........................................... 12
2. Statistical properties of white Gaussian noise ......................................... 12
3. Autocorrelation function of 1D PRN signal ........................................... 14
4. Types of spread spectrum communication techniques ................................... 14
5. Embedding principle of direct sequence spread spectrum ............................. 15
6. Decoding principle of direct sequence spread spectrum .............................. 16
7. A typical wavelet .................................................................................... 20
8. Scaling and shifting process of discrete wavelet transform ............................ 21
9. Filter bank representations of discrete wavelet transform dilations ................... 22
10. An image and its level decomposition components ........................................ 22
11. Original image and the image of the watermark ........................................... 23
12. One-dimensional watermark signal ......................................................... 24
13. Block diagram for the watermark encoding ............................................... 25
14. Relationship between distortion factor and PSNR of watermarked image for first, second and third level decompositions ........................................... 26
15. The original image, the different degradations of the watermarked images and corresponding distortion factors .......................................................... 27
16. Dual application of the system for watermarking and cryptographic applications .......................................................... 28
17. Graph of one dimensional correlation function obtained by using normally distributed PRN signal .......................................................... 30
18. Graph of one dimensional correlation function obtained by using uniformly distributed PRN signal .......................................................... 31
19. Resultant effect of attacks on a watermark ............................................... 32
20. Variation of maximum PSNR of recovered watermarks with distortion factor for first level wavelet decomposition ................................................... 35
21. Variation of maximum PSNR of recovered watermarks with distortion factor in each sub band for second level wavelet decomposition ................................................... 36
22. Variation of maximum PSNR of recovered watermarks with distortion factor in each sub band for third level wavelet decomposition ................................................... 37
23. Watermarked image ($K = 0.02$) ............................................................ 37
24. Watermarked image ($K = 0.2$) ............................................................ 38
25. Watermarked image ($K = 0.4$) ............................................................ 38
List of Figures

26 Watermarked image ($K = 1.2$) ........................................... 38
27 Watermarked image ($K = 10$) ........................................... 39
28 Watermarked image ($K = 400$) ........................................... 39
29 Attributes of the three sections of the simulation curve for first level wavelet decomposition. .. 40
30 Break up of the simulation curve into two sections to form the encoder and despreader units. ..... 41
31 Block diagram of the watermarking and cryptographic system ........................................... 42
32 Gaussian filtered watermarked image ........................................... 43
33 Average filtered watermarked image ........................................... 43
34 Laplacian filtered watermarked image ........................................... 44
35 $50^\circ$ degree rotated watermarked image ........................................... 44
36 $120^\circ$ rotated watermarked image ........................................... 44
37 $128 \times 128$ resized watermarked image ........................................... 45
38 $200 \times 200$ resized watermarked image ........................................... 45
39 Cropped watermarked image ........................................... 45
40 Multiple attack on watermarked image ........................................... 46
41 $100 \times 100$ resize attack ($K = 1.2$) on watermarked image ........................................... 46
42 $100 \times 100$ resize attack ($K = 30$) on watermarked image ........................................... 47
43 JPEG compressed (5%) watermarked image ........................................... 47
44 JPEG compressed (10%) watermarked image ........................................... 47
45 JPEG compressed (80%) watermarked image ........................................... 48
46 Watermarked image ($K = 0.02$) $T = 10, \rho = 1$ ........................................... 48
47 Watermarked image ($K = 0.02$) $T = 15, \rho = 0.1$ ........................................... 48
48 Gaussian filtered watermarked image ........................................... 49
49 Average filtered watermarked image ........................................... 49
50 Laplacian filtered watermarked image ........................................... 49
51 $50^\circ$ rotated watermarked image ........................................... 50
52 $120^\circ$ rotated watermarked image ........................................... 50
53 $128 \times 128$ resized watermarked image ........................................... 50
54 $200 \times 200$ resized watermarked image ........................................... 51
55 Cropped watermarked image ........................................... 51
1 Introduction

It is a known fact that the digital age had brought with it revolution in the handling, manipulation and transmission of digital multimedia data in all fields of human endeavour such as entertainment, media technology, agriculture, medicine, historical research and academics. Its main positive contributions include ease of authoring, editing and modification, efficient transmission and increased configurability. This positive contribution also brought with it serious negative effect – insecurity of intellectual property rights. The web dictionary [17] defines intellectual property as a term often used to refer generically to property rights created through intellectual and/or discovery efforts of a creator that are generally protectable under patent, trademark, copyright, trade secret, trade dress or other law. Insecure intellectual properties result from the fact that with modern technology multimedia data can be copied with little or no loss in quality and content. In the entertainment industry intellectual properties include manuscripts, lyrics (audio), scripts, and code for a game while in the media industry, it include still images, audio and video that are published works of authors. Usually this intellectual property is the lifeline of the individuals or industries that are rightful owners, and, loss could result in loss of revenue and possible economic collapse. No doubt governments and other established organisations have taken serious steps towards helping individuals and industry protect their intellectual properties. The modes of protection are both legal and technical. In this project work we shall be concerned with the technical form of protection. Technical protection of intellectual property not only protects the rights of rights holders to collect revenue but also verifies the authenticity of the content of their intellectual property.

Protection of intellectual property rights using watermarks date back to the 13th century. Then paper watermarks were used to differentiate paper manufacturers of that time [17]. Digital watermarking is the state-of-the art in technical multimedia content protection. According to Wikipedia web dictionary [25], Digital watermarking is a technique that allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Often associated with watermarking are steganography and cryptography. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Cryptography is the science of writing in secret code and is meant to keep communication private between only two parties while keeping the third party out of communication. Though cryptography, steganography and watermarking are applied to protecting the content of messages and their meaning, their approach is quite distinct. Cryptography approaches the issue by distorting the message as much as possible so that it will be difficult for a third party to read and understand. Both steganography and watermarking conceal the existence of the message. However steganography and watermarking differ by intent of use. While watermark is an attribute of the original image and so contains information such as copyright, licence, tracking (serial) number and authorship, in steganography the embedded message need not be related to the original image. Though a secure intellectual property protection may require at least one of the three applications, watermarking is widely thought of as the last line of defence.

The primary purpose of digital watermarking of multimedia data as outlined in [16] include

1. Copyright protection: information about the source or owner of the data are embedded to prevent other parties from claiming ownership

2. Copy protection in watermarked environment: watermarks are used to control data copying devices and prevent them from copying digital data by indicating that the media is copy-protected.

3. Fingerprinting: information about the authorized recipient of the digital data is embedded on the data. Example is serial number associated with soft ware products. This help the owner of the intellectual property to identify each distributed copy and also trace illegal usage.

4. Image authentication and integrity verification: Modification of digital data can be detected. Example is fragile watermark. Failure to detect the watermark is an indication that the digital data has been modified.
Watermarking systems are classed in [2]. They include

1. Robust watermark, which is designed to resist various signal manipulations
2. Fragile watermarks, designed with low robustness. Can be useful in tamperproof detection and image authentication
3. Public watermark, which can be extracted with known secret key
4. Private watermark, which can only be extracted by a hidden key
5. Non blind watermarking system, that requires the ‘host’ data, and or the original watermark in the decoding process
6. Blind watermarking system, requires neither the original image nor the watermark in the decoding process

Security, non-duplication, imperceptibility, robustness and payload are the five criteria used to assess a digital watermarking system’s ability to protect the ownership of intellectual property. These requirements are explained below

1. Security implies the ability of the watermarking system to detect the watermark and unambiguously prove its authenticity, and does not allow third party to detect the presence of the watermark.
2. Non-duplication: related to security mentioned above, it implies the inability of a third party to introduce another watermark on an already watermarked image so as to avoid ownership tussle.
3. By imperceptibility is meant that the watermark should be embedded such that it is invisible to the human visual system when the ‘host’ image is viewed so that the information conveyed by the host image can be fully perceived. In other words the embedding of the watermark must be such that the distortion suffered by the original image is not detected by the human visual system.
4. Robustness or strength of the watermark is the ability of the watermark to withstand legal and or malicious attacks.
5. Payload of the watermark is the size of information carried by the watermark. It implies the ability of the watermark to carry as much information as possible for the application for which it is intended.

Attacks on watermarks include

1. Lossy compression
2. Geometric distortion
3. Digital –to-analog conversion
4. Resampling
5. Requantization
6. Dithering distortion
7. Recompression
8. Linear filtering
9. Non-linear filtering
In this project we propose a simple spread spectrum wavelet watermarking system that is secure, tuneable and fully robust to all known forms and severities of attacks.

The novel feature of our watermarking system design is its model as a communication system with the original (host) image representing the communication channel, the watermark represent the message (base band) signal and the legal and malicious attacks represent the noise, interference or jamming of the message signal.

The transmission (embedding process) of the base band signal was carried out using direct sequence spread spectrum technique. The spectrum of the foreground bits of digitized image of the watermark signal were spread by successive encoding in the form of uniformly distributed pseudo-random noise (PRN) signal and added to the horizontal and vertical components of the wavelet decomposed host image. PRN signal corresponding to the background bits are generated but are not encoded. The watermarked image is obtained by inverse wavelet transformation.

The receiver (decoding) section consists of tuner (despreader), correlator and comparator units.

The despreader unit generates PRN signals synchronized with that at the embedding stage and successively add a scaled version of the signal to the horizontal and vertical components of the wavelet decomposed watermarked image. The scale of weight is variable but fixed above a threshold value. The despreader performs two functions. It despreads the high frequency watermarked image signal leaving only the watermark signal available to the next stage of the watermarking system - correlator. At same time it spreads the frequency of any form of attacking signal reducing its effect to insignificant level in the watermarked image thereby reversing the effect of any attack on the watermarked image. By varying (tuning) the scales of weight of the PRN signal the system adaptively adjust itself to reverse the effect of all forms and severities of attacks.

The correlator also generates synchronized PRN signal and computes the correlation function between the signal and the horizontal and vertical components of the wavelet decomposed output image of the tuner. Low value will be recorded for PRN signal corresponding to the background bits because there is no corresponding PRN signal in the horizontal and vertical components of the tuned signal. On the contrary, high value will be recorded for PRN signal corresponding to the foreground bits because there is corresponding PRN signal that is spatial-frequency localized in the horizontal and vertical components of the tuned signal.

Changes in the statistics of correlation values in the correlation unit are the result of attacks on watermarked image. To compensate for this the decision threshold of the comparator unit was not fixed as in other correlation based watermarking system but made to be adaptive by discretizing it in steps of the mean of the correlation function.

Experimental results from our system showed a replay of the excellent anti-jamming feature of spread spectrum communication technique and confirm the superior performance of our system over existing correlation-based spread spectrum wavelet watermarking system.

This project work is divided into twelve chapters. The next chapter focus on basic watermarking principles followed by review of related works and motivation. Chapters 5 and 6 discuss spread spectrum communication and wavelet transform followed by the design of the system’s encoder correlator, comparator and tuner. Test results from our system are given in chapter 11. The report ends with discussion, further works and conclusion in chapters 12.
2 Basic watermarking principles

2.1 Mathematical formulation

Any watermarking system can be divided into two subsystems – watermark encoder and watermark decoder [2]. The encoder embeds a watermark to a so-called ‘host’ data such that the watermark signal is unobtrusive and secure in the signal mixture. The decoder recovers the watermark signal from the signal mixture if correct decoding signal is applied to it.

Mathematically a watermarking system can be described by a tuple,

\[ (O, O_{WM}, W_0, W_E, K, E_K, D_K, C_\tau) \] (1)

Where \( O \) is the ‘host’ data, \( O_{WM} \) is the watermarked or possibly manipulated ‘host’ data, \( W_0 \) is the original watermark, \( W_E \) is the extracted watermark, \( K \) is the encoding key, \( E_K \) is the encoding process, \( D_K \) is the decoding process, \( C_\tau \) is the comparator function.

The embedding process has the ‘host’ data, the original watermark and encoding key as input parameters. It is mathematically represented as

\[ E_K : O \times W_0 \times K \rightarrow O_{WM} \] (2)

The decoding process which, depending on the decoding technique, has the watermarked or possibly manipulated ‘host’ data or the ‘host’ data itself, the original watermark and encoding key as input parameters can be mathematically represented as

\[ D_K : O_{WM} \times W_0 \times K \rightarrow W_E \] (3)

\[ C_\tau : W_E \times W_0 \rightarrow \{0, 1\} \] (4)

Eqtn. 4 is a mathematical statement which express the fact that the extracted watermark differs in general from the original watermark due to possible manipulations. Thus the comparator function compares the extracted watermark \( W_E \) with the original watermark \( W_0 \) using the threshold \( \tau \),

\[ C_\tau(W_0, W_E) = \begin{cases} 
1 & c \geq \tau \\
0 & c \leq \tau 
\end{cases} \] (5)
3 Review of related work

The major criteria for assessment of watermarking systems are security, imperceptibility and robustness to attacks. Robustness is the ability of the embedded watermark to withstand legal and malicious attacks.

The most lethal malicious attack is geometric distortion – rotation, scaling and translation. In the literature researchers have proposed methods to increase the robustness of watermarks to geometric attacks. One of such is the Fourier-mellin transform method [22] which achieves this goal by first transforming the host image into a space that has the sought invariants, followed by embedding the watermark and inverse transformation to obtain the watermarked image. Feature-based method [12] achieve this goal by extracting geometric invariant features such as edges or corners from the host image and embed watermark according to these features. Template-based method [18] approaches this issue by inserting a template alongside the watermark into the host image. The function of the template is to estimate the geometric transform suffered by the watermarked image and reverse the effect before detection of watermark is carried out. Autocorrelation function approach restricts the watermark to one with periodic pattern [13] and use the height of the peak of its autocorrelation function to estimate the geometric transform undergone by the watermarked image. Y et another relies entirely on an image registration unit [10] within the watermarking system that use the original watermarked image as base image to restore the attacked image to its original geometric status before detection process.

The last decade attention has been focused on wavelet-based watermarking because of its compatibility with the newly created wavelet-based JPEG 2000 still image compression scheme. Wavelet transform produces a combined localized frequency and time (spatial) resolution than other transform techniques. Also, JPEG 2000 can operate at higher compression ratios without generating the characteristic ‘blocky and blurry’ artifacts of the original DCT-based JPEG standard. However its lack of invariance property makes wavelet-based watermarking vulnerable to attacks such as geometric distortion.

Several watermarking algorithms and watermarking systems that are wavelet-based have been proposed in the field of digital watermarking. Wavelet-based watermarking techniques were classified in [6] according to the embedding strategies. They are

1. Linear additive embedding: Gaussian sequence (pseudo-random noise signal) and image fusion (linear sequence of bits)
2. Non-linear quantization embedding: scalar quantization and vector quantization
3. Miscellaneous embedding techniques: autocorrelation function-based technique

The embedding process in [11] begins with sorting each of the corresponding elements of the detail coefficients (vertical, horizontal and diagonal) of the wavelet transform of the host image in ascending order. This is followed by quantization and embedding of watermark consisting of a plus one or minus one using a randomly generated key according to the mode of quantization, and inverse wavelet transformation to obtain the watermarked image. The watermark recovery process, which requires the original watermark and the key, follows the same procedure of sorting the details coefficients in ascending order. The key is used to search for the location of the watermark. The watermark is assumed detected if the correlation between the extracted watermark and the original watermark is above a pre-defined threshold. The system is rated as highly secure because of the secret key and was shown to be robust to only mean filtering and JPEG compression. Robustness to geometric distortion was not discussed.

A perceptual watermark embedding scheme that searches the perceptually significant wavelet coefficients of the host image and adaptively embed the watermark bits, using different scale of weights, into different sub bands to achieve robustness as well as high perceptual quality was proposed in [23]. The system was, as in the previous system, robust to only linear filtering and compression attacks. Robustness to geometric distortion was not discussed.

Spread spectrum technique has several variants but it typically involves additive embedding of a pseudo-random noise watermark pattern or spreading the frequency of the watermark in the host image. A particular
variant \([21]\) uses a code to generate a different pseudo-random noise pattern for each bit of the watermark, which in turn is embedded onto the spatial or frequency domain of the ‘host’ image. Another variant \([8]\) repeats the watermark bits \(N\) times, where \(N\) is the number of pixels in the host image and \(Q\) is the number of pixels in the image of the watermark. In general, correlation function or filtering methods are used to detect the watermark. This method is robust to common signal processing but not to geometric distortions.

4 Motivation

Some of the watermarking techniques reviewed in the previous section lay claim to robustness to geometric attacks. A close look at the proposal in \([10]\) showed that a new system is created within the watermarking system, and this makes a supposed simple watermarking system become more complex and difficult to implement in practice. The system in \([22]\) had been reported in \([13]\) to be theoretically sound but impracticable. The system in \([13]\) restricts the watermark to one with periodic pattern hence restricting the applicability of the system. The fact that the geometric distortion suffered by the watermarked image is estimated implies that the system cannot be truly reliable.

Performance factors analysis of wavelet-based watermarking methods as carried out in \([26]\) revealed their vulnerability to severe levels of JPEG compression, median filtering and geometrical attacks.

Study of spread spectrum technique as applied to wireless communication show that the despreading process in the decoder unit of the receiver plays a key role in conferring the system with its excellent anti-jamming feature. Review of watermarking systems that implement spread spectrum technique show that none of them faithfully implement spread spectrum as applied to wireless communication. It is therefore no surprise that existing spread spectrum watermarking system cannot replay the excellent anti-jamming feature in the wireless domain.

In this project we are driven by three factors to achieve fully robust and secure watermarking system. They are faithful implementation of spread spectrum technique as applied to wireless communication, the spatial-frequency localization property of wavelet transform and compensation for change in statistics of watermarked image as a result of attacks.
5  Spread spectrum communication

5.1 Spread spectrum communication defined

A web dictionary \[24\] defines spread spectrum communication as: *A form of wireless communications in which the frequency of transmitted signal is deliberately varied. This results in a much greater bandwidth than the signal would have if its frequency were not varied.*

5.2 Theory of spread spectrum communication

Claude Shannon’s information theory states that the channel capacity, \( C \) in bits per second is related to the bandwidth, \( B \) and signal to noise ratio \( \frac{S}{N} \) by the formula,

\[
C = B \cdot \log_2 \left( 1 + \frac{S}{N} \right)
\]  

(6)

The channel capacity represents the amount of information allowed by the communication channel or rather the performance of the system. The bandwidth is the price to be paid because frequency is a limited resource. The signal to noise ratio represents the environmental condition or the physical characteristics such as obstacles, presence of jammers and interference of the communication medium or channel.

From Eqtn. 6 it is seen that the more bandwidth and the better the signal to noise ratio the more bits per second that can be pushed through a channel. Equation 6 can be reformulated as:

\[
\frac{C}{B} = \log_2 \left( 1 + \frac{S}{N} \right)
\]  

(7)

\[
= \frac{\log_e 2}{\log_{10} 2} \left( 1 + \frac{S}{N} \right)
\]  

(8)

\[
= 1.44 \cdot \log_e 2 \left( 1 + \frac{S}{N} \right)
\]  

(9)

If we consider a situation where the signal is weaker than the noise in the channel through which it is been pushed then,

\[
\log_e 2 \left( 1 + \frac{S}{N} \right) \equiv \log_e 2 (1 + x)
\]  

(10)

\( x \) is small, so that Maclaurin series expansion can be applied to obtain

\[
\frac{C}{B} = 1.44 \cdot \left( \frac{S}{N} + \frac{1}{2} \left( \frac{S}{N} \right)^2 + \frac{1}{3} \left( \frac{S}{N} \right)^3 + \ldots \ldots \right)
\]  

(11)

And since \( S/N << 1 \)

\[
\left( \frac{C}{B} \right) \approx \left( \frac{S}{N} \right)
\]  

(12)

The above equation implies that we can trade signal to noise ratio for bandwidth or vice versa, and that if a data can be encoded in a large signal bandwidth error free transmission can be obtained under condition where the noise is much more powerful than the encoded signal.
5.3 How to spread the spectrum

Spread spectrum technique is implemented by multiplying a signal that has a limited bandwidth, also called base band signal, with a signal of higher bandwidth. Because the base band signal is spread or diffused over a wider bandwidth as shown in Fig. 1 it possess much less power per bandwidth or low spectral density.

![Signal before and after spreading](image)

Figure 1: Baseband signal before and after spreading.

5.4 Random white Gaussian noise

Random white noise \[15\] with spatial domain function shown in Fig. 2(A) is a random signal with a flat power spectral density as shown in Fig. 2(D). Its signal power spectral density has equal power in any band, at any centre frequency, having a given bandwidth. The term white is used as an analogy with white light which contains all frequencies.

![White Gaussian Noise](image)

Figure 2: Statistical properties of white Gaussian noise.
Mathematically, a continuous time random process $w(t)$ where $t \in \mathbb{R}$ is a white noise process if and only if its mean function $\mu_w(t)$ and autocorrelation function $R_{ww}(t_1, t_2)$ satisfy the followings:

$$\mu_w(t) = E\{w(t)\} = 0 \quad (13)$$

$$R_{ww}(t_1, t_2) = E\{w(t_1)w(t_2)\} = \sigma^2 \delta(t_1 - t_2) \quad (14)$$

Since the Fourier transform of the delta function,

$$\mathcal{F}(\delta) = 1 \quad (15)$$

The power spectral density of the Gaussian white noise,

$$S_{ww}(\omega) = \sigma^2 \quad (16)$$

The properties of white Gaussian noise are as follows:

1. Zero mean for all time
2. Same power spectral density for all frequencies.
3. Its autocorrelation function is zero for all $t \neq 0$, that is the autocorrelation function has a large peaked maximum for synchronized or two identical white noise as shown in Fig. 2(C). The implication of this is that any two different samples of white Gaussian noise, no matter how close together in time, are uncorrelated. In other words the noise signal is totally uncorrelated from its time-shifted version for any time $t \neq 0$.
4. Gaussian probability density distribution function. See Fig. 2(B).

### 5.5 Pseudo-random noise signal

The high frequency sequence that multiplies the narrow band (base band signal) in order to achieve wider spectrum is called pseudo-random noise (PRN) signal. The PRN signal acts as a form of encryption to the base band signal. The followings summarise the properties of the PRN signal.

1. They have Gaussian distribution of mean zero and variance one.
2. They are deterministic and periodic sequence to the transmitter and receiver section of the communication system, but seems random and noisy to a third party or intruder.
3. They possess statistical properties similar to that of random white Gaussian noise. The autocorrelation function of a one-dimensional PRN signal is shown in Fig. 3. Since the PRN signal is periodic its similarity with the random white Gaussian noise is exhibited by its periodic large peaked maximum.

### 5.6 Types of spread spectrum technique

The different spread spectrum techniques are named according to the point in the communication system at which the pseudo-random noise (PRN) signal is inserted, as shown in Fig. 4.

1. Direct sequence spread spectrum (DSSS) is obtained when the PRN is inserted at the data level
2. Frequency hopping spread spectrum (FHSS) is obtained when the PRN is inserted at the carrier frequency level. In this case the carrier signal is forced to hop or change according to the pseudo-random sequence
3. Time hopping spread spectrum technique is obtained when the PRN acts as an on/off gate to the transmitted signal
5.7 Basic principle of direct sequence spread spectrum - encoding

Figure 5 explains the basic principle of the embedding process of direct sequence spread spectrum communication. We focus on the direct sequence technique because it will be adopted for our proposed watermarking system. For ease of clarification one-dimensional digital signal is used in this example. The digital data $D_T$ with narrow bandwidth $R_D$ is directly multiplied with the PRN signal $PRN_T$ having a wide bandwidth, and which itself is independent of the digital data to produce a wide band signal $T_T$ having higher bandwidth $R_T$ according to the equation:

$$T_T = D_T \ast PRN_T \quad (17)$$

and

$$R_D << R_T \quad (18)$$

From the figure it can be seen that the spectrum of the transmitted signal looks like that of white noise. The amplitude of the transmitted message signal is same as that of the original message signal. Hence the power of the transmitted signal will be same as that of the original information. Since the transmitted power is unaltered the increased bandwidth of the transmitted message signal will result in lower power spectral density determined by the bandwidth expansion factor $G$, defined as:

$$G = \frac{R_T}{R_D} \quad (19)$$
Figure 5: Embedding principle of direct sequence spread spectrum.

5.8 Basic principle of direct sequence spread spectrum - synchronized decoding

As shown in Fig. 5 at the receiver section the received signal $T_R$ is multiplied by same pseudo-random signal synchronized in time with the pseudo-random signal at the transmitter section according to the equation

$$D_R = T_R * PRN_R$$  \hspace{1cm} (20)

Since $T_R = T_T$

$$D_R = (D_T * PRN_T) * PRN_R$$  \hspace{1cm} (21)

$$= D_T (PRN_T * PRN_R)$$  \hspace{1cm} (22)

In a typical scenario the amplitude of the PRN signal at the transmitter and receiver alternates between minus one and one. For example

$$PRN_R = PRN_T = +1 -1 +1 -1 +1 -1 -1 +1 -1 -1 +1 -1 +1 -1 +1 -1.........$$  \hspace{1cm} (23)
The alternation is destroyed when the PRN sequences are perfectly synchronized and multiplied by itself according to the equation

\[ PRN_T \ast PRN_R = 111111111111 \ldots \] (24)

\[ D_R = D_T \] (25)

Thus the message signal is reproduced at the receiver output at all times provided the PRN signal at the receiver is in perfect synchronization with that of the transmitter.

The autocorrelation function of the product of the two PRN sequences is

\[ AR = mean(PRN_T \ast PRN_R) = mean(1) = 1 \] (26)

In the absence of interference in correlation-based technique, detection of the desired signal is achieved by correlating the PRN sequence at the receiver with the received transmitted signal \( T_R \). The periodic peaks in the

Figure 6: Decoding principle of direct sequence spread spectrum.
autocorrelation function between the transmitted signal and the PRN at the receiver is derived from the periodic property of the PRN sequence contained in the transmitted signal. To recover the desired signal in this example, the decision threshold is fixed at \( \tau = 1 \).

With the correlation unit decision threshold set at \( \tau = 1 \) the message signal is said to be detected or not detected according to the comparator function \( C_\tau \)

\[
C_\tau(\text{PRN}_T, \text{PRN}_R) = \begin{cases} 
1 & c \geq \tau \\
0 & c \leq \tau
\end{cases}
\] (27)

5.9 Basic principle of direct sequence spread spectrum - unsynchronized decoding

If the PRN sequence at the receiver is different from the PRN sequence at the transmitter and therefore not in perfect synchronization with the PRN sequence at the transmitter, the autocorrelation function of the PRN sequence at the transmitter and the PRN sequence at the receiver is according the equation

\[
AR = \text{mean} \{ \text{PRN}_T \ast \text{PRN}_R \} << 1
\] (28)

By correlating the two signals using the fixed decision threshold of the comparator function it is seen that the correlator unit outputs zero indicating no signal detection for all time. The zero output of the correlator is an indicator of the orthogonal property of PRN sequences.

5.10 Spread spectrum in the presence of interference

In the presence of interference the received signal \( D_R \) is expressed as

\[
D_R = D_T \ast \text{PRN}_R + I
\] (29)

To recover the message signal (input data) \( D_T \) at the receiver section, the received signal is multiplied by PRN sequence that is in perfect synchronization with that at the transmitting section according to the equation

\[
D_R = (D_T \ast \text{PRN}_T + I) \ast \text{PRN}_R
\] (30)

\[
= D_T \ast (\text{PRN}_T \ast \text{PRN}_R) + I \ast \text{PRN}_R
\] (31)

As explained in the previous section Eqtn. 28 becomes

\[
D_R = D_T + I \ast \text{PRN}_R
\] (32)

Thus the message signal with noise added is reproduced at the receiver section when the received signal is multiplied with a perfectly synchronized PRN sequence. The second term in Eqtn. 29 indicates that the PRN sequence will affect the interference the same way it affects the message signal at the transmitting section by spreading it. Spreading increase its bandwidth and decrease its power spectral density making the interfering signal much less effective and harmful on the message signal.

The process of multiplication with the PRN sequence results in a narrow band component represented by the message signal and a wide band component represented by the product of the interference and the PRN sequence at the receiver. The message signal is recovered by applying a low-pass filter with a bandwidth just large enough to accommodate the recovery of the message signal. In this way most of the interference component is filtered out.
5.11 Why spread the spectrum

The need to spread the spectrum may be the reason why spread spectrum application was first conceived in the military community. Spread spectrum technique offer a lot of advantages over other communication techniques such as amplitude modulation and frequency modulation. They are

1. Good anti jamming performance
2. Low power density hence difficulty in detection
3. Interference limited operation –immunity to interference
4. Multiple access features since more than one user share the same bandwidth
5. Privacy due to the use of unknown random codes resulting in security from eavesdropping
6. Random access probabilities resulting in bandwidth sharing
7. Reduction in multipath effects
6 Wavelet transformation

6.1 Wavelet transformation defined

Wavelet transformation is a transformation that transforms a function or array of numbers to a function that is localized both in space and frequency. Using linear algebra terms we say that wavelet transform is a transformation to basis functions that are localized in scale (frequency) and in time as well. The basis functions are the wavelets and the transformation yields wavelet coefficients.

6.2 Basis of a vector space, basis vector, basis function and wavelet defined

Basis of a vector space $V$ is a set of linearly independent vectors such that any vector $v \in V$ can be written as, or generated from linear combination of a so-called basis vectors $\phi_k$ according to the equation

$$ v = \sum_k \mu_k \phi_k $$

(33)

$\mu_k$ are coefficients associated with each basis vector. This definition implies that there may be more than one basis of a vector space, however all basis of a vector space have the same number of basis vectors. The number is the dimension of the vector space [20].

Simple examples are the vectors in Eqtn. 31.

$$ v_1(i, j) = 2i + 5j $$
$$ v_2(i, j) = 4i + 7j $$
$$ v_3(i, j) = 6i + 8j $$

(34)

All the vectors $v_1, v_2, v_3 \in V$ are the basis of the vector space $V$. $i$ and $j$ are the basis vectors. Since the numbers of basis vectors are two, the dimension of the vector space is two.

If we move from vector terms to function terms Eqtn. 30 becomes

$$ f(t) = \sum_k \mu_k \psi_k(t) $$

(35)

$$ f(t) \equiv v $$

$$ \psi_k(t) \equiv \phi_k $$

(36)

In Fourier transform of a function the basis functions are the sines and cosines functions. In the case of wavelet transform, the basis functions are wavelets, and any continuous function or signal may be uniquely projected onto the wavelet basis functions and expressed as a linear combination of the basis functions. The collections of coefficients $\mu_k$, which weight the wavelet basis functions $\psi_k(t)$ when representing an arbitrary continuous function, are referred to as the wavelet Transform of the given function.

What is a wavelet? Wavelet is a small (compact), irregular, asymmetric, real-function wave with an average value of zero and values that die out to zero as one approaches positive and negative infinity. Figure 7 shows a typical wavelet.

6.3 Wavelet transformation explained

A better grasp of the wavelet transform can be understood by comparing it to the Fourier transform. Whereas the Fourier transform breaks the signal into a series of sine waves of different frequencies, the wavelet transform
breaks the signal into its “wavelets” that are scaled and shifted versions of the “mother wavelet” \( \psi \). The mother wavelet is a prototype for generating other wavelet ‘windows’, which is the scaled and shifted version. In other words the functions used for the wavelet transformation are generated from the mother wavelet. Examples of mother wavelets are the Haar and Debauchies wavelets. By scaling is meant expansion or compression of the mother wavelet while translation has to do with the location of the mother wavelet in the signal to be analyzed. The scaled \( s \) and shifted \( \tau \) version of the mother wavelet \( \psi(t) \) is mathematically represented as

\[
\psi_{\tau,s} = \psi \left( \frac{t - \tau}{s} \right)
\]  

The wavelet transformation of a signal \( x(t) \) starts by placing the mother wavelet with a predefined minimum scale(frequency) at the beginning of the signal \( (\tau = 0) \). Different scaled and shifted versions of the mother wavelet obtained at continuous interval is multiplied by the signal and then integrated over all time duration of the wavelet as shown in Fig. 8. A constant number \( \frac{1}{\sqrt{|s|}} \) then multiplies the result of each of the integration to obtain the continuous wavelet transform or wavelet coefficients according to the equation:

\[
W(\tau,s) = \frac{1}{\sqrt{|s|}} \int x(t) \psi * \left( \frac{t - \tau}{s} \right) dt
\]  

For every scale and time interval one point of the time-scale plane is computed. Computations at one scale construct the row of the time-scale plane while computations at different scales construct the columns of the time-scale plane. During computation if the the local area of the signal to be analyzed has a spectral component that corresponds to the current scale and shifted version of the mother wavelet the product of the wavelet with the signal at the location where the spectral components exsts gives a relatively large value. Otherwise the values will be low. The “beauty” of wavelet transformation result from the fact that by shifting the wavelet in time, the signal is localized in time, and by varying the value of the scale, the signal is localized in scale (frequency) thus providing a picture of the overall match between the wavelet function and the signal. Each wavelet coefficient represents the correlation between the wavelet function at a particular size and a particular location within the signal. Localized nature of wavelet transform result from the compact and irregular nature of the wavelets. The wavelet coefficients are a measure of variations around a small region of the signal, and the "localized" nature of the wavelet transform enables detection of localized features in signals such as noise, discontinuities, edges of objects, etc.
6.4 Discrete wavelet transformation

The type or class of wavelet transformation that was discussed in the previous section is the continuous wavelet transformation (CWT). Though it uses discretely sampled data of the signal to be analyzed, the shifting and scaling process is a smooth (continuous) operation across the length of the sampled data resulting in fine resolution of both space and frequency. The trade off for this fine resolution is an increased computational time and memory required to calculate the wavelet coefficients. This led to the development of the discrete wavelet transform (DWT).

Discrete wavelet transform is wavelet transformation obtained when the wavelets used for the computation of the wavelet transforms are discretely sampled. Practically it is observed that efficient and accurate analysis of a signal is obtained when the scaled and translated versions of the mother wavelets as well as the dimension of the signal are based on powers of two usually referred to the dyadic scales and positions. Furthermore, the mother wavelet is orthogonal to all functions that are obtained by dilating (stretching) the mother by a factor of $2^j$ and shifting by multiples of $2^j$ units. The orthogonality property means that the inner product of the mother wavelet with itself is unity, and the inner products between the mother wavelet and the aforementioned shifts and dilates
of the mother are zero.

An efficient way to implement discrete wavelet transform scheme using filters was developed in 1988 by Mallat [14]. In the algorithm the signal is simultaneously passed through a set of high and low pass filters known as quadrature mirror filter. The high-pass filters act as the basis functions while the low-pass filters act as the complement of the basis functions. The output from the high-pass filter give the details coefficients and that from the low-pass filter give the approximation coefficients (LL). Spatially oriented filters are further used to decompose the details coefficients into three spatial directions and sub bands, that is horizontal (LH – low high), vertical (HL – high low) and diagonal (HH – high high). The aforementioned steps together form the first level of wavelet decomposition (resolution) of the signal. To get to another level of resolution, the decomposition is repeated on the approximation coefficients. The approximation coefficients is decomposed with high and low pass filters and then down-sampled. This is represented as a binary tree shown in Fig. 9.

![Figure 9: Filter bank representations of discrete wavelet transform dilations.](image)

Each level of DWT decomposition can be represented by the following frequency sub bands in ascending order, LL (low-low), HL (High-low), LH (low High), HH (High-high). Figure 10 obtained from MATLAB documentation [9] illustrate a one-level wavelet decomposition.

![Figure 10: An image and its level decomposition components.](image)
7 System design: Encoding

7.1 Embedding algorithm introduced

The host image is the standard Lena image of dimension 256 \times 256 having bit map (bmp) format. The watermark was designed using paint photo editor. It has dimension 30 \times 120. The watermark’s foreground pixels are pure black and were set on a pure white background so that it can easily be digitized. Both images are shown in Fig. 11(A) and Fig. 11(B). Digitization of the experimental watermark and any other watermark that may have irregular pattern is necessary because our desire is that, under ideal condition, the correlation values corresponding to foreground bits of the watermark will be high and have same value. On the contrary, all the correlation values corresponding to background bits of the watermark will be low with same value.

The watermark will not be embedded directly into the host image. Rather it will be encoded in the form of a uniformly distributed PRN signal. Even so only the foreground bits of the watermark will be encoded in the host image.

Our choice of the frequency sub band to encode the watermark in the wavelet decomposed host image is based on the relationship between the human visual system model and DWT as reported in [3]. The authors reported that the human visual system is less sensitive to distortions in high frequency sub bands. Thus we chose to encode the watermark in the middle (horizontal and vertical components) of the high frequency range in each of the resolution levels as in [4].

7.2 Embedding algorithm

The original image is processed as follows:

1. Read original image I into MATLAB
2. Process original image and determine its dimension
3. Compute the wavelet transform \( W(I) \) of the original image

The watermark is processed as follows:

1. Read watermark J into MATLAB
2. Process watermark and determine its dimension

3. Digitize watermark by dividing every pixel by the maximum pixel. Digitizing will leave the black watermark pixels (foreground) with values 0 while the white background pixels will have value one.

4. Reshape the 2-dimensional watermark into a column vector of length \( N \) with foreground bits of length \( p \) and background bits of length \( q \) so that

\[
p + q = N \tag{39}
\]

The 1D watermark signal is shown in Fig. 12. Observe that each of the distinct bar in the signal represent each alphabet in the watermark.

![One-dimensional watermark signal](image)

The spread spectrum technique is implemented as follows

1. Define secret code (key)

2. Set the state of the MATLAB PRN generator to that of the predetermined secret key. This will set the PRN generator to the same fixed state and enables repetition of same random number. In this way the generated PRN signals \( PRN_z \) are perfectly synchronized when generated at different times.

3. For every length of the watermark signal if the pixel is foreground (black) pixel generate a different and independent pseudo-random noise signal \( PRN_z \) of same dimension as the wavelet transform of the host image and add to the horizontal and vertical detail coefficients of the wavelet transform of the host image \( W(I) \) scaled by a defined distortion factor \( K \) according to the equation

\[
WQ = W(I) + K \sum_{Z=1}^{p} PRN_z \tag{40}
\]

The PRN signal is a form of encoding for each foreground pixel so that each generated pseudo-random signal represents a foreground pixel in the watermark or message signal. Note that PRN signal is generated for every background pixels but is not added to the host image.
1. Carry out inverse transform \( W^{-1}(WQ) \) to obtain the watermarked image \( WM \)

Block diagram of the embedding process is shown in Fig. 13.

**Figure 13: Block diagram for the watermark encoding.**

7.3 Simulation of encoding algorithm

The first task in the simulation algorithm is to determine the lower limit of the distortion factor. It was determined as the distortion factor that is slightly above the value that gives the error message

`error ('INCREASE PAYLOAD SIGNAL - WATERMARK NOT EMBEDDED IN THE IMAGE')`

Using the standard Lena image the lower limit was found to be 0.02. The upper limit though heuristic was determined by the perception of the human visual system (HVS). The upper limit is determined when the HVS perceive appreciable degradation in the quality of the watermarked image. Values of distortion factors ranging from the lower limit of 0.02 to upper limit of 10 in steps of 0.02 (1000 inputs) were inputted into the embedding unit to output different degradation of watermarked images. The graphical relationship is shown in Fig. 14(A), Fig. 14(B) and Fig. 14(C) for 1-level decomposition, second level decomposition and third level decomposition respectively. Fig 14(D) shows the three curves plotted on same graph. Observe the similarity (parabolic nature) of all the three curves and appreciable degradation of the images as the distortion factor increases. The degradation (PSNR) corresponding to distortion factor of value 10 for the first, second and third levels of decomposition are 10.6dB, 10dB and 7dB respectively. Figure 15 show watermarked images with different distortion factors and corresponding peak signal to noise ratio for the first level decomposition. From the images in the figure it is seen that degradation of the images is not perceived for distortion factor less than two. Beyond the value of 2 and up to the upper limit of 10 the degradation is very visible. Beyond the upper limit where the distortion factor exceeds 400, the host image is completely distorted beyond recognition. In this region the system can be used for cryptographic applications. This is illustrated in Fig. 16.
Figure 14: Relationship between distortion factor and PSNR of watermarked image for first, second and third level decompositions.
Figure 15: The original image, the different degradations of the watermarked images and corresponding distortion factors.
Figure 16: Dual application of the system for watermarking and cryptographic applications.
8 System design: Correlator

8.1 Correlation algorithm introduced

The function of the correlator unit is to determine the correlation function between the PRN sequence embedded in the watermarked image and the synchronized PRN sequence in the correlator unit. The length of the correlation function is same as the length of the watermark. As stated in section 7.1 the purpose of digitization of the watermark is to ensure that under ideal condition all elements of the correlation function corresponding to the foreground bits have same correlation value $H_i, V_i$ for the horizontal and vertical details component of the wavelet decomposed host image. Similarly all elements of the correlation function corresponding to the background bits have same value $H_j, V_j$ for the horizontal and vertical details component of the wavelet decomposed host image.

The mean of the correlation function for the horizontal $C_H$ and vertical $C_V$ details component of the host image is therefore expressed as

$$C_H = \frac{1}{N} \left( \sum_{i=1}^{p} H_i + \sum_{j=1}^{q} H_j \right)$$

$$C_V = \frac{1}{N} \left( \sum_{i=1}^{p} V_i + \sum_{j=1}^{q} V_j \right)$$

The mean of the correlation function for the horizontal $C_H$ and vertical $C_V$ details component of the host image is therefore expressed as

The correlator explores the spatial-frequency localization of the wavelet transformation; the uniformly distributed PRN sequences embedded in the horizontal and vertical details component of the wavelet decomposed host image are highly localized in space and frequency. Hence correlating synchronized PRN sequence with these sub bands will definitely give correlation function that gives a clear picture of the match between the generated synchronized PRN signal and the localized PRN sequence. The correlation between the PRN signal generated at the correlator unit (corresponding to the foreground of the watermark) and the watermarked image will be high because corresponding PRN signals were embedded and localized in frequency and space in the wavelet decomposed watermarked image. On the contrary, the correlation between the PRN signal generated at the correlator unit (corresponding to the background of the watermark) and the wavelet decomposed watermarked image will be very low (close to zero) because the corresponding PRN signals are not constituent of the wavelet decomposed watermarked image. This can be expressed mathematically as

$$\sum_{i=1}^{p} H_i >> \sum_{j=1}^{q} H_j$$

and

$$\sum_{i=1}^{p} V_i >> \sum_{j=1}^{q} V_j$$

8.2 Correlation algorithm The correlation algorithm is as follows

1. Read in the watermarked image
2. The watermarked image is transformed into the wavelet domain.
3. Define secret key, same as that used during embedding for generating PRN signal. Same secret key ensures that the generated PRN signal $PRN_D$ is in perfect synchronization with the PRN signal $PRN_Z$ generated during embedding.
4. Initialize the correlation function to zeros having same size as the length of the watermark.
5. For each length of the watermark generate a different and independent PRN signal and compute the average correlation between the details coefficients (horizontal and vertical) of the wavelet-transformed watermarked image and the PRN signal.

6. Obtain the correlation function and save for onward transmission to the comparator unit.

### 8.2 Uniformly distributed PRN signal or normally distributed PRN signal?

We were faced with the choice between uniformly distributed PRN signal and normally distributed PRN signal. Our choice was based on result of simulation result from the system. We input watermarked image with imperceptible distortion factor of 1.2 and obtained correlation function with each of the PRN signal as shown in Fig. 17 and Fig. 18. From the figures we see that the correlation function of the uniformly distributed PRN signal show better distinct peaks corresponding to the watermarks than the normally distributed PRN signal. This is an indication that uniformly distributed PRN signal have better localization in terms frequency and space in the wavelet decomposed host image than the normally distributed PRN signal.

![Graph of one dimensional correlation function obtained by using normally distributed PRN signal.](image)

Figure 17: Graph of one dimensional correlation function obtained by using normally distributed PRN signal.
Figure 18: Graph of one dimensional correlation function obtained by using uniformly distributed PRN signal.
9 System design: Comparator

9.1 Comparator algorithm introduced

The comparator unit begins its operation by creating a null vector having same dimension as the watermark. Scanning through every correlation values in the correlation function follows this. The correlation function itself has same dimension as the watermark. It compares each of this value to a predefined scalar number called decision threshold value $\tau$. If any of the correlation function value is greater than the decision threshold value one bit is entered into the corresponding point in the initially created null vector space. Otherwise a 0 bit is entered. In the absence of attack and under ideal condition, the decision threshold $\tau$ is given by

$$\tau = \frac{1}{2} (C_H + C_V)$$  \hspace{1cm} (45)

Substituting for $C_H, C_V$ in Eqtn. 38 and Eqtn. 39

$$\tau = \frac{1}{N} \left( \sum_{i=1}^{p} H_i + \sum_{j=1}^{q} H_j \right)$$  \hspace{1cm} (46)

$$+ \frac{1}{N} \left( \sum_{i=1}^{p} V_i + \sum_{j=1}^{q} V_j \right)$$  \hspace{1cm} (47)

Since $H_i >> H_j$ and $V_i >> V_j$,

$$\tau \approx \frac{1}{N} \left( \sum_{i=1}^{p} H_i + \sum_{j=1}^{q} V_i \right)$$  \hspace{1cm} (48)

Attack changes the spatial and frequency domain statistics of the watermarked image. The correlation values obtained by the comparator unit will also respond to this change. There are two possible changes for each of the correlation values. They are either an increase or a decrease in the correlation values leading also to either an upward or downward decrease in decision threshold value. The comparator unit of the watermarking system reflect this by assigning to the attack-induced elements of the null space a bit value of one for a supposed value of 0 and a bit value of 0 for a supposed bit value of one. This is illustrated in Fig. 19 that show watermark recovered from an attacked watermarked image. The shift in correlation values if not compensated for will result in error of judgement regarding the presence of watermark.

Assume that the net increase in correlation values for the horizontal and vertical components are $\Delta H_i, \Delta V_i$,
\( \Delta H_j, \Delta V_j \) respectively, the new correlation decision threshold value based on Eqtn. 42 becomes

\[
\tau_D = \frac{1}{N} \left( \sum_{i=1}^{p} (H_i \pm \Delta H_i) + \sum_{j=1}^{q} (H_j \pm \Delta H_j) \right) + \frac{1}{N} \left( \sum_{i=1}^{p} (V_i \pm \Delta V_i) + \sum_{j=1}^{q} (V_j \pm \Delta V_j) \right)
\]  

(49)

\[
\tau_D = \frac{1}{N} \left( \sum_{i=1}^{p} H_i \pm \sum_{j=1}^{q} H_j \right) + \frac{1}{N} \left( \sum_{i=1}^{p} V_i \pm \sum_{j=1}^{q} V_j \right) + \frac{1}{N} \left( \sum_{i=1}^{p} (\Delta H_i \pm \Delta H_j) + \sum_{j=1}^{q} (\Delta V_i \pm \Delta V_j) \right)
\]  

(50)

\[
\tau_D = \tau \pm \Delta \tau
\]  

(51)

From Eqtn. 47

\[
\tau_D > \tau \text{ or } \tau_D < \tau
\]  

(55)

The above equation indicates that attacks cause an upward or downward shift in the threshold decision values of the comparator. The severity of attacks on a watermarked image cannot be precisely measured by a watermarking system; hence the recovery decision threshold value resulting from this attack cannot be precisely determined. The best we have done so far is to determine that there is either an upward or downward shift in the threshold decision value. This issue was addressed in [3; 19] using probabilistic approach. The design principle of the comparator unit of our watermarking system is a departure from existing probabilistic technique. In line with Eqtn. 48 the recovery decision threshold of the comparator unit is discretized upwards and downwards in steps \( T \) of the mean correlation function, \( \tau \) using step size \( \rho \) according to the equation

\[
\tau_D = T \ast \rho \ast \tau
\]  

(56)

The step size \( \rho \) gives the comparator unit the resolution power to search the decision threshold space for value(s) that gives correct judgement on recovery of the watermark, and compensate for the shift in the statistics of correlation values. By so doing the watermarking system is robust, sensitive and adaptive to all known forms and severities of attacks that cause a shift of the decision threshold during decoding in correlation-based technique. We adopted heuristic approach to determine the step size used for discretizing the mean threshold value.

### 9.2 Comparator algorithm

The comparator unit of the decoding algorithm is as follows

1. Read in the correlation function \( C \)
2. Compute the mean of the correlation function \( \tau \).
3. Define the number of discrete steps \( T \) of the mean correlation and step size \( \rho \)
4. Initialize the recovered watermark to zeros having same dimension as the correlation function \( C \).

5. Obtain recovered watermarks that are equal in number to the discrete steps of the decision threshold.

6. For each element of the correlation function, and for each discrete step compute the product of the mean correlation \( \tau \), the step size \( \rho \) and discrete step \( T \). Assign bit value of 0 to the corresponding element in the initialized recovered watermark if correlation function value is greater than the product of discrete step, step size and mean of correlation function. Otherwise assign bit value of one. The extracted watermark, \( W_E \) is according to the equation:

\[
W_E = C_\tau = \begin{cases} 
1, & c \geq T \ast \rho \ast \tau \\
0, & c \leq T \ast \rho \ast \tau 
\end{cases}
\]  (57)
10 System design: Despreader

The watermarking system we have designed so far consists of the encoder, correlator and comparator. We shall simulate the system. Analysis of the simulation result will substantiate the argument for the need to have a tuner or despreader included in the watermarking system.

10.1 Simulation of watermarking system

Values of distortion factors ranging from the lower limit of 0.02 to upper limit of 20 in steps of 0.02 were inputted into the watermarking system. Each distortion factor value gives ten peak signal to noise ratio because the decision threshold of the comparator is discretized in ten steps of the mean correlation function. However, in this simulation, the output is the maximum of the ten peak signal to noise ratios of the ten recovered watermarks. Simulation results for first, second and third level wavelet decomposition of the host image are shown graphically in Fig. 20, Fig. 21 and Fig. 22.

![Variation of maximum PSNR of recovered watermarks with distortion factor for first level wavelet decomposition](image)

Figure 20: Variation of maximum PSNR of recovered watermarks with distortion factor for first level wavelet decomposition.

10.2 Analysis of simulation result: First sub bands in first, second and third level

A cursory look at each of the simulation curve reveals a common feature in the first sub band for each of first, second and third level wavelet decomposition. The maximum peak signal to noise ratio (PSNR) of the recovered watermark increases steeply from its lowest level of 3.19dB for the first level, 3.35dB for the second level and 3.19dB for the third level, until it attains a threshold value of 18.8012dB where it remains constant no matter the increase in distortion factor. The lowest level of PSNR correspond to distortion factor of 0.02 while the threshold
Figure 21: Variation of maximum PSNR of recovered watermarks with distortion factor in each sub band for second level wavelet decomposition.

value correspond to distortion factor approximately equal to 1.2. Note that the watermark is imperceptible in the watermarked image for distortion factor in the range (0.02 - 1.2). But the watermark though imperceptible cannot be recovered by the system because the maximum peak signal to noise ratio of recovered watermarks is very low and beyond human perception.

Each of Fig. 23, Fig. 24, Fig. 25, Fig. 26, Fig. 27 and Fig. 28 show a degraded watermarked image with imperceptible watermarks and corresponding distortion factors (0.02, 0.2, 0.4, 1.2, 10 and 400), the ten recovered watermarks and signal to noise ratios obtained from a first level wavelet watermarking system.
Figure 22: Variation of maximum PSNR of recovered watermarks with distortion factor in each sub band for third level wavelet decomposition.

Figure 23: Watermarked image ($K = 0.02$).
Figure 24: Watermarked image ($K = 0.2$).

Figure 25: Watermarked image ($K = 0.4$).

Figure 26: Watermarked image ($K = 1.2$).
10.3 Analysis of simulation result: Second sub bands in second and third level

The second sub bands in second and third level decompositions have similar features. The maximum PSNR of the recovered watermark increases with less slope compared to the first sub band, from its lowest level of 3.7dB for the second level and 3.37dB for the third level, until it attains a threshold value of 16.84dB for the second level and 16.24dB for the third level, where it remains constant no matter the increase in distortion factor. The minimum degradation of the watermark correspond to distortion factor of 0.02 while the threshold value correspond to distortion factor approximately equal to four.

10.4 Analysis of simulation result: Third sub bands in third level

The maximum PSNR of the recovered watermarks increases very slowly compared to the first and second sub-bands, from its lowest level of 3.39dB for the third level until it attains a threshold value of 11.22dB where it remains constant no matter the increase in distortion factor.
10.5 General analysis of simulation result

The simulation result for a first level wavelet decomposition is broken down into three sections in Fig. 29 and the attributes of each section outlined. The threshold value for the PSNR of the recovered watermarks reduces as the level of sub bands increase. This is illustrated in Fig. 22 where the values are 18.8dB, 16.2dB and 11.22dB for a third level wavelet decomposition. This is expected because the resolution level of the wavelet decomposition decreases with increase in subband. Based on the simulation result we conclude that the trade off for an imperceptible watermarked image is decrease in peak signal to noise ratio of the recovered watermark. But our watermarking system can only be reliable if the watermark in the watermarked image is imperceptible. The implication is that if we want to have an imperceptible watermarked image we will not be able to recover or detect the watermark and if we choose to have a watermarked image whose watermarks are perceptible then it will be possible to recover the watermark. Can this simulation result be explained? The answer is positive.

1. During encoding there is spreading of the spectrum of the watermark signal to obtain the watermarked image.
2. Hence it is expected that despreading of the watermarked image will take place before watermark detection – correlation and comparison with the original watermark.
3. From the simulation result it seen that between the lower limit of distortion factor and the threshold value, the PSNR of recovered watermarks are very low and imperceptible. Hence we conclude that there was no despreading of the watermarked image in this region of the simulation curve.
4. However close to the threshold value we can conclude that there is slight despreading of the watermarked image. This is because the recovered watermarks are barely perceptible.
5. Beyond the threshold value the recovered watermarks are perceptible to the human visual system. Hence we conclude that in this region of the simulation curve there is full despreading of the watermarked image.

10.6 The need for a despreader unit

The objective of our watermarking system design is to embed a watermark that is imperceptible and that can also be unambiguously detected. In the previous section we have seen that from the simulation result if we choose to have an imperceptible watermark we need to trade off unambiguous detection and if we choose to have
a watermark that can be unambiguously detected in an image we will have to trade off imperceptibility of the watermark.

To achieve our goal of imperceptibility and unambiguous detection of the watermark our design strategy is break the simulation curve (distortion factor versus maximum PSNR of recovered watermark) into two sections to derive two independent units – the encoding (spreading) and despreading units. The encoder unit will then be fed into the despreader unit. The despreading unit will despread the output of the encoding unit (watermarked image). Sectioning of the simulation curve to obtain the encoding and despreading units for a first level decomposition is shown in Fig. 30.

![Figure 30: Break up of the simulation curve into two sections to form the encoder and despreader units.](image)

Based on our simulation result the distortion factor of the encoder is set at $K < 1.2$ and the minimum distortion factor of the despreader is set at $K \geq 1.2$. This is the minimum value at which the despreader and of course the watermarking system can operate to encode watermark imperceptibly and detect unambiguously. The system algorithm is designed to execute watermarking task if the distortion factor of the encoder is less than 1.2 and execute cryptographic task for distortion factor greater than 400. These design parameters makes sense because for $K < 1.2$ at the encoding unit the watermark will be imperceptible and for $K \geq 1.2$ at the despreader unit the watermarked image will be fully despread before detection can take place. However for $K \leq 1.2 \leq 2$ the degradation suffered by the host image is subjective; it depends on individual perceptual assessment of the host image. Full distortion of the host image is achieved for $K > 400$. During cryptographic operation the despreader unit is bypassed because it is not required for the operation. Block diagram of the watermarking and cryptographic system is shown in Fig. 31.
Figure 31: Block diagram of the watermarking and cryptographic system.
11 Test results

Figure 32: Gaussian filtered watermarked image.

Figure 33: Average filtered watermarked image.
Figure 34: Laplacian filtered watermarked image.

Figure 35: 50° degree rotated watermarked image.

Figure 36: 120° rotated watermarked image.
Figure 37: 128 × 128 resized watermarked image.

Figure 38: 200 × 200 resized watermarked image.

Figure 39: Cropped watermarked image.
Figure 40: Multiple attack on watermarked image.

Figure 41: 100 × 100 resize attack ($K = 1.2$) on watermarked image.
Figure 42: $100 \times 100$ resize attack ($K = 30$) on watermarked image.

Figure 43: JPEG compressed (5%) watermarked image.

Figure 44: JPEG compressed (10%) watermarked image.
Figure 45: JPEG compressed (80%) watermarked image.

Figure 46: Watermarked image ($K = 0.02$) $T = 10, \rho = 1$.

Figure 47: Watermarked image ($K = 0.02$) $T = 15, \rho = 0.1$. 
Figure 48: Gaussian filtered watermarked image.

Figure 49: Average filtered watermarked image.

Figure 50: Laplacian filtered watermarked image.
Figure 51: 50° rotated watermarked image.

Figure 52: 120° rotated watermarked image.

Figure 53: 128 × 128 resized watermarked image.
Figure 54: 200 × 200 resized watermarked image.

Figure 55: Cropped watermarked image.
The test results displayed show that our algorithm is fully immune to all known forms and severities of attacks including rotation, scaling and multiple attacks. Scaling attacks become more severe as the host image is scaled downwards. However the tuning property of our system is used to checkmate this type of attack as shown in Fig. 36 and Fig. 37. By varying or tuning the distortion factor of the despreader unit from $K = 1.2$ to $K = 30$ the recovered watermarks are more visible, have higher maximum peak signal to noise ratio and so can be said to be unambiguously detected.

The system is designed to execute watermarking task if the distortion factor of the encoder is less than 1.2 and execute cryptographic task for distortion factor greater than 400. It is very important to note that this design parameter is based on the standard Lena image as the host image and the watermark shown in Fig. 11. Obviously the system parameters will be different for same host image and watermark of different size, and for different host image and watermark.

12 Conclusion

Faithful implementation of spread spectrum communication technique in the digital watermarking world has long been a Herculean task for image processing engineers and researchers. In this report we developed a digital watermarking algorithm that faithfully implement spread spectrum technique, and replay its excellent anti-jamming property. Our proposal is a fully robust, secure and tunable spread spectrum correlation-based wavelet watermarking and cryptographic system. Experimental results obtained from our system confirm its superior performance over existing wavelet based spread spectrum watermarking systems.
References


