Ministry of Higher Education and Scientific Research

Third Cycle Doctoral lmd

Thesis

Submitted in partial fulfillment for the requirements of the Doctorate Degree Deivred By

University Mohammed Khider of Biskra

Doctorale School "Applied Mathematics"

Presented and defended publicly by

SOUALHI SARRA

The 23rd February 2017

Multi -resolution Analysis Theory and signal decomposition on wavelets basis

Supervisor : **Zouhir MOKHTARI**

Examination Committee

Mr. Khaled MELKEMI,	Professor	University of Batna2	President
Mr. Zouhir MOKHTARI,	Professor	University of Biskra	Supervisor
Mr. Djabrane YAHIA,	MCA	University of Biskra	Examiner
Mr. Mokhtar Hafayedh,	MCA	University of Biskra	Examiner
Mr. El Amir Djeffal,	MCA	University of Batna 2	Examiner

LMA
Applied Mathematics Laboratory
post Box 145, Biskra University, Biskra, Algeria

THESE

Contents

List of Figures

List of Tables

Chapter 1

Preliminary

One, remember to look up at the stars and not down at your feet. Two, never give up work. Work gives you meaning and purpose and life is empty without it. Three, if you are lucky enough to find love, remember it is there and don't throw it away.

Stephen Hawking

Sommaire

1.1 Cryptography

The development of computer and networks in our everyday lives has made protecting data a necessity and adding security an important issue. Most data transmitted over a network is sent in clear text making it easy for unwanted persons to capture and read sensitive information. Algorithms used in encryption methods has protecting data from intruders and making sure that only the intended recipient can decode and read the information.

1.1.1 Cryptography

Definition 1 *Cryptography is the practice of encoding data, so that it can only be decoded by specific individuals.*

A system for encrypting and decrypting data is a cryptosystem. These usually employ an algorithm for combining the original data called *"plaintext"* with one or more *"keys"*-numbers or strings of characters known only by the sender and/or recipient; the resulting output is known as *"ciphertext"*.

The security of a cryptosystem usually relies on the secrecy of the keys rather than the supposed secrecy of the algorithm. The width of range of possible keys involve a strong cryptosystem so that it is not possible to just try all possible keys. A strong cryptosystem has producing ciphertext which appears random to all standard statistical test and can resist all known breaking codes methods.

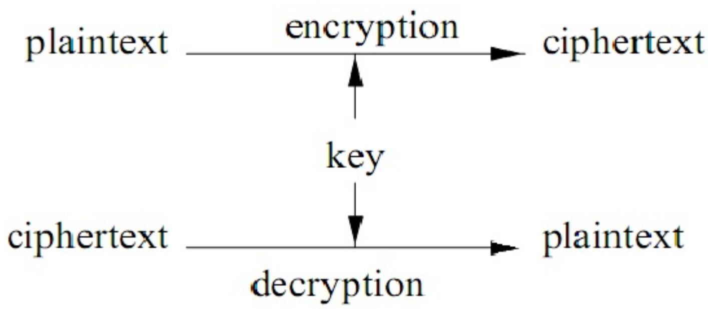

Figure 1.1: Cryptography

1.1.2 Encryption and Decryption

Usually, encryption is a mechanism which transform message in order that only the sender and the recipient can see.
Encryption is simply the translation of data into a secret code (is a formula used to turn data into a secret code), and it is considered the perform way to ensure data security. To read an encrypted file, you must have access to secret key or password (string of bits) that you make enables to decrypt it.
Modern encryption is achieved using algorithms based on key to encrypt information into digital nonsense and then decrypting it by return it to its original form. Not that the lager of key is the more bits in the key.
the number of potential combinations that can be created must be greater to be harder to break the code and unscramble the contents.

1.1.3 Common Types of Encryption

There are tow main types of encryption: symmetric encryption or secret key cryptography (one key) and asymmetric encryption also known as public (private)-key encryption (tow keys) and there are many algorithms for encrypting data based on these types.

Secret Key (Symmetric) Encryption

Symmetric encryption, also referred to as conventional encryption or single key (ie: using the same key to encrypt and decrypt message) was the only type of encryption in use prior to the development of public-key encryption.

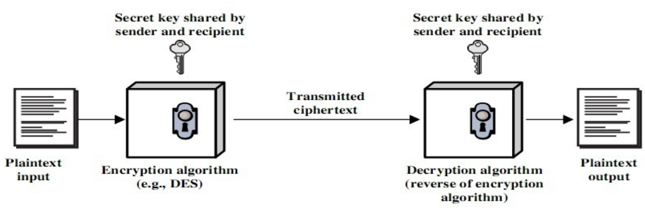

Figure 1.2: Model of Symmetric Encryption

- **The advantages of secret key cryptography**

  1. It is Perform and very fast.
  2. It has been well tested.

- **The disadvantages of secret key cryptography**

  There are two requirements for a symmetric key cryptosystem

  1. We assume it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret.
  2. Sender and the receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communications using this key is readable.

Public Key (Asymmetric) Encryption

This encryption type gives each person a pair of keys (a public key and a private key), where Each person's public key is published but the private key is kept secret.
Encryption of messages use the intended recipient's public key while its decryption require only this private key.
This method of encryption eliminates the need for the sender and the receiver to share secret information (key) with a secure channel. All communications use only public keys, and no private key is ever transmitted or shared.

- **The advantages of public key cryptography**

  1. Only one part must be kept secret (public keys)
  2. We don't need to change the public/private key pair (unless someone finds the public key)
  3. Communication of N people need only be N public/private key pairs.
  4. There is no need for initial key exchange.

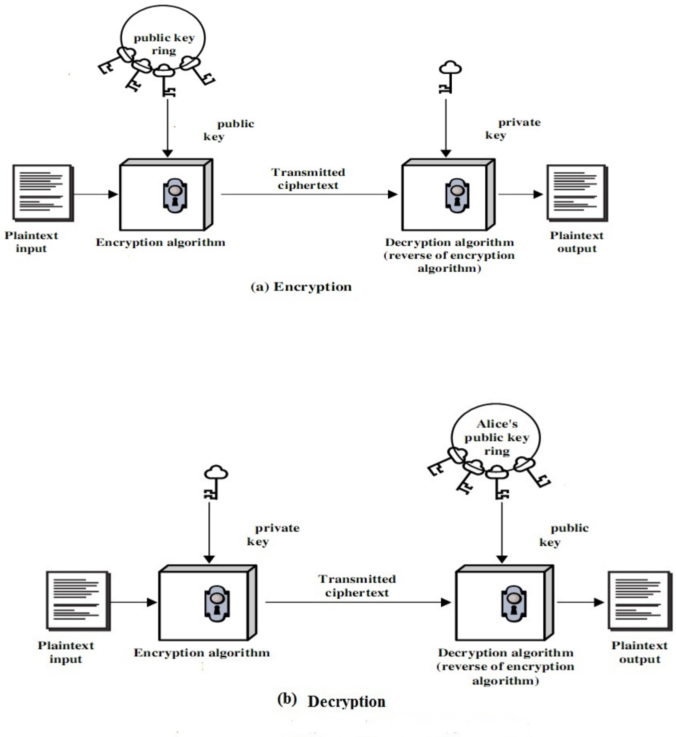

Figure 1.3: Model of Public Key Encryption

- **The disadvantages of public key cryptography**

  1. Slow do to the enormous amount of computation involved.
  2. Keys must be long (at least 1024 bits these days).
  3. There is no proof for that any public key scheme is secure.
  4. It has not been around long enough to be tested as much.

1.1.4 Classification Attacks

As we said previously in several areas there are transmitted message which may in different attacks.

There are several families of cryptanalytic attacks, the best known being the frequency analysis, differential cryptanalysis and linear cryptanalysis, the latter are often characterized by the data they require as follows:

- **Cipher text-only**: The cryptanalyst has copies of encrypted messages, it can make assumptions about the original messages it does not have. Cryptanalysis is more difficult by the lack of information available.

- **Known-plaintext attack**: The cryptanalyst has messages or parts of messages in plain and encrypted versions. Linear cryptanalysis is part of this category.

- **Chosen-plaintext attack**: the cryptanalyst has text messages, it can generate the encrypted versions of these messages with the algorithm that can therefore be considered as a black box. Differential cryptanalysis is an example of attack chosen plaintext.

- **Chosen-ciphertext attack**: The cryptanalyst has encrypted messages and calls for clear version of some of these messages to lead the attack.

1.1.5 The Importance of Encryption

With the rapid development of multimedia exchanges, it is necessary to dispose secure systems to protect data and ensure the security of transfer; so it would be careless to undervalued the role that encryption technology plays in safeguarding our public and private networks. it is important because it protects things such as email, medical record, confidential corporate information, data on personal buying habits and transaction, legal documents, credit histories , and government and regulatory agency databases. securing this data is critical to peace of mind in communicating business and personal information.

1.2 Signals and Systems

We are all immersed in a sea of signals. All of us from the smallest living unit, a cell, to the most complex living organism(humans) are all time time receiving signals and are processing them. Survival of any living organism depends upon processing the signals appropriately. So what is signal? To define this precisely is a difficult task. Anything which carries information is a signal. In this section we will learn some of the mathematical representations of the signals, which has been found very useful in making information processing systems. But before that we must distinct between signals and systems and the relation between them:

A signal is a function representing a physical quantity, and it contains information about the behavior or nature of the phenomenon. From a communication point of view a signal is any function that carries some information; where A system is a function that maps signals from its domain—its input signals—into signals in its range—its output signals. Both the domain and the range are sets of signals (signal spaces). Thus, systems are functions that operate on functions.

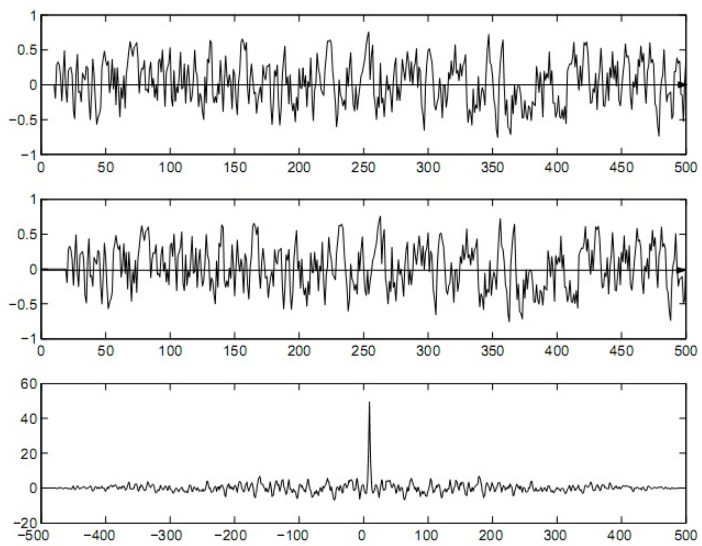

Figure 1.4: Model of Signals

1.2.1 Signals

Definition 2 *A signal is a real (or complex) valued function of one or more real variable(s).*

- When the function depends on a single variable, the signal is said to be one- dimensional.

  A speech signal, daily maximum temperature, annual rainfall at a place, are all examples of a one dimensional signal.

- When the function depends on two or more variables,the signal is said to be multi-dimensional.

An image is representing the two dimensional signal,vertical and horizontal coordinates representing the two dimensions. Our physical world is four dimensional (three spatial and one temporal).

Mathematically

Definition 3 *A signal is a sequence of numbers* $\{x(n)\}_{n\in\mathbb{Z}}$ *satisfying* $\sum_{n\in\mathbb{Z}} |x(n)| < \infty$. *Such a sequence is also referred to as being in* ^{1}(Z), *or just in* ^{1}. *A sequence* $\{x(n)\}$ *satisfying* $\sum_{n\in\mathbb{Z}} |x(n)|^2 < \infty$ *is referred to as an* ^{2}) *sequence.*

1.2.2 Classification of Signals

Here we introduce briey from Baraniuk [2009] some of the basic classifications of signals and the most important properties of these signals are explained.

1. **Continuous-Time and Discrete-Time**

   As the names suggest,

   - A continuous-time signal will contain a value for all real numbers along the time axis.

     In contrast to this,

   - A discrete-time signal is often created by using the sampling theorem to sample a continuous signal, so it will only have values at equally spaced intervals along the time axis.

2. **Analog and Digital**

   There are similarity between analog and digital, and continuous-time and discrete-time signals; but here with respect to the value of the function (y-axis). Analog corresponds to a continuous y-axis, while digital corresponds to a discrete y-axis.We have an example of a digital signal is a binary sequence, where the values of the function can only be one or zero.

3. **Periodic and Aperiodic**

   Periodic signals has repeating with a period T, while aperiodic, or non-periodic, signals don't. We can define a periodic function through the following mathematical expression, where we take t any number and T is a positive constant: $f(t) = f(\mathrm{T}+t)$. The fundamental period of our function$f(t)$, is the smallest value of T that allows the above mathematical expression, to be true.

4. **Causal and Anti-causal and Non-causal**

   - Causal signals are signals that are zero for all negative time.
   - Conversely, anti-causal are signals that are zero for all positive time.
   - But Non-causal signals are signals that have nonzero values in both positive and negative time.

5. **Even and Odd**

   An even signal is any signal f satisfying: $f(-t) = f(t)$. Which means that even signals are symmetric around the vertical axis. On the other hand, an odd signal is a signal f such that $f(t) = -(f(-t))$. Using the definitions of even and odd signals, we can show that any signal can be written as a combination of an even and odd signal. That is, every signal has an odd-even decomposition. Demonstration of this, drive us to look no further than a single equation.

$$f(t) = \frac{1}{2}(f(t) + f(-t) + \frac{1}{2}(f(t) - f(-t))$$

   By multiplying and adding this expression out, it can be shown to be true. Also, it can be shown that:

   - $f(t) + f(-t)$ fulfills the requirement of an even function,while
   - $f(t) - f(-t)$ fulfills the requirement of an odd function.

6. **Deterministic and Random**

   - Deterministic signal is a signal in which each value of the signal is fixed and can be determined by a mathematical expression, rule, or table. Because of this the future values of the signal can be calculated from past values with complete confidence.
   - On the other hand, a random signal has a lot of uncertainty about its behavior. The future values of a random signal cannot be accurately predicted and can usually only be guessed based on the averages of sets of signals.

7. **Right-Handed and Left-Handed**

   A right-handed signal and left-handed signal are defined by signals whose value is zero between a given variable and positive or negative infinity. Mathematically, a right-handed signal is defined as any signal such that $f(t) = 0$ for $t < t_1 < \infty$, and a left-handed signal is defined as any signal such that $f(t) = 0$ for $t > t1 > -\infty$.

8. **Finite and Infinite Length**

   As the name applies, signals can be characterized as to whether they have a finite or infinite length set of values. We use finite length signals when dealing with discrete-time signals or a given sequence of values. Mathematically speaking, $f(t)$ is a finite-length signal if it is nonzero over a finite interval $t_1 < f(t) < t_2$; where $t_1 > -\infty$ and $t_2 < \infty$. Likewise, an infinite-length signal, is defined as nonzero over all real numbers: $-\infty \le f(t) \le \infty$

1.2.3 Systems

Definition 4 *A System is any physical set of components that takes a signal, and produces a signal. In terms of engineering, the input is generally some electrical signal x, and the output is another electrical signal (response) y. However, this may not always be the case.*

Mathematically,

Definition 5 *A system is any transformation* T *that takes an input signal* $x(n)$ *to an output signal* $y(n)$. *We write* $\mathrm{T}x(n) = y(n)$.

1.2.4 Proprieties Of Systems

1. **Linearity**: a system is linear if

$$\mathrm{T}(ax_1 + bx_2)(n) = a\mathrm{T}x_1(n) + b\mathrm{T}x_2(n)$$

   where $x_1, x_2 \in {}^1$, and a, b are constants.

2. **Stability**: a linear system T is stable if for some $\mathrm{C} > 0$,

$$\sum_{n\in\mathbb{Z}} |\mathrm{T}x(n)| \leq \mathrm{C} \sum_{n\in\mathbb{Z}} |x(n)|$$

   for all signals $x(n)$.

3. **Translation**: for $k \in \mathbb{Z}$, the translation operator τ_k, for signals is $\tau_k x(n) = x(n-k)$.

4. **LTI**: a linear translation–invariant system is a linear system T for which:

$$\mathrm{T}(\tau_k x)(n) = \tau - k(\mathrm{T}x)(n) = \mathrm{T}x(n-k)$$

5. **Convolution**: the convolution of signals $x_1, x_2 \in {}^1$, denoted: $x_1 * x_2(n)$, is

$$y(n) = x_1 * x_2(n) = \sum_{n\in\mathbb{Z}} x_1(k)x_2(n-k)$$

   .

1.3 Blind Source Separation Problem

Blind Source Separation (BSS) is a prominent problem in signal processing. In the past few decades, it was applied to many fields, in which separation of compound signals, simultaneously observed by different sensors, is of interest. The problem can be considered as built-up of three physical elements: sources (also called transmitters), sensors (also called receivers) and communication channels which reflect the properties of the physical medium propagating the signals form the sources to the sensors.

The signals detected by the sensors are commonly referred to as observations and are assumed to be algebraic combinations of the unknown sources signals.

BSS approach assumes limited a priory information on the communication channels (linearity, memory properties...) and tries to reconstruct the source signals out of the detected signals only.

Analysis of the communication channels is important mainly for selection of a proper processing technique.

1.3.1 Blind Source Separation Problem

Definition 6 *The blind source separation (BSS) problem consists on recovering a set of source signals* $s(\tau) = (s_1(\tau), \ldots, s_m(\tau))^T$ *from a set of mixtures* $x(\tau) = (x_1(\tau), \ldots, x_n(\tau))^T$ *formed with a mixing matrix* A*:*

$$x(\tau) = A^T s(\tau)$$

where $\tau \in$ *tau is an index representing temporal or spatial variation of the signals.*

The term blind means that the values of the mixing matrix A and the source signals $s(\tau)$ are unknown.

The (BSS) problem is solved by finding an unmixing matrix W to reconstruct the sources via the transformation:

$$y(\tau) = W^T x(\tau)$$

such that

$$y(\tau) = \mathrm{DP}s(\tau)$$

where D is a diagonal matrix, and P is a permutation matrix. This means that the reconstructed signals do not keep the original order of the source signals but their *"wave"* form. A general approach to solve the BSS problem is assuming that the source signals $s_i(\tau)$ satisfy a property P, and that they minimize (maximize) a measure $q(s)$ related to the property P . Thus, the BSS problem is yet regarded as an optimization problem: the unmixing matrix W is an optimal parameter used to transform linearly the mixtures $x(\tau)$ into the signals $y(\tau)$, which minimizes (maximizes) the *"quality"* of the reconstructed signals.

1.4 Genetic Algorithm

1.4.1 The Fundamental Theorem of Genetic Algorithms

Genetic algorithms (G.A) are a type of optimisation algorithm, meaning they are used to find the optimal solution(s) to given computational problem that maximizes or minimizes a particular function. Genetic algorithms represent one branch of the field of study called *"evolutionary" "computation"* KINNEAR [1994], in that they imitate the biological processes of reproduction and natural selection to solve for the *fittest* solutions. Like in evolution, many of a genetic algorithm's processes are random, however this optimization technique allows one to set the level of randomization and the level of control.
These algorithms are far more powerful and efficient than random search and exhaustive search algorithms, yet require no extra information about the given problem. these feature allows them to find solutions to problem that other optimization methods cannot handle due to a lack of continuity, derivability, linearity, or other featuresCARR [2014].
Genetic algorithms are typically characterized by the following aspectsRANGEL-MERINO

et collab. [2005]:

1. The G.A work with the base in the code of the variable group and not with the variables in themselves.

2. The G.A work with a set of potential solutions (population) instead of trying to improve a single solution.

3. The G.A don't use information obtained directly from object function, of its derivatives, or of any other auxiliary knowledge of the same one

4. The G.A apply probabilistic transition rules, not deterministic rules

1.4.2 Working Principle of Genetic Algorithms

The Workability of genetic algorithms is base on Darwinian's theory of survival of the fittest. Genetic algorithms my contain a chromosome, a gene, set of population, fitness function, breeding, mutation and selection.

Genetic algorithms begin with a set of solutions represented by chromosomes called population. solutions from one population are taken and used to form a new population, which is motivated by the possibility that new population will be better than the old one. Further, solutions are selected according to their fitness to form new solutions, that is offspring (details or steps of work are found in MALHOTRA et collab. [2011])

1.5 Références

BARANIUK, R. 2009, *Signals and systems*, Orange Grove Books. 8

CARR, J. 2014, «An introduction to genetic algorithms», *See: karczmarczuk. users. greyc. fr/TEACH/IAD/GenDoc/carrGenet. pdf*. 13

KINNEAR, K. E. 1994, *Advances in genetic programming*, vol. 1, MIT press. 13

MALHOTRA, R., N. SINGH et Y. SINGH. 2011, «Genetic algorithms: Concepts, design for optimization of process controllers», *Computer and Information Science*, vol. 4, 2, p. 39. 14

RANGEL-MERINO, A., J. LÓPEZ-BONILLA et R. L. Y MIRANDA. 2005, «Optimization method based on genetic algorithms», *Apeiron*, vol. 12, 4, p. 393–408. 13

Chapter 2

Wavelets Transform

Never memorize something that

you can look up.

If we knew what it was we were

doing, it would not be called

research, would it?

Albert Einstein

Sommaire

In recent years wavelets analysis (also called wavelets theory, or just wavelets) have emerged as a powerful mathematical tool and a new framework within a common link is established between diversified problems that are of interest to different fields including electrical engineering (signal processing and image, data compression, sub-band coding, radar, optics....), mathematical analysis (harmonic analysis, operator theory, partial differential equations...) and physics (fractals,quantum field theory, turbulence...). this concept is based on analysing-localized variation of power within a time by decomposing a time series into time-frequency spaces, one is able to determine both the dominant modes of variability and how those mode vary in time. Mathematically, wavelets are functions that satisfy certain mathematical requirement and are used in representing data or other functions.

2.1 Multi-resolution Analysis

The method of multi-resolution is to represent a function (Signal) with a collection of coefficients, where each of which provide information about the position as well as the frequency of signal (function). Multi-resolution analysis (MRA) is a method for $\mathbb{L}^2$- approximation of functions with arbitrary precision; MRA give approximation on different scales in such a way that an approximation on a fine scale can be obtained by adding the " details" to an approximation on a coarse scale.

2.1.1 Multi-resolution Analysis and Orthonormal Wavelets Bases

The Scaling Function and the Subspaces V_j

A multi-resolution analysis of $\mathbb{L}^2(\mathbb{R})$ is a family $M = \{V_j\}_{j\in\mathbb{Z}}$ of embedded vectorial subspaces with the properties below that we can group in three blocks :

1. $\{V_j\}_j \in \mathbb{Z}$ is a set of approximation spaces i.e:-
    - V_j is a closed subspace of $\mathbb{L}^2$
    - $V_j \subset V_{j-1}$
    - $\overline{\bigcup_{j\in\mathbb{Z}} V_j} = \mathbb{L}^2(\mathbb{R})$ and $\bigcap_{j\in\mathbb{Z}} V_j = \{0\}$

2. The V_j spaces are obtained by dyadic dilatation or contraction of the function of the single space, this property relates to the translation of functions.

$$\forall j \in \mathbb{Z}, v(t) \in V_j \Longleftrightarrow v(2t) \in V_{j-1}$$

3. It suppose the existence of function, with makes it possible to build a bases of V_0 by integer translation : $\phi \in V_0$ such that $\{\phi(t-k\}_{k\in\mathbb{Z}}$ is a Riesz base of V_0 , where ϕ is called *scaling function*.

   Since $\phi \in V_1 \subset V_0$, a sequence (h_k) in ^{2} exists such that the scaling function satisfies

$$\phi(x) = 2\sum_k h_k \phi(2x-k)$$

under conditions:

$$\sum_k h_k = 1$$

$$\int_{-\infty}^{+\infty} \phi(x)dx = 1$$

The Relation of $\hat{\phi}$ with m_0

Taking the Fourier transform of functional equation:

$$\phi(x) = \sqrt{2}\sum_k h_k \phi(2x-k)$$

gives,

$$\hat{\phi}(\omega) = \frac{1}{\sqrt{2}}\sum_k h_k e^{-ik\frac{\omega}{2}}\hat{\phi}(\frac{\omega}{2})$$

which can be written as:

$$\hat{\phi}(\omega) = m_0(\frac{\omega}{2})\hat{\phi}(\frac{\omega}{2}) \tag{2.1}$$

whith

$$m_0(\omega) = \frac{1}{\sqrt{2}}\sum_k h_k e^{-ik\omega}$$

The function m_0 is 2π-periodic, and $m_0 \in \mathbb{L}^2([0,2\pi])$, because $\sum_{k\in\mathbb{Z}} |h_k|^2 < \infty$ We also know that, by definition,

$$\int_{-\infty}^{+\infty} \phi(x)dx = 1$$

Hence, $\hat{\phi}(0) = 1$, and therefore

$$m_0(0) = 1 \tag{2.2}$$

recursively on values: $\frac{\omega}{2}, \frac{\omega}{4}, \ldots$. we get $\hat{\phi}(\omega = m_0(\frac{\omega}{2}) m_0(\frac{\omega}{4}) \hat{\phi}(\frac{\omega}{4})$ and arrive at the infinite product formula:

$$\hat{\phi}(\omega) = \frac{1}{\sqrt{2\pi}} \prod_{j=1}^{\infty} m_0(2^{-j}\omega)$$

A very important point is to show that this product converge to a function in $\mathbb{L}^2(\mathbb{R})$. Details of this can be found in Daubechies [1992]

Example of Scaling Function

- The cardinal B-spline of order 1 is the box function $N_1(x) = \chi_{[0,1]}(x)$. For $m > 1$ the cardinal B-spline N_m is defined recursively as a convolution:

  $$N_m = N_{m-1} * N_1$$

  this function satisfy,

  $$N_m(x) = 2^{m-1} \sum_{k=0}^{m} \binom{m}{k} N_m(2x-k)$$

  and

  $$\hat{N}_m(\omega) = (\frac{1-e^{-i\omega}}{i\omega})^m.$$

- Classical example, is the Shannon sampling function.

  $$\phi(x) = \frac{sin(\pi x)}{\pi x}$$

with

$$\hat{\phi}(\omega) = \chi_{[-\pi,\pi]}(\omega)$$

We may take

$$m_0(\omega) = \chi_{[\frac{-\pi}{2},\frac{\pi}{2}]}(\omega) \text{ for } \omega \in [-\pi,\pi]$$

and consequently,

$$h_{2k} = \frac{1}{2}\delta_k \text{ and } h_{2k+1} = \frac{(-1)^k}{(2k+1)\pi} \text{ for } k \in \mathbb{Z}.$$

The Wavelet Function and the Detail Spaces W_j

We will use W_j to denote a space complimenting V_j in V_{j-1}, i.e: a space that satisfies

$$V_{j-1} = V_j \oplus W_j$$

In other words, each element of V_{j-1} can be written (in a unique way) as the sum of an element of V_j and an element of W_j. We note that the spaces W_j themselves are not necessary unique, they may be several ways to complement V_j in V_{j-1}.

the space W_j contains the "$detail$" information needed to go from an approximation at resolution j to an approximation at resolution $j-1$. Consequently,

$$\bigoplus_j W_j = \mathbb{L}^2(\mathbb{R})$$

A function ψ is *wavelet* if the collection of functions $\{\psi(x-k)\ k \in \mathbb{Z}\}$ is a Riesz basis of W_0.

The collection of wavelet functions $\{\psi_{j,k}\ / j,k \in \mathbb{Z}\}$ is then a Riesz basis of $\mathbb{L}^2(\mathbb{R})$.

Since the wavelets ψ is an element of V_1, a sequence $(g_k) \in {}^2(\mathbb{Z})$ exists such that:

$$\psi(x) = 2\sum_k g_k \phi(2x-k)$$

The Relations of $\hat{\psi}$ with m_1

Similarly, if we distinct tow scales relations for the wavelet function ψ in the frequency domain,

$$\psi(x) = \sqrt{2}\sum_k g_k \psi(2x-k)$$

we get

$$\hat{\psi}(\omega) = \frac{1}{\sqrt{2}}\sum_k g_k e^{-ik\frac{\omega}{2}}\hat{\phi}(\frac{\omega}{2})$$

or:

$$\hat{\psi}(\omega) = m_1(\frac{\omega}{2})\hat{\phi}(\frac{\omega}{2}) \tag{2.3}$$

whith

$$m_1(\omega) = \frac{1}{\sqrt{2}}\sum_k g_k e^{-ik\omega}$$

Where the function m_1 is also 2π-periodic.

Note that, $\hat{\psi}$ is defined in terms of $\hat{\phi}$ through m_1, in the same way ψ is defined in terms of ϕ through (g_k) in the spacial domain.

1. The definition of $\psi_{j,k}$ is similar to the one of $\phi_{j,k}$.

2. Each space V_j and W_j has a complement in $\mathbb{L}^2(\mathbb{R})$ denoted by V_j^c and W_j^c, respectively.

3. We have:

$$V_j^c = \bigoplus_{i=j}^{\infty} W_i \text{ and } W_j^c = \bigoplus_{i\neq j}^{\infty} W_i$$

4. We define P_j as the projection operator onto V_j and parallel to V_j^c, and Q_j as the projection operator onto W_j and parallel to W_j^c, so a function f can be written as:

$$f(x) = \sum_j Q_j f(x) = \sum_{j,k} D_k^j \psi_{j,k}(x)$$

2.1.2 Orthogonal Wavelets

The class of orthogonal wavelets is particularly interesting. starting by introducing the concept of an *orthogonal multi-resolutionanalysis.*

This is a multi-resolution analysis where the wavelet spaces W_j is the orthogonal of complement of V_j in V_{j-1}. Consequently, the spaces W_j with $j \in \mathbb{Z}$ are all mutually orthogonal, the projections P_j and Q_j are orthogonal, and the expansion

$$f(x) = \sum_j Q_j f(x)$$

is an orthogonal expansion .

In this section we give series of properties for the $\{W_j\}_{j\in\mathbb{Z}}$ spaces which are useful for the geometrical understanding of the construction:-

$$w(t) \in W_j \Longleftrightarrow w(2t) \in W_{j-1} \tag{2.4}$$

$$W_j \perp W_k, j \neq k \tag{2.5}$$

$$W_j \perp V_k, j \leq k \tag{2.6}$$

$$V_J = V_k \bigoplus W_k .... \bigoplus W_{J+1}, J < k \tag{2.7}$$

$$V_J = \bigoplus_{j=J+1}^{+\infty} W_j \tag{2.8}$$

$$\mathbb{L}^2(\mathbb{R}) = V_J \bigoplus \{ \bigoplus_{j=-\infty}^{J} W_j \} \tag{2.9}$$

$$\mathbb{L}^2(\mathbb{R}) = \bigoplus_{j=-\infty}^{+\infty} W_j \tag{2.10}$$

Let us note $A^j = P_{V_j}(f)$ and $D^j = P_{W_j}(f)$, the orthogonal projections of $f \in \mathbb{L}^2$ on spaces V_j and W_j respectively; then we have:-

$$A^{j-1} = A^j + D^j \text{ with } A^j \perp D^j$$

Spaces $\{V_j\}$ are approximation spaces in the following sens: A^j converge to f in $\mathbb{L}^2(\mathbb{R})$ when j tends to $\{-\infty\}$; In the same way, spaces $\{W_j\}$ are detail spaces in the sens that in $\mathbb{L}^2(\mathbb{R})$ we have , on the one hand, D^j which converge to 0 when j tends to $\{-\infty\}$ and on the other hand, $f = A^J + \sum_{\{-\infty\}}^{J} D^j$. In the word, for a fixed level of approximation J, the D^j are correction to be added to the approximation to find f. Now we represent the fundamental result associated with multi-resolution analysis; noting $f_{j,k}(t) = 2^{\frac{-j}{2}} f(2^{-j}t - k)$ for any function.

Orthonormal Wavelets Bases

Let M be a multi-resolution analysis of $\mathbb{L}^2(\mathbb{R})$. Starting from the sequence (g), we can build a scaling function ϕ then a wavelet ψ such that:- $\forall J \in \mathbb{Z}, \{\{\phi_{j,k}\}_{k\in\mathbb{Z}}, \{\psi_{j,k}\}_{j,k\in\mathbb{Z}}, j \leq J\}$ is an orthonormal base of $\mathbb{L}^2(\mathbb{R})$ and $\{\psi_{j,k}\}_{j,k\in\mathbb{Z}}$is an orthonormal wavelets base of $\mathbb{L}^2(\mathbb{R})$.

2.2 Multi-resolution Analysis's Construction

Here we establish on the links between the concept of multi-resolution analysis and the orthogonal wavelet, and we propose a manner of building the second starting from the first. This construction also shows the fundamental part played by the tow-scales equations in the time and frequency domain; starting by the construction of the scaling function.

2.2.1 Construction of the Scaling Function

Let us consider the scaling function ϕ defined using its Fourier transform $\hat{\phi}$ by: $\hat{\phi} = \frac{\hat{g}(\omega)}{(\sum_{k\in\mathbb{Z}} |\hat{g}(\omega+k)|^2)^{\frac{1}{2}}}$
Then,

- $\phi \in V_0$

- $\{\phi_{0,k} = \phi(t-k)\}_{k\in\mathbb{Z}}$is an orthonormal base of V_0

- tow-scale equation for ϕ:-

$$\exists! h = \{h_k\}_{k\in\mathbb{Z}}, h \in l^2(\mathbb{Z})$$

  such that:

$$\tfrac{1}{2}\phi(\tfrac{t}{2}) = \textstyle\sum_{k\in\mathbb{Z}} h_k \phi(t-k) \text{ in } \mathbb{L}^2$$

- $m_0(\omega) = \sum h_k e^{-2i\pi\omega}$ is periodic with period 1, $m_0 \in \mathbb{L}^2(0,1)$ and verifies

$$\hat{\phi}(2\omega) = m_0(\omega)\hat{\phi}(\omega) \qquad p.p.\omega \in \mathbb{R}$$

$$|m_0(\omega)|^2 + |m_0(\omega + \frac{1}{2})|^2 = 1 \qquad p.p.\omega \in \mathbb{R}$$

- more generally, $\{\forall j \in \mathbb{Z}, \phi_{j,k} = 2^{\frac{-j}{2}}\phi(2^{-j}t-k)\}_{k\in\mathbb{Z}}$ is an orthonormal base of V_j

2.2.2 Characterization of m_0

In order to define the properties of m_0, the fact that $\phi(x-k)$, the integer translates of ϕ from an orthonormal basis of V_0 is used. this impose some restrictions on m_0.

$$\int_{-\infty}^{\infty} \phi(x)\overline{\phi(x-k)}dx = \int_{-\infty}^{\infty} |\hat{\phi}(\xi)|^2 e^{ik\xi} d\xi$$
$$= \delta_{k,0}$$
$$= \int_{-\infty}^{\infty} e^{ik\xi} \sum_{l\in\mathbb{Z}} |\hat{\phi}(\xi + 2\pi l)|^2 d\xi$$
$$= \delta_{k,0}$$

The above equation implies that,

$$\sum_{l} |\hat{\phi}(\xi + 2\pi l)|^2 = \frac{1}{2\pi} \tag{2.11}$$

substituting equation 2.1 in the above equation, with $\omega = \frac{\xi}{2}$, we have

$$\sum_{l} |m_0(\omega + \pi l)|^2 |\hat{\phi}(\omega + \pi l)|^2 = \frac{1}{2\pi}$$

We can split the sum into terms with even and odd l, and because m_0 is 2π-periodic we have:

$$|m_0(\omega)|^2 \sum_{l} |\hat{\phi}(\omega + 2l\pi)|^2 + |m_0(\omega+\pi)|^2 \sum_{l} |\hat{\phi}(\omega + (2l+1)\pi)|^2 = \frac{1}{2\pi}$$

Substituting 2.11 and simplifying, we obtain,

$$|m_0(\omega)|^2 + |m_0(\omega+\pi)|^2 = 1 \tag{2.12}$$

This is the first important condition characterizing m_0, via orthonormality of ϕ. If we put together equation 2.2 with 2.11, we obtain that,

$$m_0(\pi) = 0$$

This gives us a hint that m_0 is of the form

$$m_0(\omega) = (\frac{1+e^{i\omega}}{2})^m Q(\omega)$$

with $m \geq 1$, and where Q is a 2π-periodic function. (Observe that $e^{i\pi} = -1$. So, when $\omega = \pi$ the first term vanishes, and the product has to vanish.) We impose $Q(0) = 1$, to ensure that $m(0) = 1$, and also $Q(\pi) \neq 0$, so that the multiplicity of the root of m_0 at π is not increased by Q.

2.2.3 Construction of the Wavelets

Wavelet ψ is defined using its Fourier transform $\hat{\psi}$. Let ρ be a periodic function with a period of $\frac{1}{2}$, for almost all $\omega \in \mathbb{R}$, and let us pose $m_1(\omega) = \rho(\omega) e^{-2i\pi k\omega} \overline{m_0(\omega + \frac{1}{2})}$ and define: $\hat{\psi} = m_1(\frac{\omega}{2})\hat{\phi}(\frac{\omega}{2})$

- $\psi \in W_0$

- $\{\psi_{0,k} = \psi(t-k)\}_{k\in\mathbb{Z}}$ is an orthonormal base of W_0

- tow-scale equation for ψ:-

$$\exists! g = \{g_k\}_{k\in\mathbb{Z}}, g \in l^2(\mathbb{Z}) \text{ such that: } m_1(\omega) = \sum g_k e^{-2i\pi k\omega} \text{ and}$$

$$\tfrac{1}{2}\psi(\tfrac{t}{2}) = \textstyle\sum_{k\in\mathbb{Z}} g_k \phi(t-k) \text{ in } \mathbb{L}^2$$

- m_1 is periodic with period of 1, $m_0 \in \mathbb{L}^2(0,1)$ and verifies

$$|m_1(\omega)|^2 + |m_1(\omega + \frac{1}{2})|^2 = 1 \qquad p.p.\omega \in \mathbb{R}$$

$$m_0(\omega)\overline{m_1(\omega)} + m_0(\omega + \tfrac{1}{2})\overline{m_1(\omega + \tfrac{1}{2})} = 0 \text{ for almost all } \omega \in \mathbb{R}$$

- more generally, $\{\forall j \in \mathbb{Z}, \psi_{j,k} = 2^{\frac{-j}{2}}\psi(2^{-j}t - k)\}_{k\in\mathbb{Z}}$ is an orthonormal base of W_j

- $\{\psi_{j,k}\}_{j,k\in\mathbb{Z}}$ is an orthonormal base of $\mathbb{L}^2(\mathbb{R})$

2.2.4 Characterization of m_1

To link m_0 with m_1, we use the orthogonality between ϕ and ψ. More precisely, the constraint that $W_0 \perp V_0$ implies that $\psi \perp \phi_{0,k}$ and

$$\int_{-\infty}^{\infty} \hat{\psi}(\omega)\overline{\hat{\phi}(\omega)}e^{ik\omega}d\omega = 0$$

or, in terms of the Fourier series

$$\int_{0}^{2\pi} e^{ik\omega}\sum_{l\in\mathbb{Z}} \hat{\psi}(\omega+2\pi l)\overline{\hat{\phi}(\omega+2\pi l)}d\omega = 0$$

hence

$$\sum_{l} \hat{\psi}(\omega+2\pi l)\overline{\hat{\phi}(\omega+2\pi l)} = 0$$

for all $\omega \in \mathbb{R}$;

Substituting in the above equation the expression 2.1 and 2.3 of $\hat{\phi}$ and $\hat{\psi}$ in terms of, respectively m_0 and m_1 we obtain after regrouping the sums for even and odd l,

$$m_1(\omega)\overline{m_0(\omega)} + m_1(\omega+\pi)\overline{m_0(\omega+\pi)} = 0 \tag{2.13}$$

This is the second important condition characterizing m_0 and m_1.

We also know that, $\overline{m_0(\omega)}$ and $\overline{m_0(\omega+\pi)}$ can not be zero simultaneously because of 2.12 therefore m_1 can be written using m_0 and a function λ

$$m_1(\omega) = \lambda(\omega)\overline{m_0(\omega+\pi)} = 0$$

such that λ satisfies

$$\lambda(\omega) + \lambda(\omega+\pi)$$

The simple choice of λ is $\lambda(\omega) = e^{i\omega}$, which gives m_1, satisfying the above equation

$$m_1(\omega) = e^{-i\omega}\overline{m_0(\omega+\pi)}, \tag{2.14}$$

Note that m_1 is defined in term of m_0, as expected. This also give $\hat{\psi}$ in term of $\hat{\phi}$

$$\hat{\psi}(\omega) = e^{i\frac{\omega}{2}}\overline{m_0(\frac{\omega}{2}+\pi)}\hat{\phi}(\frac{\omega}{2})$$

From the above relations, we can construct an orthogonal wavelet from a scaling function ϕ, using 2.14 and choosing the coefficients $\{g_k\}$ as :

$$g_n = (-1)^k h_{-k+1}$$

that is

$$\psi(x) = \sqrt{2}\sum_k (-1)^k h_{-k+1}\phi(2x-k)$$

We conclude that, since m_1 is trivially defined from m_0, all we need to construct orthogonal scale and wavelet bases, is to find a function m_0 satisfying 2.12 and 2.13, or equivalently, find the coefficients (h_k) of the representation sequence of m_0.

2.3 Bi-orthogonal Multi-resolution Analysis and Filters

Bi-orthogonal wavelets constitute a generalisation of orthogonal wavelet. Under this framework, instead of a signal orthogonal basis, a pair of dual bi-orthogonal basis functions is employed: One for the analysis step and other for the synthesis step, i.e: we have reciprocal frame as defined in MRA.

Recall that, in the context of orthogonal multi-resolution analysis we have defined the projection operator onto the subspaces V_j and W_j respectively.

$$ProjV_j(f) = \sum_k \langle f, \phi_{j,k}\rangle \phi_{j,k} \text{ and } ProjW_j(f) = \sum_k \langle f, \psi_{j,k}\rangle \psi_{j,k}$$

Where the function ϕ and ψ perform a double duty i.e: they are used:

Analysis: compute the coefficient of the representation of f in therms of the basis ϕ and ψ of the spaces V_j and W_j respectively; and we have $a_j^k = \langle f, \phi_{j,k}\rangle$ and $d_j^k = \langle f, \psi_{j,k}\rangle$.

Synthesis: reconstruct the projection of f into V_j and W_j; from the coefficient of the representation respectively $ProjV_j(f) = a_j^k \phi_{j,k}$ and $ProjW_j(f) = d_j^k \psi_{j,k}$.

The more general framework of bi-orthogonal multi-resolution analysis employ similar projection operators: $P_j(f) = \sum_k \langle f, \phi_{j,k}\rangle \tilde{\phi}_{j,k}$ and $Q_j(f) = \sum_k \langle f, \psi_{j,k}\rangle \tilde{\psi}_{j,k}$

2.3.1 Properties of Bi-orthogonal Wavelets

Let us suppose that wavelets are constructed, and let us analyze their properties. The two families $M = \{V_j\}_{j\in\mathbb{Z}}$ and $\tilde{M} = \{\tilde{V}_j\}_{j\in\mathbb{Z}}$ are multi-resolution analysis of $\mathbb{L}^2(\mathbb{R})$. They were characterized by the property: $\mathbb{L}^2(\mathbb{R}) = V_0 + \tilde{V}_0^{\perp}$

Let us note by $V_j, W_j, \tilde{V}_j$ and $\tilde{W}_j$ the spaces generated respectively by families of functions: $\{\phi_{j,k}\}_{k\in\mathbb{Z}}, \{\psi_{j,k}\}_{k\in\mathbb{Z}}, \{\tilde{\phi}_{j,k}\}_{k\in\mathbb{Z}}$ and$\{\tilde{\phi}_{j,k}\}_{k\in\mathbb{Z}}$.

These spaces and these functions verify a set of relations highlighting multi-resolution and bi-orthogonality properties.
Let us start with the first aspect.
For each family of spaces $\{E_j\}_{j\in\mathbb{Z}}$ we pass from E_j to E_{j-1} by dilatation. We have the inclusions:

$$V_j \subset V_{j-1}, W_j \subset W_{j-1}, \tilde{V}_j \subset \tilde{V}_{j-1} \text{ and } \tilde{W}_j \subset \tilde{W}_{j-1}$$

Finally, there are the decomposition:

$$V_j = V_{j+1} \oplus W_{j+1} \text{ and } \tilde{V}_j = \tilde{V}_{j+1} \oplus \tilde{W}_{j+1}$$

note that, they are not orthogonal.

Let us now pass to the relations of duality as follow:

$$\langle \phi_{0,k}, \tilde{\phi}_{0,p}\rangle_{\mathbb{L}^2} = \delta_{k,p} (= 1 \text{ if } k = p; 0 \text{ if not})$$

The couple of spaces $(V_j, \tilde{V}_j)$ and $(W_j, \tilde{W}_j)$ satisfy

$$\langle \phi_{j,k}, \tilde{\phi}_{j,p}\rangle_{\mathbb{L}^2} = \delta_{k,p} \text{ and } \langle \psi_{j,k}, \tilde{\psi}_{j,p}\rangle_{\mathbb{L}^2} = \delta_{k,p}$$

The couple of spaces $(V_j, \tilde{W}_j)$ and $(\tilde{V}_j, \tilde{W}_j)$ are orthogonal and with this we have:-

$$\langle \phi_{j,k}, \tilde{\psi}_{j,p}\rangle_{\mathbb{L}^2} = 0 \text{ and } \langle \tilde{\phi}_{j,k}, \psi_{j,p}\rangle_{\mathbb{L}^2} = 0$$

Thanks to inclusions: $V_n \perp \tilde{W}_j$ and $\tilde{V}_n \perp W_j$ for $n \geq j$ which imply that for $n \neq j$ we have bi-orthogonality relations:

$$\langle \psi_{j,k}, \tilde{\psi}_{j,p} \rangle_{\mathbb{L}^2} = \delta_{n,j}\delta_{k,p} \text{ where-from } W_n \perp \tilde{W}_j \text{ for } n \neq j$$

The usable projections here, are oblique projection P_j to V_j parallel to the direction of $(\tilde{V}_j)^{\perp}$ which are written for a signal f:

$$P_j(f) = \sum_{k\in\mathbb{Z}} \tilde{a}_j^k \phi_{j,k} \text{ where } \tilde{a}_j^k = \langle f, \tilde{\phi}_{j,k} \rangle$$

2.3.2 Bi-orthogonality and Filters

The two pairs of scaling functions and wavelets ϕ, ψ and $\tilde{\phi}, \tilde{\psi}$ are defined recursively by the two pairs of filters m_0, m_1 and $\tilde{m}_0, \tilde{m}_1$

In the frequency domain these relations are JAWERTH et SWELDENS [1994]:

$$\hat{\phi}(\omega) = m_0(\tfrac{\omega}{2})\hat{\phi}(\tfrac{\omega}{2}),\ \hat{\psi}(\omega) = m_1(\tfrac{\omega}{2})\hat{\phi}(\tfrac{\omega}{2})$$

$$\hat{\tilde{\phi}}(\omega) = \hat{m}_0(\tfrac{\omega}{2})\hat{\tilde{\phi}}(\tfrac{\omega}{2}),\ \hat{\tilde{\psi}}(\omega) = \hat{m}_1(\tfrac{\omega}{2})\hat{\tilde{\phi}}(\tfrac{\omega}{2})$$

where,

$$m_0(\omega) = \tfrac{1}{2}\sum h_k e^{-ik\omega},\ m_1(\omega) = \tfrac{1}{2}\sum g_k e^{-ik\omega},$$

$$\tilde{m}_0(\omega) = \tfrac{1}{2}\sum \tilde{h}_k e^{-ik\omega},\ \tilde{m}_1(\omega) = \tfrac{1}{2}\sum \tilde{g}_k e^{-ik\omega},$$

By computing the Fourier Transform of inner products in equation:

$$\langle \tilde{\phi}(x), \psi(x-k) \rangle = \int \tilde{\phi}(x)\overline{\psi(x-k)}dx = 0$$

$$\langle \tilde{\psi}(x), \psi(x-k) \rangle = \int \tilde{\psi}(x)\overline{\psi(x-k)}dx = \delta_k$$

and using the same argument of the characterization of m_0 and m_1; we can see that the bi-orthogonality condition in the frequency domain is equivalent to:

$$\sum \hat{\tilde{\phi}}(\omega + 2k\pi)\overline{\hat{\phi}(\omega + 2k\pi)} = 1$$

$$\sum \hat{\tilde{\psi}}(\omega + 2k\pi)\overline{\hat{\psi}(\omega + 2k\pi)} = 1$$

$$\sum \hat{\tilde{\psi}}(\omega + 2k\pi)\overline{\hat{\phi}(\omega + 2k\pi)} = 0$$

$$\sum \hat{\tilde{\phi}}(\omega + 2k\pi)\overline{\hat{\psi}(\omega + 2k\pi)} = 0$$

This means that the filters m_0, m_1 and their duals $\tilde{m}_0$ and $\tilde{m}_1$ have to satisfy:

$$\tilde{m}_0(\omega)\overline{m_0(\omega)} + \tilde{m}_0(\omega+\pi)\overline{m_0(\omega+\pi)} = 1$$

$$\tilde{m}_1(\omega)\overline{m_1(\omega)} + \tilde{m}_1(\omega+\pi)\overline{m_1(\omega+\pi)} = 1$$

$$\tilde{m}_1(\omega)\overline{m_0(\omega)} + \tilde{m}_1(\omega+\pi)\overline{m_0(\omega+\pi)} = 0$$

$$\tilde{m}_0(\omega)\overline{m_1(\omega)} + \tilde{m}_0(\omega+\pi)\overline{m_1(\omega+\pi)} = 0$$

The set of equations above can be written in Matrix form as:

$$\forall \omega \in \mathbb{R}; \begin{bmatrix} \tilde{m}_0(\omega) & \tilde{m}_0(\omega+\pi) \\ \tilde{m}_1(\omega) & \tilde{m}_1(\omega+\pi) \end{bmatrix} \overline{\begin{bmatrix} m_0(\omega) & m_1(\omega) \\ m_0(\omega+\pi) & m_1(\omega+\pi) \end{bmatrix}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Or

$$\tilde{\mathrm{M}}(\omega)\overline{\mathrm{M}^t(\omega)} = \mathrm{I}$$

Where M is the modulation matrix introduced as follow:

$$\mathrm{M}(\omega) = \begin{bmatrix} m_0(\omega) & m_0(\omega+\pi) \\ m_1(\omega) & m_1(\omega+\pi) \end{bmatrix}$$

By interchanging the matrices on the left-hand side, we get:

$$\forall \omega \in \mathbb{R}, \begin{cases} \overline{m_0(\omega)}\tilde{m}_0(\omega) + \overline{m_1(\omega)}\tilde{m}_1(\omega) = 1 \\ \overline{m_0(\omega)}\tilde{m}_0(\omega+\pi) + \overline{m_1(\omega)}\tilde{m}_1(\omega+\pi) = 1 \end{cases} \tag{2.15}$$

Note that, the orthogonal case corresponds to M being a unitary matrix. Crammer's rule now states that:

$$\tilde{m}_0(\omega) = \frac{\overline{m_1(\omega+\pi)}}{\overline{\Delta(\omega)}}$$

and

$$\tilde{m}_1(\omega) = -\frac{\overline{m_0(\omega+\pi)}}{\overline{\Delta(\omega)}}$$

Where

$$\Delta(\omega) = det\mathrm{M}(\omega)$$

The fact that the wavelets form a basis for the complementary spaces ensures that Δ does not vanish. The projection operators take the form:

$$\mathrm{P}_j f(x) = \sum_k \langle f, \tilde{\phi}_{j,k}\rangle \phi_{j,k} \text{ and } \mathrm{Q}_j f(x) = \sum_k \langle f, \tilde{\psi}_{j,k}\rangle \psi_{j,k}$$

and

$$f = \sum_{j,k} \langle f, \tilde{\psi}_{j,k}\rangle \psi_{j,k}$$

Not that this can be viewed as a *discrete wavelet transform* and that the conditions on ψ are less restrictive than in the orthogonal case. From the equations $\langle \tilde{\phi}_{j,l}, \phi_{j,l'}\rangle = \delta_{l-l'}$ and $\langle \tilde{\psi}_{j,l}, \psi_{j',l'}\rangle = \delta_{j-j'}\delta_{l-l'}$ such that: $j, j', l, l' \in \mathbb{Z}$ we see that:

$$\tilde{h}_{k'-2k} = \langle \tilde{\phi}(x-k), \phi(2x-k')\rangle \text{ and } \tilde{g}_{k-2k'} = \langle \tilde{\psi}(x-k), \phi(2x-k')\rangle$$

In particular, by writing $\phi(2x-k) \in \mathrm{V}_1$ in the bases of V_0 and W_0, we obtain that

$$\phi(2x-k') = \sum \tilde{h}_{k-2k'}\phi(x-k) + \sum \tilde{g}_{k-2k'}\psi(x-k)$$

2.4 The Discrete Wavelet Transform (DWT)

2.4.1 One Dimensional DWT

Discrete wavelet transform is computed with a cascade of filtering followed by a factor 2 sub-simpling KOCIOŁEK et collab. [2001]

where,

- H and L denote respectively high and low pass filters

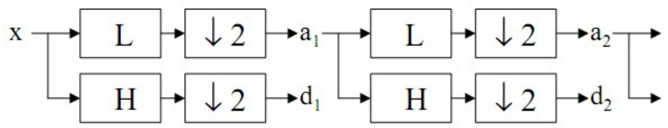

Figure 2.1: Wavelet Decomposition for One-Dimensional Signal

- 2 ↓ denote sub-simpling
- a_j and d_j are called *wavelet coefficients*, determine out put of transform given by the following equations:-

$$a_{j+1}(k) = \sum \mathrm{L}(n-2k)a_j(n)$$

$$d_{j+1}(k) = \sum \mathrm{H}(n-2k)d_j(n)$$

2.4.2 Two Dimensional DWT

One dimensional DWT can be easily extended to two dimensions which can be used for two-dimensional pictures.
The DWT is performed firstly for all images rows and then for all columns using high and low pass-filters. This process is also called multi-level decomposition.

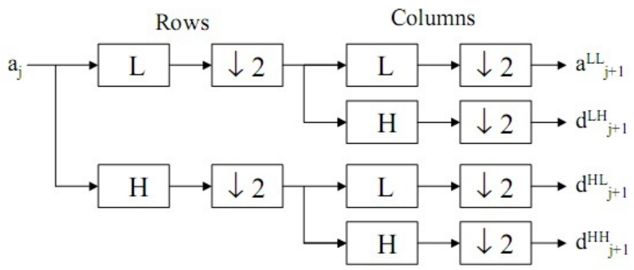

Figure 2.2: Wavelet Decomposition for Tow-Dimensional Signal

1. By using the wavelets, given function can be analysed at various level of resolution.
2. The main feature of DWT is multiscale presentation of functions.
3. The DWT is also invertible and can be orthogonal.

2.5 Références

DAUBECHIES, I. 1992, *Ten lectures on wavelets*, vol. 61, SIAM. 21

JAWERTH, B. et W. SWELDENS. 1994, «An overview of wavelet based multiresolution analyses», *SIAM review*, vol. 36, 3, p. 377–412. 32

KOCIOŁEK, M., A. MATERKA, M. STRZELECKI et P. SZCZYPIŃSKI. 2001, «Discrete wavelet transform-derived features for digital image texture analysis», dans *International Conference on Signals and Electronic Systems, Łódź-Poland*, p. 99–104. 34

Chapter 3

Blind-Source Separation Based on Wavelet Transform and Spearman's Rho

The important thing is not to stop questioning. Curiosity has its own reason for existence. One cannot help but be in awe when he contemplates the mysteries of eternity, of life, of the marvelous structure of reality. It is enough if one tries merely to comprehend a little of this mystery each day.

Albert Einstein

Sommaire

3.1 Introduction

Blind sources separation has been among the essential parts of development in signal processing (see for example CARDOSO [1992]; CARDOSO et LAHELD [1996]; COMON et collab. [1991]; GAETA et collab. [1990]). We assume here the simplest case where N sequences $X_1(t),...,X_N(t)$ are observed, each one is a linear combination of N independent unknown sequences $S_1(t),...,S_N(t)$. Thus we can write $X(t) = MS(t)$ where $X(t)$ and $S(t)$ denote the vectors of components $X_1(t),...,X_N(t)$ and $S_1(t),...,S_N(t)$ respectively, M is a square matrix that is called the mixing matrix.

The problem is to recover the unknown sources $S_1(t),...,S_N(t)$ from the observations, without any priori knowledge on their probabilistic structure. It is only assumed that the sources are mutually independent. The first solution of this problem proposed in HÉRAULT et collab. [1985], was based on cancellation of higher order moments. However, it has been proved COMON et collab. [1991]; FORT [1991], that the algorithm can diverge if the sources have not even probability density function.

Other criteria have been used by several researchers which are based on minimization of cost functions, such as the sum of square forth-order cumulants COMON [1989]; LACOUME et RUIZ [1988], or contrast function CARDOSO [1989]; COMON [1994]. Other authors related this problem of *BSS* to the independent component analysis (*ICA*) which was introduced by Common COMON [1994], and improved by PHAM [1996] .

Given a random vector X with a probability distribution P_x , the *ICA* problem is to find a square transformation matrix B such that the components of transformed vector BX are as independent as possible, if $X = AS$ with S having independent components, then $B = A^{-1}$ (such as A is the mixing matrix), then B is a solution to the *ICA* problem. In this chapter we propose a method of blind source separation based on the discrete wavelet transform, exploiting the fundamental characteristic of this transform which is the preservation of the signal shape in the approximation sub-band of the wavelet domain, and we use the spearman's rho as a measure of dependence between the random variables, so in this case the spearman's rho represents our criterion to minimize using genetic algorithms. Finally, some simulations are executed showing the behavior of this method SOUALHI et collab..

3.2 Spearman's Rho

Spearman's rho represent a measure of dependence between random variables. In our method we use the estimator of multivariate spearman's rho introduced by F. Schmid in SCHMID et SCHMIDT [2007], such as in this chapter authors estimate the spearman's rho trough the copula function, so we try to summarize some essential notions concerning this estimation of spearman's rho. Let $X_1, ..., X_d$ be the set of d random variables with joint distribution function:

$F(x) = P(X_1 \leq x_1, X_2 \leq x_2, ..., X_d \leq x_d)$, where $x = (x_1, x_2, ..., x_d) \in \mathbb{R}^d$ and marginal function $F_i(x) = P(X_i \leq x)$ for $x \in \mathbb{R}^d$ and $i = 1, 2, ..., d$. If not stated otherwise, we will assume that the F_i are continuous functions. Thus, Sklar's theorem states that there exists a unique copula $C : [0,1]^d \to [0,1]$ such that $F(x) = C(F_1(x_1), ..., F_d(x_d))$ for all $x \in \mathbb{R}^d$

The copula C is the joint distribution function of the random variables

$$U_i = F_i(X_i), i = 1, 2, ..., d \text{ where } U_i \sim U[0,1].$$

Moreover:

$$C(u) = F(F_1^{-1}(u_1), F_2^{-1}(u_2), ..., F_d^{-1}(u_d)) \text{ for all } u \in [0,1]^d$$

where F^{-1} represents the generalized inverse of F such as:

$$F^{-1}(u) := inf\{x \in \mathbb{R} \cup \{\infty\} / F(x) \geq u\} \qquad \forall u \in [0,1]$$

and

$$F^{-1}(0) := sup\{x \in \mathbb{R} \cup \{-\infty\} / F(x) = 0\}$$

According to the detailed treatment of copulas, we can state some important results concerning the copulas.

1. Every copula C is bounded in the following sense:

$$W(u) \leq C(u) \leq M(u)$$

such as

$$W(u) := max\{u_1 + u_2 + ... + u_d - (d-1), 0\} .$$

and

$$M(u) := min\{u_1, u_2, ..., u_d\} \qquad \text{for all} \qquad u \in [0,1]^d.$$

Where M and W are called the upper and lower frechet-hoeffding bounds, respectively.

2. An other important copula is the independence copula $\prod(u) = \prod_{i=1}^{d}(u_i), u \in \mathbb{R}^d$ describing the dependence structure of stochastically independent random variables $X_1, X_2, ..., X_d$.

Authors in GAETA et collab. [1990] give the expression of the Spearman's rho in the case of d-dimensional random vector X with copula C by:

$$\begin{aligned}
\rho &= \frac{\int_{[0,1]^d} C(u)du - \int_{[0,1]^d} \prod(u)du}{\int_{[0,1]^d} M(u)du - \int_{[0,1]^d} \prod(u)du} \\
&= \frac{d+1}{2^d-(d+1)}(2^d \int_{[0,1]^d} C(u)du - 1)
\end{aligned}$$

Thus, ρ can be interpreted as the normalized average distance between the copula C and the independent copula $\prod(u)$. In the case of $d = 2$, with a simple calculation we can obtain these results

$$\int_{[0,1]^2} M(u_1, u_2)du_1 du_2 = \frac{1}{3}$$

And

$$\int_{[0,1]^2} \prod(u_1, u_2)du_1 du_2 = \frac{1}{4}$$

Then the formula of ρ can be rewritten as:

$$\rho = 12 \int_0^1 \int_0^1 C(u_1, u_2)du_1 du_2 - 3$$

3.2.1 Non Parametric Estimation

The aim of this estimation is to estimate spearman's rho via the copula. Let $(X_k)_{k=1,n}$ be a random sample from a d-dimensional random vector X with joint distribution function F and copula C which are completely unknown.
The non parametric estimator of the marginal distribution functions is:

$$\hat{F}_{i,n}(x) = \frac{1}{n}\sum_{i=1}^{n} 1_{X_{ik}} \leq x \qquad \forall x \in \mathbb{R}$$

And

$$\hat{U}_{ik,n} := \hat{F}_{i,n}(X_{ik}) \qquad i = 1,\dots,d \quad k = 1,\dots,n$$

Note that

$$\hat{U}_{ik} := \frac{1}{n}(\ Rank\ of\ (X_{ik})\ in\ (X_{i1},\dots,X_{in}))$$

The copula C is estimated by the empirical copula which is defined as:

$$\hat{C}_n(u) = \frac{1}{n}\sum_{k=1}^{n}\prod_{i=1}^{d} 1_{\{\hat{U}_{ik,n}\leq u_i\}} \qquad \forall u = (u_1,\dots,u_d) \in [0,1]^d$$

Finally the estimator of ρ is given by:

$$\hat{\rho} = h(d)(2^d \int_{[0,1]^d} \hat{C}_n(u)du - 1) \tag{3.1}$$

$$= h(d)(\frac{2^d}{n}\sum_{k=1}^{n}\prod_{i=1}^{d}(1-\hat{U}_{ik,n}) - 1) \tag{3.2}$$

with

$$h(d) = \frac{d+1}{2^d - (d+1)}$$

3.3 Proposed Algorithm

In this section, we propose the following algorithm to achieve the fast separation of a several unknown source signals. This algorithm is based on discrete wavelet transform *DWT*. The role of this transform is to estimate the inverse of the mixing matrix from the approximation sub-band. Concerning the criterion to minimize it is the absolute value of the spearman's rho ($|\rho|$), algorithm genetics represent a tool for the minimization of this criterion, so we can divide our algorithm in the following steps:

- Step 1

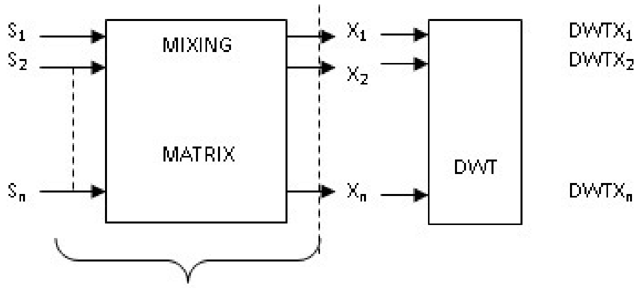

Figure 3.1: Decomposition of Observed Signals

Such as

$$\mathrm{DWTX}_i = [\mathrm{CA}_i^3, \mathrm{CD}_i^3, \mathrm{CD}_i^2, \mathrm{CD}_i^1], \qquad for \quad i = 1, ..., n$$

- CA_i^j : Approximation coefficient at level j.

- CD_i^j : Detail coefficient at level j

In this step we decompose each observed signal by the pyramidal digital wavelet transform, using the bi-orthogonal wavelet Bior(4.4) up to the level 3.

- Step 2

From the previous step we can formulate our objective function with the following way:

Let IM is the inverse mixing matrix such as:

$$\mathrm{IM} = \begin{pmatrix} m_{11} & ... & m_{1n} \\ ... & ... & ... \\ m_{n1} & ... & m_{nn} \end{pmatrix}$$

Where IM is an unknown square matrix and, $\mathrm{CA} = [\mathrm{CA}_i^3, \mathrm{CA}_2^3, ..., \mathrm{CA}_n^3]$ is the vector of the approximation coefficients wavelets decomposition.

The formula of the objective function is calculated by:

$$f(m) = |\mathrm{R}ho(\mathrm{IM.CD})|$$

Where Rho is the spearman's rho,IM.CD is the simple product between the matrix IM and the vector CD and m is a vector of the variables with dimension $n \times n$.

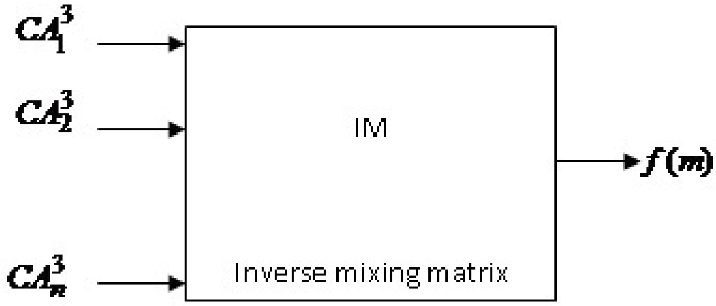

Figure 3.2: Formulate the Objective Function

- Step 3

In this part of the algorithm, we estimate the inverse mixing matrix by the optimum m^* of the objective function which is calculate with genetic algorithms.

- Step 4

In this step we estimate the source signals $\hat{S_1}, \hat{S_2}, ..., \hat{S_n}$ with the simple product between the observed signals $X_1, X_2, ..., X_n$ and the previous estimated mixing matrix $\widehat{\mathrm{IM}}$

3.4 Experimental Results

We present here some experimental examples of signals, we choose the case of two and three source signals, therefore we present some visual results that we obtained with the aim to prove the effectiveness of the proposed method in the recovering of the source signals shape . In our case we obtain the source signals within determinations. Using some treatment techniques after the separation operation we can obtain the source signals almost exactly.

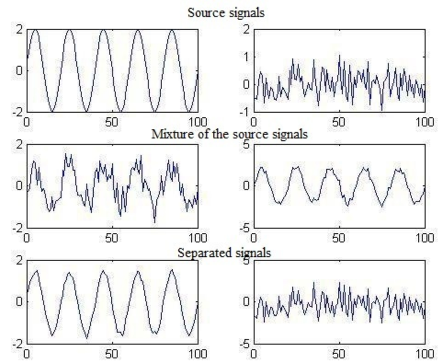

Figure 3.3: A Sinisoidal Signal with the Gaussian Noise

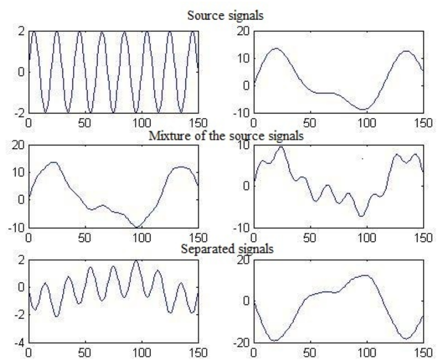

Figure 3.4: Two Sources Signals

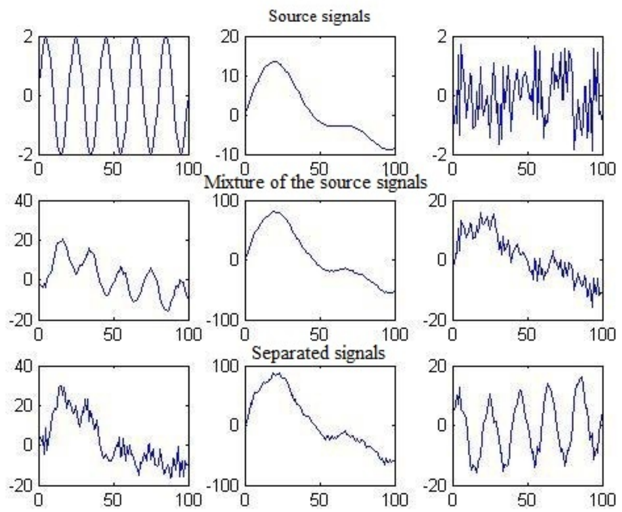

Figure 3.5: Three Sources Signals

3.5 Références

CARDOSO, J.-F. 1989, «Source separation using higher order moments», dans *Acoustics, Speech, and Signal Processing, 1989. ICASSP-89., 1989 International Conference on*, IEEE, p. 2109–2112. 38

CARDOSO, J.-F. 1992, «Iterative techniques for blind source separation using only fourth-order cumulants», dans *Proc. EuSIPCO*, vol. 92, p. 739–742. 38

CARDOSO, J.-F. et B. H. LAHELD. 1996, «Equivariant adaptive source separation», *Signal Processing, IEEE Transactions on*, vol. 44, 12, p. 3017–3030. 38

COMON, P. 1989, «Separation of sources using higher-order cumulants», dans *33rd Annual Techincal Symposium*, International Society for Optics and Photonics, p. 170–183. 38

COMON, P. 1994, «Independent component analysis, a new concept ?», *Signal processing*, vol. 36, 3, p. 287–314. 38

COMON, P., C. JUTTEN et J. HERAULT. 1991, «Blind separation of sources, part ii: Problems statement», *Signal processing*, vol. 24, 1, p. 11–20. 38

FORT, J.-C. 1991, «Stabilité de l'algorithme de séparation de sources de jutten et hérault», *TS. Traitement du signal*, vol. 8, 1, p. 35–42. 38

GAETA, M., J.-L. LACOUME et collab.. 1990, «Source separation without a priori knowledge: the maximum likelihood solution», dans *Proc. EUSIPCO*, vol. 90, Barcelona, Spain, p. 621–624. 38, 40

HÉRAULT, J., C. JUTTEN et B. ANS. 1985, «Détection de grandeurs primitives dans un message composite par une architecture de calcul neuromimétique en apprentissage non supervisé», dans *10° Colloque sur le traitement du signal et des images, FRA, 1985*, GRETSI, Groupe d'Etudes du Traitement du Signal et des Images. 38

LACOUME, J. et P. RUIZ. 1988, «Sources indentification: a solution based on the cumulants», dans *Spectrum Estimation and Modeling, 1988., Fourth Annual ASSP Workshop on*, IEEE, p. 199–203. 38

PHAM, D. T. 1996, «Blind separation of instantaneous mixture of sources via an independent component analysis», *Signal Processing, IEEE Transactions on*, vol. 44, 11, p. 2768–2779. 38

SCHMID, F. et R. SCHMIDT. 2007, «Multivariate extensions of spearman's rho and related statistics», *Statistics & Probability Letters*, vol. 77, 4, p. 407–416. 39

SOUALHI, S., Z. MOKHTARI et A. BOUSSAAD. «Blind source separation based on wavelet and spearman's rho», *Journal of Numerical Mathematics and Stochastics*, vol. 8, 1, p. 1–8. 38

Chapter 4

Crypting Methods Based on Singular Values Decomposition

An expert is a person who has made all the mistakes that can be made in a very narrow field.

Niels Bohr

Sommaire

4.1 Introduction

It is now common to transfer multimedia data via internet with the coming era of electronic commerce (images, messages, Videos ...; etc), but digital images are easy to copy, edit, modify from the internet, television and other medias MOHAMED [2014], MOKHTARI et MELKEMI [2011], Than there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment, so many encryption techniques been proposed in recent yearsALFALOU et collab. [2011].
Since cryptography is the science of securing data which categorized generally into two parts, encoding and decoding LEE et collab. [2014] it coming to solve this problem (to protect information security).
Cryptography is the science of using mathematics to crypting and decrypting; the singular value decomposition SVD is one of the mathematics tools that used (also SVD is very important tools that used in other applications SHIH et collab. [2012], WAZWAZ [2002], YADANI et collab. [2010].
The main problem in this paper HOUAS et collab. [2016] is how to propose new methods of cryptography, in which the level of security is increasing and improving the contrast to achieve the perfect blackness and whiteness of the recovered image NAOR et SHAMIR [1996], RUFAI et collab. [2014]. By using (SVD) two methods of crypting images are proposed such that the second method is the simple modification of the first one and the application of this methods is on rectangular and square PNG's images.
The using of the singular value decomposition in images encryption is come from the fact that the SVD is one of the mathematical tools of matrix reduction.
The SVD procedure is already used for several purposes, we have for examples: Curve fitting, Resolution of the system Ax=B bay the least square, Comparison matrices and Approximation matrices.
Since the matrix analysis is a useful tool in the image processing generally and specially in image compression, this fact give chance to compress and crypt in the same scheme. This work includes cryptography with compression and other uncompressed HOUAS et collab. [2016].

4.2 Singular Value Decomposition (SVD)

This decomposition is used in :

- Theoretical and practical solution of linear system on / unknown.
- Application to geometry problems for computer vision.

Definition 7 *Singular value decomposition (SVD) is a lossy compression technique which achieves compression by using a small rank to approximate the original matrix representing an image.*
Let M be a matrix, $\mathrm{M} \in \mathbb{M}(\mathbb{K}^n \times \mathbb{K}^m)$*),* $\mathbb{K} = \mathbb{R}$ *or* $\mathbb{C}$ *then, there exist a factorization of the form :* $\mathrm{M} = \mathrm{USV}^{\mathrm{T}}$
Where,

- U*: is a* $(n \times n)$ *unitary matrix on* $\mathbb{K}$*, it contains a set of orthonormal basis vectors of* K^{M} *called "output".*
- S*: is a* $(n \times m)$ *matrix in which the diagonal coefficients are real or nulls called "singular values" of the matrix* M *and all the others coefficients are zeros.*
- V^{T}*: is a* $(n \times m)$ *unitary matrix adjoint of*V*, it also contains a set of orthonormal basis vectors of* K^{M} *called input or analysis.*

Definition 8 *a singular value decomposition is a factorization of the matrix* M *into the product three matrices as follow:*

$$\mathrm{M} = \mathrm{USV}^{\mathrm{T}}$$

1. Singular values are the square roots of the eigenvalues of both: $\mathrm{M}^{\mathrm{T}}\mathrm{M}$ and MM^{T}
   - U: is the matrix of eigenvectors of:$\mathrm{M}^{\mathrm{T}}\mathrm{M}$
   - V: is the matrix of eigenvectors of: MM^{T}.
2. the matrix S is uniquely determined from M, but U and V are not.
3. The value of $\mathrm{S}_{i,i}$ are ranked in decreasing order.

4. We denote by S_k the matrix in which we conserve only the k first singular values $\sigma_1, \sigma_2, ..., \sigma_k$.

$$S_k = \begin{pmatrix} \sigma_1 & 0 & 0 & ... & ... & 0 \\ 0 & \sigma_2 & 0 & ... & ... & 0 \\ .. & & & 0 & ... & .. \\ .. & ... & ... & \sigma_k & ... & 0 \\ 0 & & ... & ... & & 0 \\ 0 & & ... & ... & & 0 \\ 0 & & ... & .. & & 0 \end{pmatrix}$$

4.2.1 Existence and Uniqueness of SVD

Any matrix $M \in \mathbb{C}^{(m \times n)}$ own a singular value decomposition (SVD).

The singular values σ_i are determined unique ways.

If M is square and singular values σ_i are distinct, the input and output vectors u_i, v_i are determined uniquely to a complex factor unit.

4.2.2 Characterization of Singular Value Decomposition

(Theorem of Echart-Young) If the matrix $M_k = US_kV^T$, then M_k is the best rank k approximation to M in the sense of $Fubini\ norm$ defined by:

$$\|M\|_F = \sqrt{\sum_{i=1}^{m}\sum_{i=1}^{n} M_{ij}^2} = \sqrt{trace(M^T M)}$$

and we have:

$$\|M - M_k\|_F = \sqrt{\sum_{i=k+1}^{m} \sigma_i^2}$$

So it is only necessary to store the first k columns of U and V in order to present M_k

Lets, $M \in \mathbb{C}^{(n \times n)}$, we have:

$$\sigma_i(M) = \sqrt{M_I(M^T M)} \qquad \forall 1 \leq i \leq n$$

4.3 Proposed Schemes

As it's mentioned previously, cryptography can be categorized into two parts, encoding and decoding. In the encoding step of the scheme the original image is divided into three parts or images U,S and V by SVD mentioned earlier, such as U, S and V are illegible images. After the images are successfully transmitted to the receiver; the secret image can be decoded by transposing V to obtain V^T and multiplying U, S and V^T. To compress images U, S and V before transmission the SVD technique is again used, so after decoding the secret image we obtain compressed image. The bellow results illustrate this scheme in the two cases (with compression and without compression).

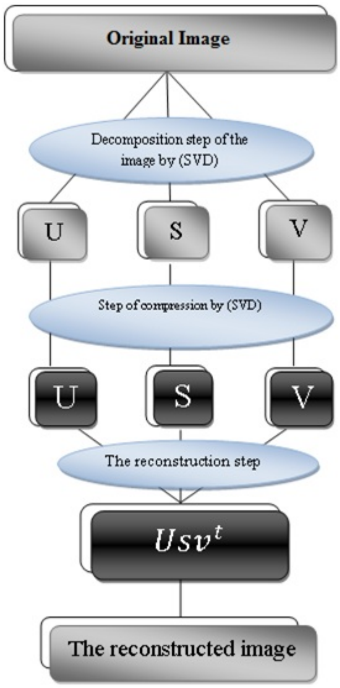

Figure 4.1: A Diagram Showing the First Scheme Proposed

The second method is a result of a small change to the previous scheme, the purpose is to obtaining a more complex and more secure Technique. This modification concerned the original image which is decomposed on two images (image1, image2) and applying the SVD procedure on these two last images. In this case the receiver received six illegible pictures $(U1, S1, V1)$ and $(U2, S2, V2)$. get the secret image the receiver must follow the same steps of the first scheme on each collection also get two images illegible, and by summing this two he obtain the result.

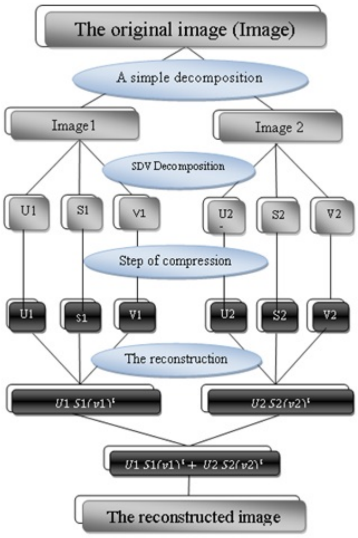

Figure 4.2: A Diagram Showing the Second Scheme Proposed

4.4 Numerical Results and Discussion

4.4.1 Discussion of Results without Compression

The results obtained by the two methods (schemes) proposed above will be discussed by calculating PSNR, NNZ and the distortion is very clear visually.

- Joulia is a rectangular image which reconstructed with PSNR = 34.84 by the first method, with PSNR = 28.73 by the second method and with NNZ=216600 by the two methods. Then the results obtained by the first method are better than them of the second method.

Table 4.1: Results of Reconstructed Images without Compression

Images		**Joulia**	**Man**	**Mandrill**	**Boat**
Method N1	PNSR	34.8141	8.8841	27.6011	5.4173
	MSE	21.4621	$8.4.10^4$	112.9725	$1.8.10^4$
	PNZ	216600	262144	57288	50625
Method N 2	PNSR	28.7399	29.3517	27.0861	30.419
	MSE	86.941	75.4935	127.1945	59.0446
	PNZ	216600	262144	57288	50625

- Man (resp: Boat) is square image (512*512) (resp: (225*225)) which reconstructed with PSNR = 8.88 (resp: PSNR = 5,41) by the first method, with PSNR = 29.35 (resp: PSNR = 30.41) by the second method and with the same NNZ=262144 (resp: NNZ=50625) by the two method. Unlike to the rectangular images, in this case, the results obtained by the second method are better, but the difference between them is very prominent because MSE = 8.4075e+003 (resp: MSE=1.8679e+004) in the first method and MSE=75.49 (resp: MSE=59.04) in the second.

- Mandrill a rectangular image with a small dimension constructed by the first method with PSNR= 27.6 and by the second method, with PSNR =27.07, and the same NNZ=57288. So, with this type of image the result is almost the same for both methods. We can conclude:

  1. In this case, generally the results of the first method are the better, but with square images the result reversed.
  2. Rectangular images with small dimension are almost the same behavior of the square images.
  3. The images "Man" and "Boat" reconstructed with the first method are the worst results in this case.

The following examples illustrate the results:

Figure 4.3: Some Examples of Scheme1, (a) and (c) Original Images, (b) and (d) Reconstructed Images

Figure 4.4: Some Examples of Scheme2, (a) and (c) Original Images, (b) and (d) Reconstructed Images

4.4.2 Discussion of Results with Compression

- Joulia's image is reconstructed by the both methods with number of singular values equal to 120 and NNZ=216600. In the first method PNSR=34.29 and PSNR =10.33 in the second one, so in this case and with this image the first method is the best.

- Man's image is reconstructed by the first method with number of singular values equal to 290 and PSNR =37.53, by the second method with number of singular values equal to 230 and PSNR =5.85, and by the both methods with NNZ=262144, also here the first method is the best.

- Boat's image is reconstructed by the first method with number of singular values equal to 150, NNZ=50625, PSNR =15.34, and by the second method with the number of singular values equal to 112 and the same NNZ but with PSNR= 16.36. The image reconstructed is not clear, than the result is not accepted.

Table 4.2: Results of Julia's Images with Compression

Number of Singular Values		**200**	**230**	**260**	**290**
Method N1	PNSR	35.3658	36.4287	37.1810	37.5306
	MSE	18.9016	14.7983	12.4445	11.4822
	PNZ	262141	262141	262141	262141
Method N 2	PNSR	10.3414	10.3374	10.3374	10.3374
	MSE	$6.01.10^3$	$6.0165.10^3$	$6.0165.10^3$	$6.0165.10^3$
	PNZ	216600	216600	216600	216600

Table 4.3: Results of Man's Image Reconstructed with Compression

Number of Singular Values		**90**	**120**	**180**	**210**
Method N1	PNSR	34.7963	34.8141	34.8141	34.8141
	MSE	21.5502	21.4621	21.4621	21.4621
	PNZ	216600	216600	216600	216600
Method N 2	PNSR	28.7399	27.0861	27.0861	30.419
	MSE	$1.68.10^4$	$1.68.10^4$	$1.69.10^4$	$1.69.10^4$
	PNZ	262141	262141	262141	262141

Table 4.4: Results of Boat's Image Reconstructed with Compression

Number of Singular Values		**90**	**112**	**150**	**185**
Method N1	PNSR	33.9261	35.4824	36.2717	36.2717
	MSE	26.3314	18.4009	15.343	15.343
	PNZ	50625	50625	50625	50625
Method N 2	PNSR	16.3566	16.361	16.361	16.361
	MSE	$1.504.10^3$	$1.504.10^3$	$1.504.10^3$	$1.504.10^3$
	PNZ	262141	262141	262141	262141

We can say in the case of compression:

1. The results of the first method are the best.

2. The worst results obtained by applying the second method to square imge (boat).

The figures bellow illustrate this results:

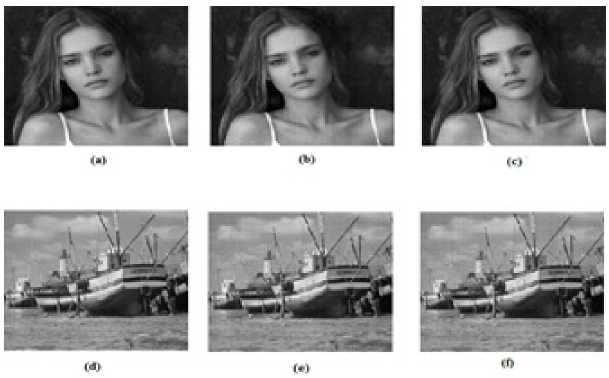

Figure 4.5: Some Examples of Scheme1, (a) and (d) Original Images, (b) Reconstructed Image with 70 SV, (c) Reconstructed Image with 110 SV, (e) Reconstructed Image with 112 SV, (f) Reconstructed Image with 150 SV.

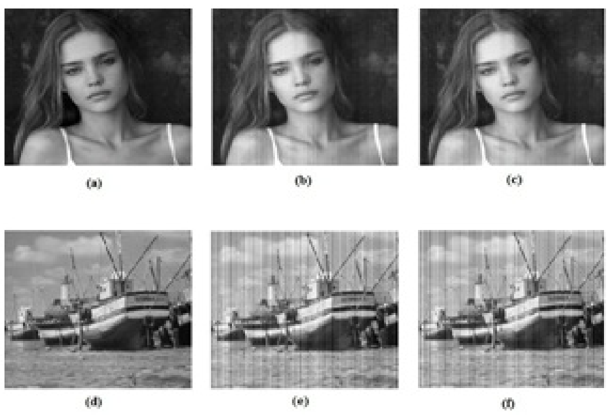

Figure 4.6: Some Examples of Scheme2, (a) and (d) Original Images, (b) Reconstructed Image with 70 SV, (c) Reconstructed Image with 110 SV, (e) Reconstructed Image with 112 SV, (f) Reconstructed Image with 150 SV.

4.5 Références

ALFALOU, A., C. BROSSEAU, N. ABDALLAH et M. JRIDI. 2011, «Simultaneous fusion, compression, and encryption of multiple images», *Optics express*, vol. 19, 24, p. 24 023–24 029. 48

HOUAS, A., S. SOUALHI et Z. MOKHTARI. 2016, «Novel crypting methods based on singular values decomposition.», *Journal of Applied Computer Science & Mathematics*, vol. 10, 22. 48

LEE, C.-C., H.-H. CHEN, H.-T. LIU, G.-W. CHEN et C.-S. TSAI. 2014, «A new visual cryptography with multi-level encoding», *Journal of Visual Languages & Computing*, vol. 25, 3, p. 243–250. 48

MOHAMED, F. K. 2014, «A parallel block-based encryption schema for digital images using reversible cellular automata», *Engineering Science and Technology, an International Journal*, vol. 17, 2, p. 85–94. 48

MOKHTARI, Z. et K. MELKEMI. 2011, «A new watermarking algorithm based on entropy concept», *Acta applicandae mathematicae*, vol. 116, 1, p. 65–69. 48

NAOR, M. et A. SHAMIR. 1996, «Visual cryptography ii: Improving the contrast via the cover base», dans *International Workshop on Security Protocols*, Springer, p. 197–202. 48

RUFAI, A. M., G. ANBARJAFARI et H. DEMIREL. 2014, «Lossy image compression using singular value decomposition and wavelet difference reduction», *Digital Signal Processing*, vol. 24, p. 117–123. 48

SHIH, Y.-T., C.-S. CHIEN et C.-Y. CHUANG. 2012, «An adaptive parameterized block-based singular value decomposition for image de-noising and compression», *Applied Mathematics and Computation*, vol. 218, 21, p. 10 370–10 385. 48

WAZWAZ, A.-M. 2002, «A new method for solving singular initial value problems in the second-order ordinary differential equations», *Applied Mathematics and computation*, vol. 128, 1, p. 45–57. 48

YADANI, K., K. KONDO et M. IWASAKI. 2010, «A singular value decomposition algorithm based on solving hyperplane constrained nonlinear systems», *Applied Mathematics and Computation*, vol. 216, 3, p. 779–790. 48

Conclusion

In the aim of improving the performance of security of : transmission, storage,compression of the signal (information); the research work presented in this thesis consists to study in detail the steps of techniques proposed in tow papers

- Blind-Source Separation Based on Wavelet Transform and Spearman's Rho.
- Novel Crypting Methods Based on Singular Values Decomposition.

As well as the package used to achieve it.

that's why;We have chosen to present this work in two parts:

The first one concern signal processing domain,especially, source separation in which the problem of blind source separation is treated (solved) in the simplest case, where N sequences $X_1(t), ..., X_N(t)$ were observed (each one was a linear combination of N independent unknown sequences $S_1(t), ..., S_N(t)$ using discrete wavelet transform and genetic algorithm where we estimate the mixing matrix through the sub-band approximation . The proof of robustness of this method was done in the form of visual results that obtained by choosing the case of tow and three sources signals.

The second method has relation with the world of secrets ; so it was a new encryption technique ; The tool that we based on to develop this method was the singular values decomposition, with which we benefit the compression of informations (signal) at the time of encyption.

The efficiency of this technique was illustrate by numerical results given by calculation of MSE and PNSR in form of tables and also some visual result as a consequence of application of this method on png square and rectangular images.