COMPRESSION AND SECURITY OF ANALOG SIGNAL INFORMATION USING COMPRESSIVE SENSING AND HYBRID CRYPTOGRAPHY

RANDRIANANDRASANA Marie Emile

Dept. of Telecommunication, Antsirabe Vankinankaratra High Education Institute,
University of Antananarivo, Madagascar,

ABSTRACT

For many reasons, CS or compressive sensing can also be used in signal processing. For example, one of the many reasons is its ability to compress a signal. It uses many mathematical theories; each one has a role to play. In general, they are used to detect the sparse representation of a signal during a phase called the signal reconstruction phase. To protect the useful information of an analog signal, cryptography was used and CS was exploited. Indeed, we were able to model a securing technique and a visualization technique of this useful information.

Keywords: *Signal processing, compressive sensing, CS, sparse representation, cryptography.*

1. INTRODUCTION

Nowadays, the power of processors increases faster than storage capacities. There is therefore an imbalance between the volume of data that can be processed and stored. Consequently, it is therefore necessary to reduce the size of the data to compensate for the inadequacies of the storage memory capacities. Reducing data size can also save power, transmission medium bandwidth, and storage memory capacity. As information nowadays can be extremely valuable and have enormous economic value, its storage and transmission through channels sometimes requires a guarantee of security. [1] [2] [3] [4]

2. PARSIMONY

A discrete signal $x \in \mathbb{R}^{N\times 1}$ is said to be sparse if its norm l_0 is equal to a natural number $K(K << N)$. Mathematically, this norm is defined by the following relation:

$$\|x\|_0 = \#\{i: x_i \neq 0\} = K \quad (1)$$

where the symbol # and x_i respectively represent the cardinal of any set and the nonzero element of the signal x.
In the case where the signal x is not sparse in the time domain, it can have a sparse representation $\alpha \in \mathbb{R}^{N\times 1}$ with respect to another domain $\Psi \in \mathbb{R}^{N\times N}$. This sparse representation α is defined as follows:

$$x = \Psi\alpha \; with \; \|\alpha\|_0 = K \quad (2)$$

The degree of parsimony ρ of a signal x is defined by the following relation:

$$\rho = \frac{K}{N} \quad (3)$$

where K and N represent respectively the non-zero number and the dimension of x. It measures the degree of compressibility because the lower ρ, the more compressible the signal. . [5] [6]

3. DOMAIN OF PARSIMONY

3.1 Discrete Fourier transform

For a discrete signal x with N elements, its discrete Fourier transform $X(f)$ is defined as follows

$$X(f) = \sum_{n=0}^{N-1} x(n)e^{-2i\pi f\frac{n}{N}} \; with \; f = 0, 1, \dots, N-1 \quad (4)$$

The inverse discrete Fourier transform $x(n)$ is defined by the following relation:

$$x(n) = \frac{1}{N}\sum_{f=0}^{N-1} X(f)e^{2i\pi f\frac{n}{N}} \; with \; n = 0, 1, \dots, N-1 \tag{5}$$

3.2 Discrete cosine transform

For a discrete signal x with N elements, its discrete cosine transform $X(f)$ is defined as follows:

$$X(f) = \sqrt{\frac{2}{N}}C(f)\sum_{n=0}^{N-1} x(n)cos\left[\frac{\pi(2n+1)f}{2N}\right] \; with \; f = 0, 1, \dots, N-1 \tag{6}$$

where $C(f) = \frac{1}{\sqrt{2}}$ for $f = 0$ and $C(f) = 1$ for $f \neq 0$.

The inverse discrete cosine transform $x(n)$ is defined by the following relation:

$$x(n) = \sqrt{\frac{2}{N}}\sum_{f=0}^{N-1} C(f)X(f)cos\left[\frac{\pi(2n+1)f}{2N}\right] \; with \; n = 0, 1, \dots, N-1 \tag{7}$$

3.3 Wavelet transform

The continuous wavelet transform consists in creating, from a parent function $\varphi(the\ wavelet)$, a family of wavelets $\varphi(\alpha x + \beta)$ where α and β are real numbers. α is used to expand the function φ and β is used to translate it. The continuous wavelet transform $C(\alpha, \beta)$ of a signal $x(t)$ is expressed as follows:

$$C(\alpha, \beta) = \int_{-\infty}^{+\infty} x(t)\,\varphi(\alpha x + \beta)dt \tag{8}$$

The discrete version of this transformation only considers discrete expansions and translations of the wavelet. . [7]

4. PRINCIPLE OF COMPRESSIVE SENSING

4.1 Acquisition phase or measurement phase

During this acquisition phase or measurement phase, the signal x is directly captured in a compressed format in a vector $y \in \mathbb{R}^{M\times 1}$ by multiplying it by a rectangular matrix $\Phi \in \mathbb{R}^{M\times N}$ $(M < N)$:

$$y = \Phi x \tag{9}$$

where the vector y and the matrix Φ represent respectively the measurement vector and the measurement matrix.

4.2 Reconstruction phase

Since the signal x has a sparse representation with respect to a domain or a basis Ψ, equation (9) becomes:

$$y = A\alpha \; with \; A = \Phi\Psi \in \mathbb{R}^{M\times N} \tag{10}$$

Taking into account the presence of additive noise during the acquisition phase or the measurement phase, equation (10) becomes:

$$y = A\alpha + \mathcal{E} \tag{11}$$

where $\mathcal{E} \in \mathbb{R}^{M\times 1}$ is a vector representing the noise.

During this reconstruction phase, the original signal is reconstructed from the measurement vector y, the measurement matrix Φ and that of the domain Ψ. It is done in two steps: the first step consists in finding the vector$\hat{\alpha}$ corresponding to the solution of the equation (10) or (11). Once $\hat{\alpha}$ is obtained, the second step consists in the reconstruction of the signal $\hat{x} = \Psi\hat{\alpha}$.

Since the matrix $A \in \mathbb{R}^{M\times N}$ is rectangular $(M < N)$, there are infinitely many vectors α satisfying equation (10) and (11). But taking into account the assumption that α is sparse in the domain Ψ, the problem consists in solving the following minimization:

$$\min_{\hat{\alpha}} \|\hat{\alpha}\|_0 \; such \; as \; y = A\alpha \tag{12}$$

Taking additive noise into account, equation (11) becomes:

$$\min_{\hat{\alpha}} \|\hat{\alpha}\|_0 \; such \; as \; \|y - A\hat{\alpha}\|_2 \leq b \tag{13}$$

where $b = \|\mathcal{E}\|_2$ is the noise amplitude. The norm l_2 of the vector $\mathcal{E}$ is defined as follows:

$$\|\mathcal{E}\|_2 = \sqrt{\sum_{i=1}^{M} \mathcal{E}_i^2} \tag{14}$$

5. PROPERTIES OF THE MEASUAREMENT MATRIX

5.1 Uniqueness

To guarantee that two distinct signals α_1 and $\alpha_2 (\alpha_1 \neq \alpha_2)$ generate two vectors of different measurement $y_1 = A\alpha_1$ and$y_2 = A\alpha_2$ $(y_1 \neq y_2)$, Donoho and al. [1] established the following theorem:

$$K < \frac{1}{2}\text{spark}(A) \tag{15}$$

Then for each measure vector y, there is at most one sparse signal α with $\|\alpha\|_0 = K$, such that $y = A\alpha$.
By definition, the spark(A) of a matrix A is equal to the least number of columns of A which are linearly dependent. Since the value of spark(A) varies between 2 and$(M + 1)$, then $M > 2K$. Although this theorem is important since it guarantees the uniqueness of the representation of a sparse vector, it is difficult to evaluate for a matrix A given. . [8]

5.2 Restricted Isometry Proprety (RIP)

A matrix A satisfies the restricted isometry property of order K if the most small constant $\delta_K (0 < \delta_K < 1)$ called restricted isometry constant or RIC verifying the following condition exists [2]:

$$(1 - \delta_K)\|\alpha\|_2^2 \leq \|A\alpha\|_2^2 \leq (1 + \delta_K)\|\alpha\|_2^2 \tag{16}$$

For any sparse vector α, such that $\|\alpha\|_0 = K$. The RIP checks whether the measure matrix A is close to an isometry, i.e. if it preserves the distance between two measurement vectors. That is, if the measurement matrix satisfies the RIP, then the distance between two measurement vectors $y_1 = A\alpha_1$ and $y_2 = A\alpha_2$ is proportional to the distance between α_1 and α_2. The RIP is an important property that ensures signal reconstruction. However, it is difficult to check whether a matrix satisfies or not the RIP [3].

5.3 Coherence

It is easier to evaluate compared to the two properties presented previously. This is the major advantage of coherence. The coherence μ(A) of a matrix A is equal to the greatest absolute value of the scalar product between two distinct column vectors of A [4]:

$$\mu(A) = \max_{i \neq j} \frac{\left|\langle a_i , a_j \rangle\right|}{\|a_i\|_2 \left\|a_j\right\|_2} \tag{17}$$

Where a_i and a_j are the columns of the matrix A. Coherence measures the correlation maximum between the different column vectors of a matrix. Welch demonstrated that for a given matrix A [5][6]:

$$\sqrt{\frac{N - M}{M(N - 1)}} \leq \mu(A) \leq 1 \tag{18}$$

The lower bound of μ is called the Welch limit. When $M \ll N$, this bound lower tends towards$\frac{1}{\sqrt{M}}$. A matrix A is said to be incoherent when the value of μ(A) tends towards this Welch limit.
The lower bound of the spark(A) of a matrix A can be expressed as a function of μ(A) [9]:

$$\text{spark}(A) \geq 1 + \frac{1}{\mu(A)} \tag{19}$$

The uniqueness condition can be expressed in terms of coherence. By combining equations (15) and (19), when the following relation is satisfied:

$$K < \frac{1}{2}\left(1 + \frac{1}{\mu(A)}\right) \tag{20}$$

Then for a measure vector $y \in \mathbb{R}^{M \times 1}$, there exists at most one signal α such that $y = A\alpha$. These equations show that the measurement matrix A must have low coherence. Indeed, a low value of the coherence μ increases the upper bound of K. For minimize the value of μ, the column vectors of A must be the most orthogonal possible [9].
Caï and al. [9] demonstrated that the upper bound of the RIP can be expressed as consistency function. If a matrix A has a coherence μ(A) then it satisfies the RIP with a constantδ_K such that:

$$\delta_K \leq (K - 1)\mu(A) \tag{21}$$

This equation shows that when a matrix has low coherence, it implies that it satisfies the RIP [10]. Since the RIP is difficult to assess, in practice it is replaced by coherence [11].
The notion of coherence can be extended for a base pair. Mutual coherence between Φ and Ψ is defined as follows [12]:

$$\mu(\Phi, \Psi) = \sqrt{N} \max_{i,j} \frac{\left|\langle \Phi_i , \Psi_j \rangle\right|}{\|\Phi_i\|_2 \left\|\Psi_j\right\|_2} \tag{22}$$

where Φ_i and $\Psi_j$represent respectively the row vectors of Φ and the column vectors of Ψ. It measures the maximum correlation between the row vectors of Φ and the vectors columns of Ψ. The range of mutual coherence values is:

$$1 \leq \mu(\Phi, \Psi) \leq \sqrt{N} \tag{23}$$

6. EXAMPLES OF MEASUREMENT MATRIX

6.1 Random

The elements of the matrix are generated from a random process.

6.2 Determistic.

The elements of the matrix are generated from a deterministic process.

6.3 Ternary

The elements of the matrix take only three possible values.

6.4 Binary

The elements of the matrix take only two possible values,

6.5 Toeplitz

The elements of the matrix on a diagonal descending from left to right are the same.

6.6 Diagonal block

A matrix having blocks on the main diagonal, such that the off-diagonal blocks are zero matrices.

7. RECONSTRUCTION ALGORITHM

7.1 Convex relaxation

To circumvent the complexity linked to the l_0 norm, methods based on convex relaxation, such as BP, relax the problem by replacing the l_0 norm with an l_1 norm and use convex solvers to solve it [13]:

$$\min_{\hat{\alpha}} \|\hat{\alpha}\|_1 \text{ such as } y = A\hat{\alpha} \tag{24}$$

The l_1 norm of a vector $\boldsymbol{x} \in \mathbb{R}^{N\times 1}$ is defined by the following relation:

$$\|\boldsymbol{x}\|_1 = \sum_{i=1}^{N} |\boldsymbol{x}_i| \tag{25}$$

When the matrix A satisfies certain criteria, BP can find the unique most sparse solution $\hat{\alpha}$ with a high probability. Taking additive noise into account, the problem formulated by equation (24) becomes [14]:

$$\min_{\hat{\alpha}} \|\hat{\alpha}\|_1 \; such\; as \; \|y - A\hat{\alpha}\|_2 \leq b \tag{26}$$

In the literature, this method is called basis pursuit with inequality constraints or BPIC. Another variant of this method, called basis pursuit denoising or BPDN, consists in reformulating the problem as follows:

$$\min_{\hat{\alpha}} \frac{1}{2} \|y - A\hat{\alpha}\|_2^2 + \lambda \|\hat{\alpha}\|_1 \tag{27}$$

7.2 Greedy Pursuit

These are iterative methods and generally easy to implement. At each iteration, they select one or more columns of the matrix **A** according to its correlation with the measurement vector y. Then, they calculate an approximation of the signal and update the residual which will be used in the next iteration. The greedy algorithms are distinguished in particular by the method of selecting the columns of the matrix **A** and on the way in which the residual is updated. When the measurement matrix **A** is an orthogonal basis, it is possible to reconstruct an approximation of the signal by selecting one by one the columns of **A** having a maximum correlation with the residual. Adaptive pursuit (AP) is the simplest version of greedy algorithms.

8. XOR CRYPTOGRAPHY

The XOR is a logical operator which corresponds to an exclusive OR: it is the (A OR B) that is used in logic but which excludes the case where A and B are simultaneously true. Here is its truth table:

Table 1 : XOR truth table

A	B	A XOR B
FALSE	FALSE	FALSE

FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	FALSE

9. RSA CRYPTOGRAPHY

An RSA key $k = (k^{pub}, k^{priv})$ is defined from the following parameters:

- p and q are two (large) distinct prime numbers of the same binary size;
- e and d are integers such that $ed = 1\ mod\ (p-1)(q-1)$
- $N = pq$

Then $k^{pub} = (N, e)$ and $k^{priv} = (N, d)$.

Clear and encrypted messages are identified with elements of $\mathbb{Z}/N\mathbb{Z}$. The encryption and decryption functions are defined by:

$$E_{k^{pub}}: \begin{matrix} \mathbb{Z}/N\mathbb{Z} \to & \mathbb{Z}/N\mathbb{Z} \\ m \to & m^e\ mod\ N \end{matrix} \quad (28)$$

$$E_{k^{pub}}: \begin{matrix} \mathbb{Z}/N\mathbb{Z} \to & \mathbb{Z}/N\mathbb{Z} \\ m \to & m^e\ mod\ N \end{matrix} \quad (29)$$

Suppose now that Bob wants to transmit a message m to Alice, guaranteeing Alice that he is the author of this message. This is a problem, authentication, totally different from that of confidentiality Indeed, this time, Bob does not wish to prevent the opponent Oscar from learning about m. He wishes to prevent Oscar from being able to impersonate him, for example by communicating with Alice by pretending to be Bob.

Here is how it can proceed: it calculates $s = D_{k_B^{priv}}(m)$ and transmits the pair (m, s) to Alice. Alice, to convince herself that the couple (m, s) does indeed come from Bob, checks that:

$$E_{k_B^{pub}}(s) = m \quad (30)$$

10. COMPRESSION AND SECURING OF ANALOG SIGNAL INFORMATION

The steps to follow are as follows:

- Conversion of the analog signal $x(t)$ into a sampled signal $x \in \mathbb{R}^{N\times 1}$
- Application of the acquisition phase or the measurement phase of compressive sensing
- Digitization of the measure vector $y \in \mathbb{R}^{M\times 1}$
- XOR encryption of the measurement vector
- RSA encryption of measurement vector encryption keys
- Application of RSA authentication (associated with the measurement vector)
- Digitization of the measurement matrix Φ
- XOR encryption of the measurement matrix
- RSA encryption of measurement matrix encryption keys
- Application of RSA authentication (associated with the measurement matrix)

11. VISUALIZATION OF THIS COMPRESSED AND SECURED INFORMATION

The steps to follow are as follows:

- Verification of RSA authentication (associated with the measurement matrix)
- RSA decryption of measurement matrix decryption keys
- XOR decryption of the measurement matrix
- Conversion of the digitized measurement matrix to the initial measurement matrix
- Verification of RSA authentication (associated with the measurement vector)
- RSA decryption of measurement vector decryption keys
- XOR decryption of the measurement vector
- Conversion of the digitized measure vector to the original measure vector
- Application of the reconstruction phase of compressive sensing

12. EXAMPLE

Take the case of an analog signal $x(t) = \sin(2000\pi t) + \sin(4000\pi t) + \sin(8000\pi t)$. Its representative curve in the closed time interval $[0\,;0{,}1]$ is shown as follows:

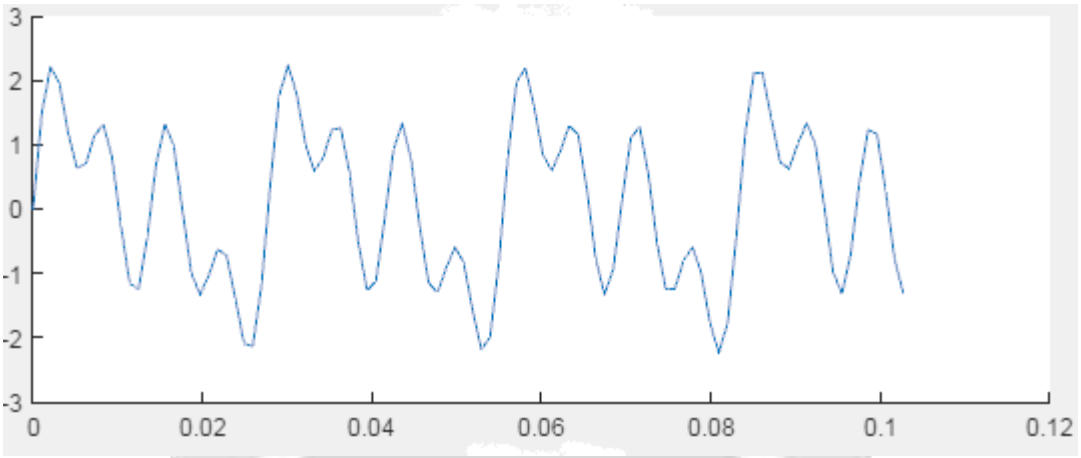


Fig-1 : Representative curve

To acquire the information of this analog signal $x(t)$, we will sample it with a sampling frequency $f_e = 10000Hz$. In this case, the sampled signal is represented as follows:

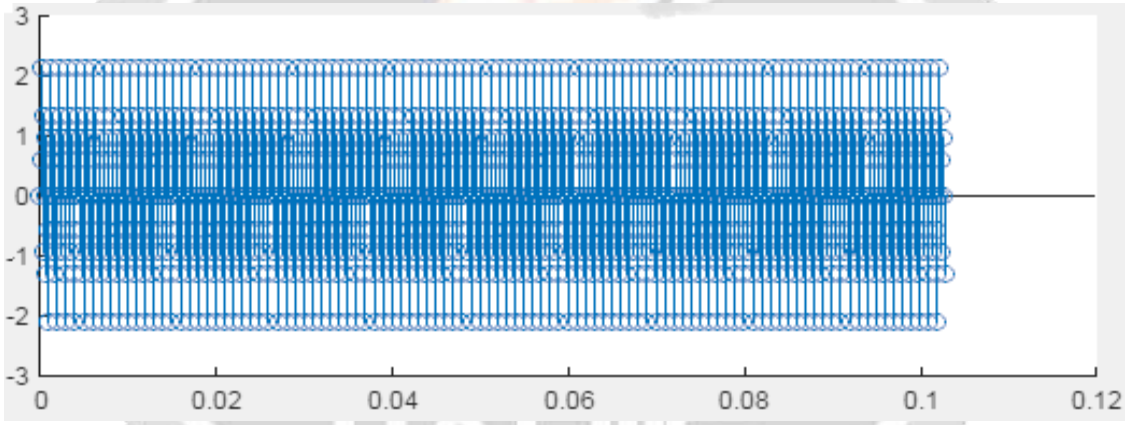


Fig-2 : Sampled signal

From Figure 2, it can be seen that the sampled signal is not sparse in the time domain because almost all of its elements are non-zero. However, it has a sparse representation in another domain which is only the discrete Fourier transform. Its sparse representation is shown as follows:

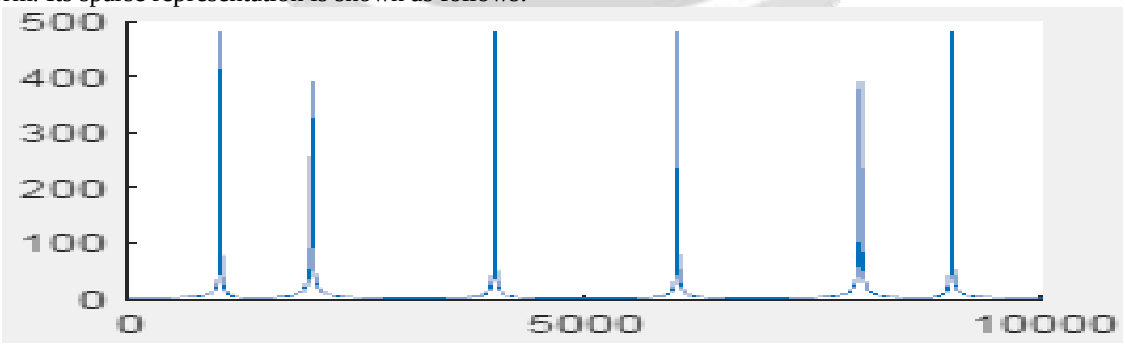


Fig-3 : Sparse representation

From Figure 3, it is clearly seen that the discrete Fourier transform of the sampled signal is sparse because most of its elements are zero.

Let $\boldsymbol{I} \in \mathbb{R}^{N\times N}$ be an identity matrix defined by:

$$\boldsymbol{I} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} \\ \vdots & \vdots & \dots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} \end{bmatrix} \tag{31}$$

During the application of the acquisition phase or the measurement phase of the compressive sensing, we will use a random measurement matrix. This measurement matrix $\boldsymbol{\phi} \in \mathbb{R}^{\boldsymbol{M}\times\boldsymbol{N}}$ is constructed by randomly choosing M from among the N rows of the identity matrix I to randomly take M from among the N samples of the sampled signal.
The measurement vector therefore only contains M samples and the intervals which separate these samples are not uniform. Non-uniform sampling then takes place during this acquisition phase or measurement phase.
Let's take $M = 400$, the measurement vector is represented as follows:

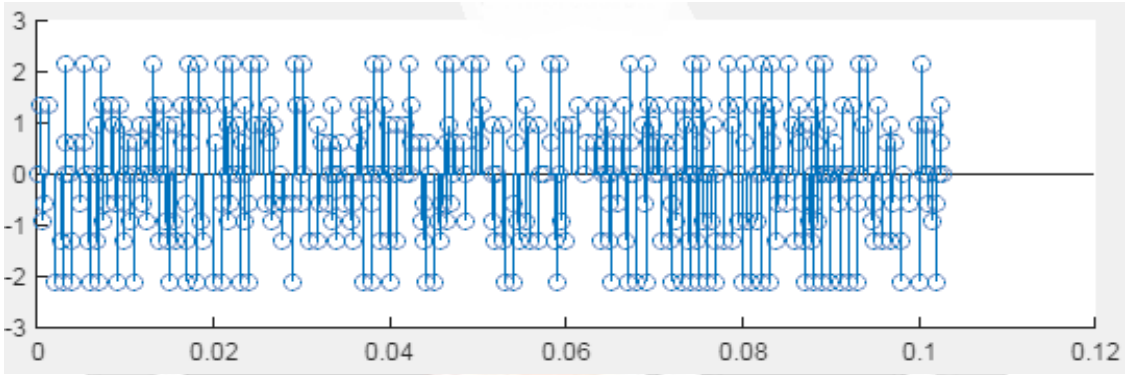


Fig-4 : Measurement vector

To digitize the measurement vector, an algorithm is used that simulates the operating principle of an analog-to-digital converter or ADC. Take for example a 3-bit ADC output with a uniform quantization step $Q = 1$. The operating principle of this ADC can be explained by the following table:

Table 2 **:** Principle of operation of a 3-bit ADC

Sample value	Quantification	Binary value of sample
$[-\mathbf{3,5} \quad - \quad -\mathbf{2,5}[$	7	111
$[-\mathbf{2,5} \quad - \quad -\mathbf{1,5}[$	6	110
$[-\mathbf{1,5} \quad - \quad -\mathbf{0,5}[$	5	101
$[-\mathbf{0,5} \quad - \quad \mathbf{0,5}[$	0	000
$[\mathbf{0,5} \quad - \quad \mathbf{1,5}[$	1	001
$[\mathbf{1,5} \quad - \quad \mathbf{2,5}[$	2	010
$[\mathbf{2,5} \quad - \quad \mathbf{3,5}[$	3	011

For this type of ADC, the digitized measurement vector figure is as follows:

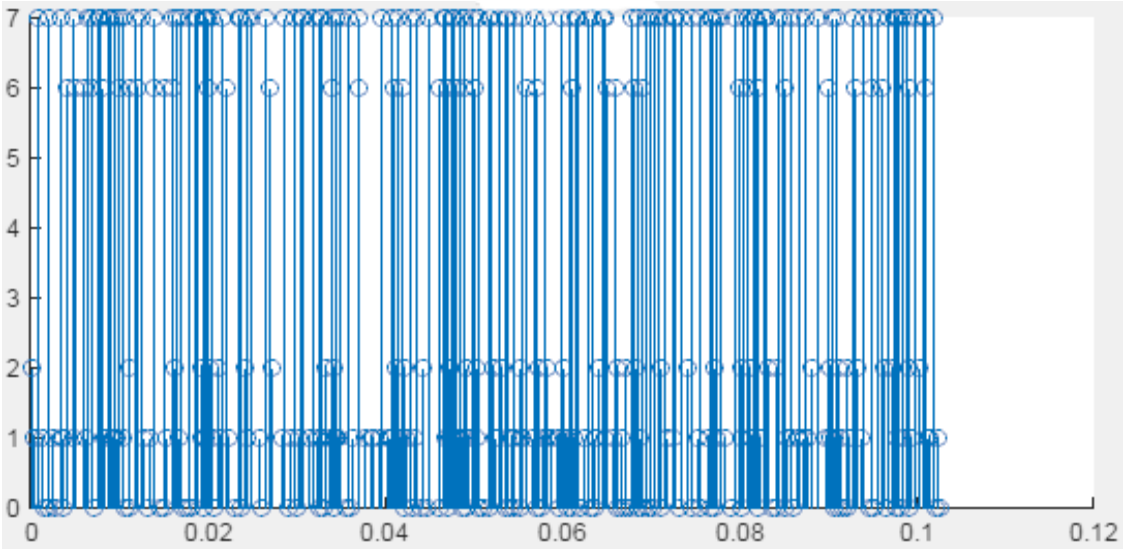


Fig-5 : Digitized measurement vector

Figure 5 shows that the binary value of each sample corresponds to the binary representation of each natural number that associates it in the y-axis.

To encrypt the digitized measurement vector, an XOR encryption algorithm is used. For example, consider the following encryption key values: 2,6,4. The algorithm encrypts each sample of the digitized measurement vector by looping through these 3 encryption key values. For this example, the figure of the encrypted digitized measurement vector is as follows:

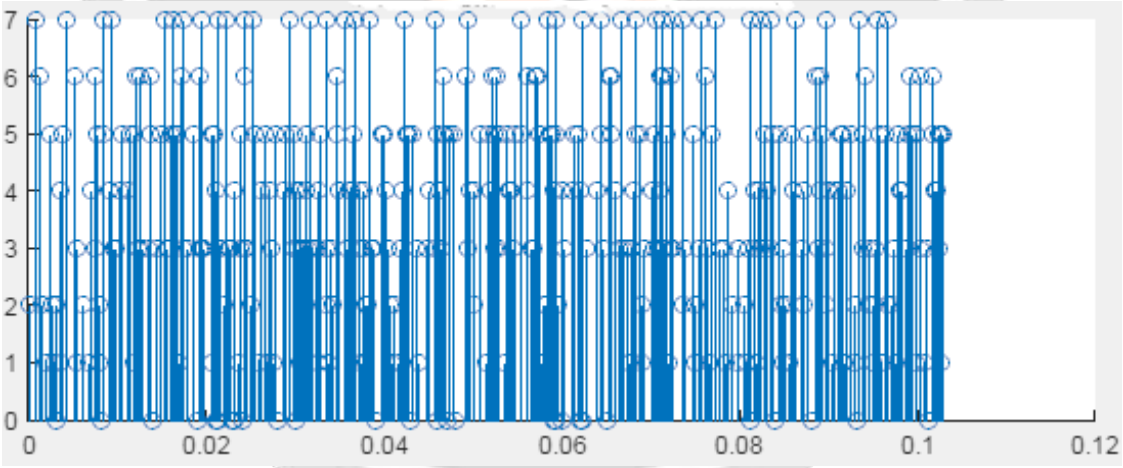


Fig-6 : Encrypted digitized measurement vector

Figure 6 shows that the encrypted value of each sample of the digitized measurement vector corresponds to the binary representation of each natural number that associates it in the y-axis.

To encrypt the measurement vector encryption keys, an RSA encryption algorithm is used. The RSA encryption of these measurement vector encryption keys is shown as follows (receiver's public key: e=3 and n=33):

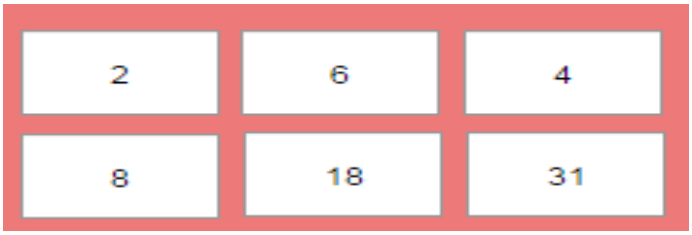


Fig-7 : RSA encryption of these measurement vector encryption keys

To sign the encrypted encryption keys of the measurement vector, an RSA authentication algorithm is used. The following figure illustrates this signature (Sender's private key: d=11 and n=15):

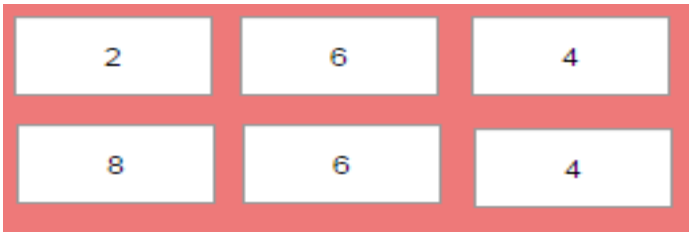


Fig-8 : Signatures of the encryption keys of the measurement vector

To digitize the measurement matrix, a digitization algorithm is used. The following figure illustrates the digitization of the measurement matrix:

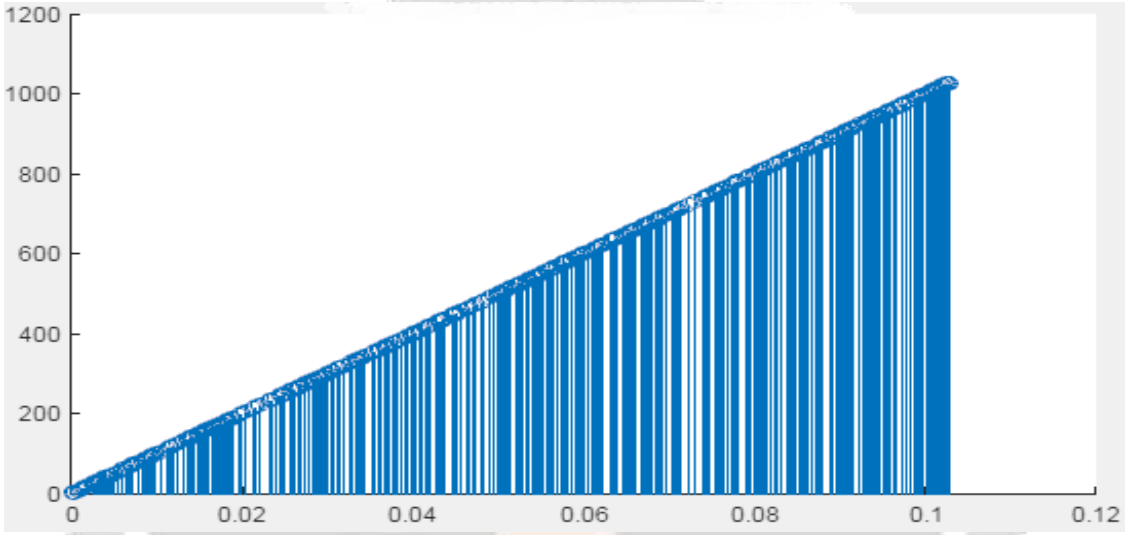


Fig-9 : Digitization of the measurement matrix

Figure 9 shows that the binary value of each element of the measurement matrix corresponds to the binary representation of each natural number that associates it in the y-axis.

To encrypt the measurement matrix, an XOR encryption algorithm is used. The following figure illustrates the XOR encryption of the measurement matrix with encryption keys 7,14,12:

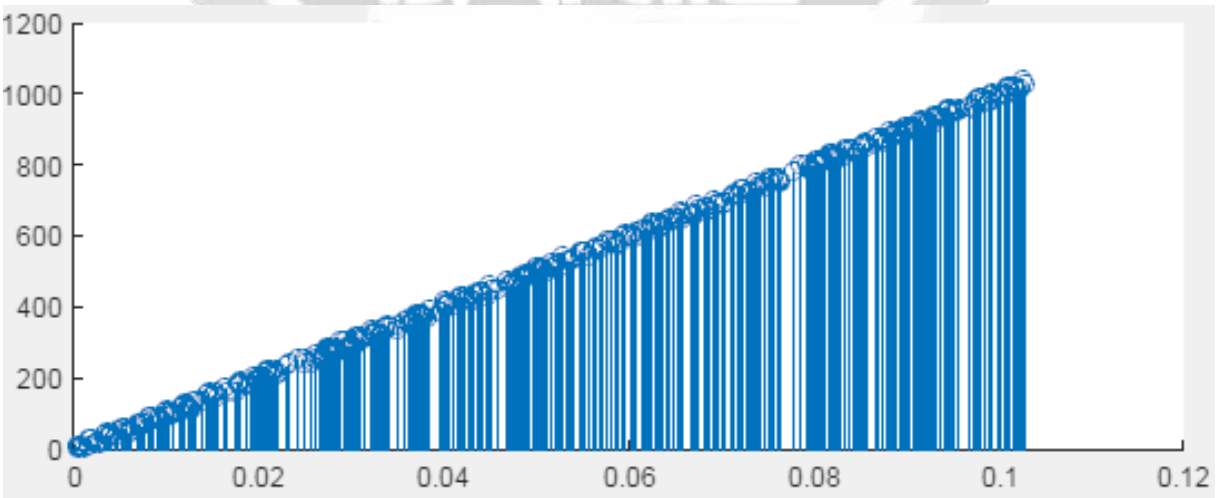


Fig-10 : XOR encryption of the measurement matrix

Figure 10 shows that the value encrypted in XOR of each element of the measurement matrix corresponds to the binary representation of each natural number which associates it in the y-axis.

To encrypt the measurement matrix encryption keys, an RSA encryption algorithm is used. The following figure illustrates the RSA encryption of the measurement matrix encryption keys (receiver's public key: e=3 and n=33):

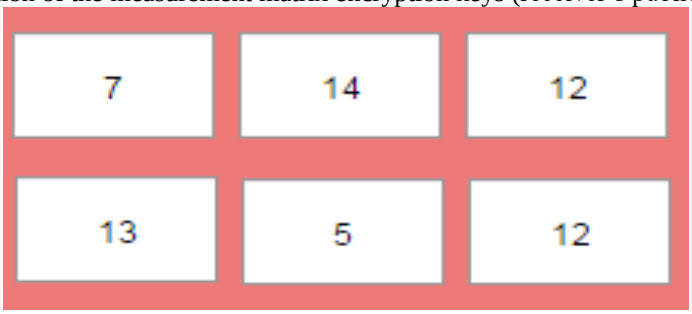


Fig-11 : RSA encryption of the measurement matrix encryption keys

To sign the encryption keys of the measurement matrix, an RSA authentication algorithm is used. The following figure illustrates the signatures of the encryption keys of the measurement matrix (Sender's private key: d=11 and n=15):

:

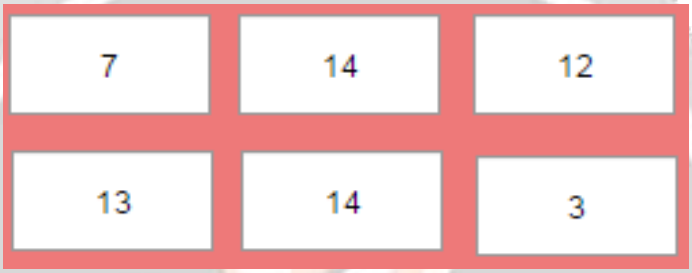
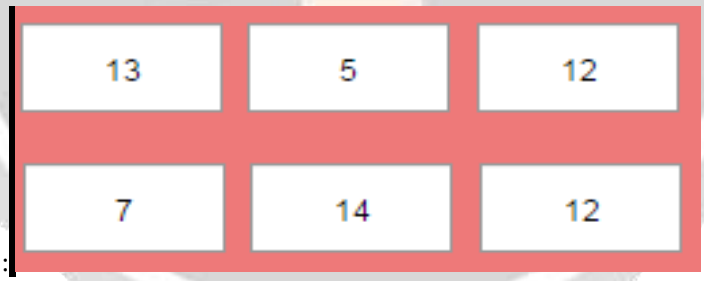


Fig-12 : Signatures of the encryption keys of the measurement matrix

To decrypt the encryption keys of the measurement matrix, an RSA decryption algorithm is used. The following figure illustrates the RSA decryption of the measurement matrix encryption keys (receiver's private key: d=7 and n=33):



:

Fig-13 : RSA decryption of the measurement matrix encryption keys

To verify the signatures of the encrypted encryption keys of the measurement matrix, an algorithm that verifies RSA authentication is used. The following figure illustrates the verification of the signatures of the encrypted encryption keys of the measurement matrix (Sender's public key: e=3 and n=15):

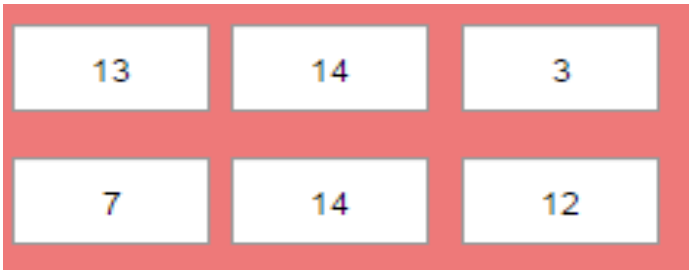


Fig-14 : Verification of the signatures of the encrypted encryption keys of the measurement matrix

To decrypt the measurement matrix, an XOR decryption algorithm is used. The following figure illustrates the XOR decryption of the measurement matrix:

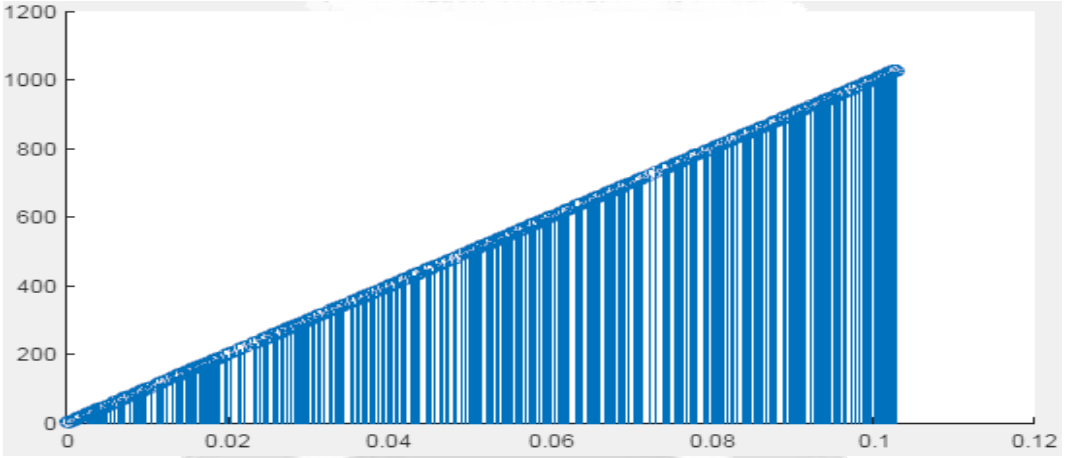


Fig-15 : XOR decryption of the measurement matrix

Figure 15 shows that the deciphered value in XOR of each element of the measurement matrix corresponds to the binary representation of each natural number which associates it in the y-axis.

To decrypt the measurement vector decryption keys, an RSA decryption algorithm is used. The following figure illustrates the decryption of the measurement vector encryption keys (Receiver's private key: d=7 and n=33):

8	18	31
2	6	4

Fig-16 : Decryption of the measurement vector encryption keys

To verify the signatures of the encrypted encryption keys of the measurement vector, an RSA authentication algorithm is used. The following figure illustrates the verification of the signatures of the encrypted encryption keys of the measurement vector (Sender's public key: e=3 and n=15):

8	6	4
2	6	4

:

Fig-17 : Verification of the signatures of the encrypted encryption keys of the measurement vector

To decrypt the measurement vector, an XOR decryption algorithm is used. The following figure illustrates the XOR decryption of the measurement vector:

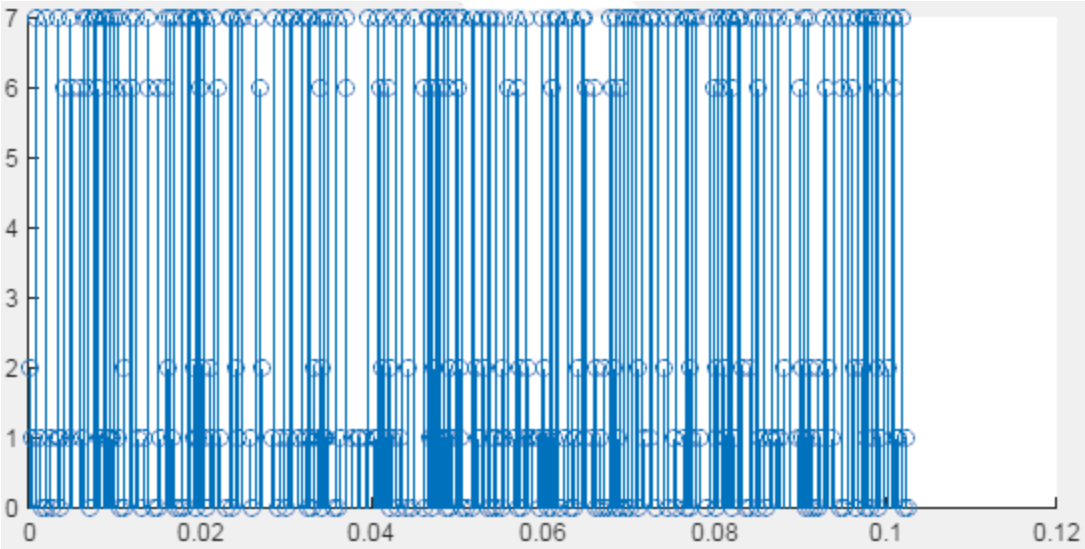


Fig-18 : XOR decryption of the measurement vector

Figure 18 shows that the value deciphered in XOR of each sample of the measurement vector corresponds to the binary representation of each natural number which associates it in the y-axis. To convert all the binary elements of the measurement vector into decimal, an algorithm is used which simulates the operating principle of a digital-analog converter or DAC. Take for example a 3 bit input DAC. The operating principle of this DAC can be explained by the following table:

Table 3 : Principle of operation of a 3-bit DAC

Binary value	Decimal value
000	0
001	1
010	2
011	3
101	-1
110	-2
111	-3

For this type of DAC, the measurement vector in decimal is illustrated by the following figure:

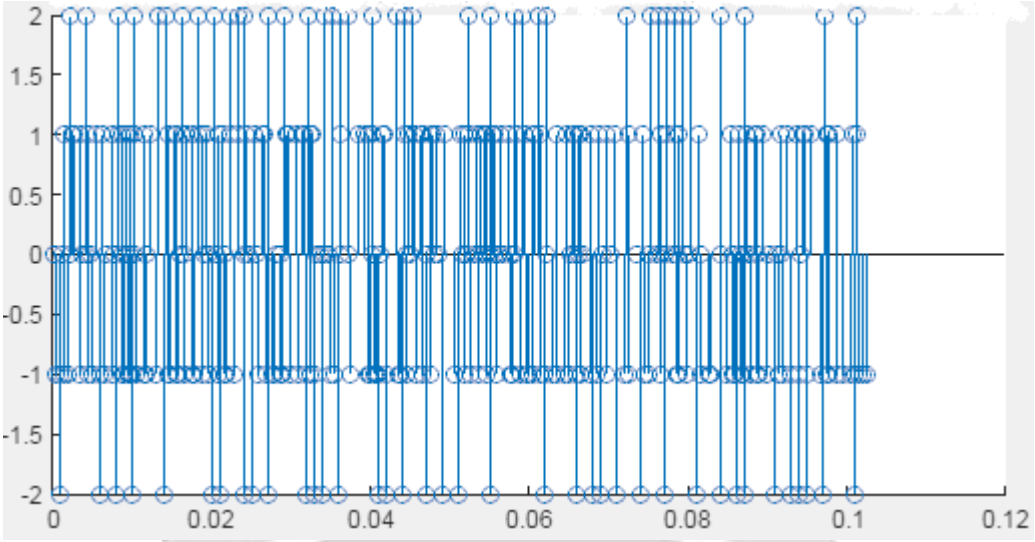


Fig-19 : Measurement vector in decimal

Figure 19 shows that the decimal value of each sample of the measurement vector corresponds to each whole number that associates it in the y-axis.
To reconstruct the initial information, we use:

- The measurement vector $y \in \mathbb{R}^{M \times N}$;
- The measurement matrix $\phi \in \mathbb{R}^{M \times N}$;
- The discrete Fourier transform matrix $\psi \in \mathbb{R}^{N \times N}$;
- The orthogonal matching pursuit (OMP).

First, the OMP visualizes the discrete Fourier transform of the sampled signal x. For our example, the following figure illustrates the Discrete Fourier transform of the sampled signal x visualized by the OMP:

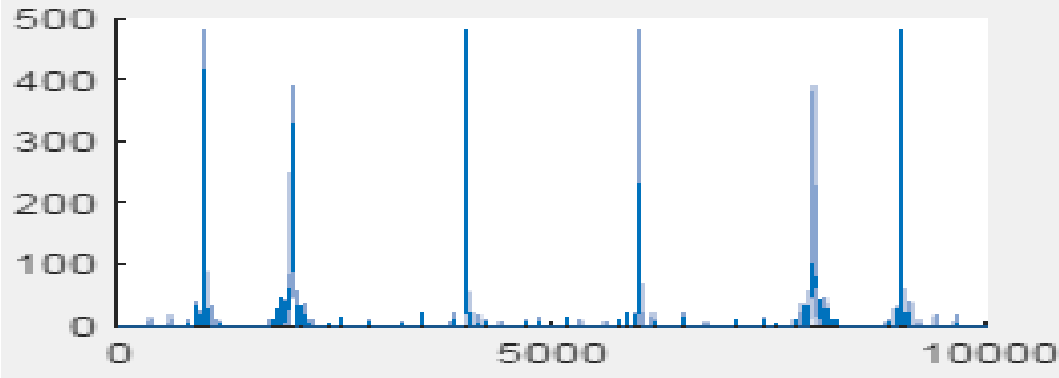


Fig-20 : Discrete Fourier transform of the sampled signal $\boldsymbol{x}$ visualized by the OMP

From Figure 20, it is clearly seen that the signal visualized by the OMP is sparse in the frequency domain because most of its elements are equal to zero.
In the second time, it suffices to visualize the initial sampled signal by calculating it by the following equation:

$$\boldsymbol{x = \psi \alpha} \tag{32}$$

The following figure illustrates the visualization of the information of the sampled signal x:

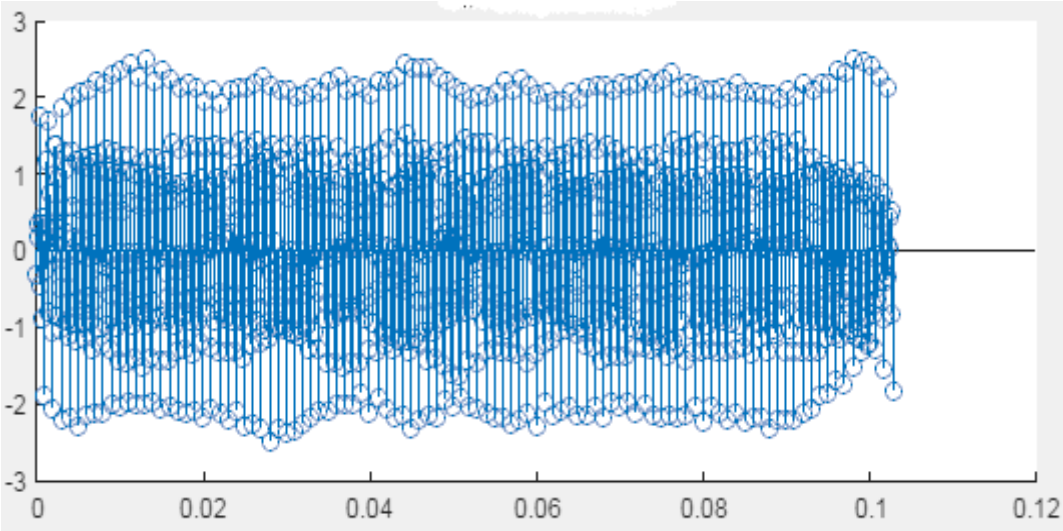


Fig-21 : Information of the sampled signal $\boldsymbol{x}$

There are some differences between the initial information and the visualized information. Likewise for its discrete Fourier transforms. These differences are caused by these two reasons:

- Quantization noise during analog to digital conversion;
- The OMP approximation error when viewing the sparse representation of the sampled signal.

13. CONCLUSION

Through the use of compressive sensing which is just the new theory of signal acquisition and compression, we were able to reduce the information size of an analog signal to save energy, bandwidth transmission medium and storage memory capacities. The acquisition and compression of this information are done at the same time by an intelligent process of taking measurements. Thanks to the use of XOR cryptography and RSA cryptography, we were able to encrypt and decrypt the information of this analog signal with a fairly fast speed and a guarantee of security.

14. REFERENCES

[1] David L. Donoho and Michael Elad. *« Optimally sparse representation in general (nonorthogonal) dictionaries via l1 minimization »*. Proceedings of the National Academy of Sciences, URL : http : //www.pnas.org/content/100/5/2197.abstract,

[2] E.J. Candès and T. Tao. *« Decoding by linear programming »*. IEEE Tran*sactions* on Information Theory, December 2005.

[3] AS. Bandeira, E. Dobriban, D.G. Mixon, and W.F. Sawin. *« Certifying the restricted isometry property is hard »*. IEEE Transactions on Information Theory, June 2013.

[4] Z. Ben-Haim, Y.C. Eldar, and M. Elad. *« Coherence-based performance guarantees for estimating a sparse vector under random noise »*, IEEE Transactions on Signal, October 2010.

[5] L. Welch. *« Lower bounds on the maximum cross correlation of signals (corresp.) Information Theory »*, IEEE Transactions, May 1974.

[6] Dejan E. Lazich, Henning Zoerlein, and Martin Bossert. *« Low coherence sensing matrices based on best spherical codes. In* Systems, Communication and Coding *(SCC) »*, Proceedings of 2013 9th International ITG Conference, Jan 2013.

[7] J.A. Tropp. *« Greed is good: algorithmic results for sparse approximation. Information Theory »*, IEEE Transactions, Oct 2004.

[8] L. Zelnik-Manor, K. Rosenblum, and Y.C. *« Eldar. Sensing matrix optimization for block-sparse decoding. Signal Processing »*, IEEE Transactions, Sept 2011.

[9] T.T. Cai, Guangwu Xu, and Jun Zhang. *« On recovery of sparse signals via l1 minimization. Information Theory »*, IEEE Transactions, July 2009.

[10] T.T. Cai and Lie Wang. *« Orthogonal matching pursuit for sparse signal recovery with noise »*. IEEE Transactions on Information Theory, July 2011.

[11] H. Mamaghanian, N. Khaled, D. Atienza, and P. Vandergheynst. *« Compressed sensing for real-time energy-efficient ECG compression on wireless body sensor nodes »*. IEEE Transactions on Biomedical Engineering.

[12] Emmanuel Candès and Justin Romberg. *« Sparsity and incoherence in compressive sampling »*, 2007.

[13] Heping Song and Guoli Wang. *« Sparse signal recovery via ECME thresholding pursuits »*. Mathematical Problems in Engineering, 2012, URL : http : //www.hindawi.com.bases - doc.univlorraine.fr/journals/mpe/2012/478931/

[14] S. Chen, D. Donoho, and M. Saunders. *« Atomic decomposition by basis pursuit »*. SIAM Journal on Scientific Computing, January 1998.