Compressed sensing in cryptography

A. HadjBrahim*- A. ALI PACHA - N. HADJ SAID

Laboratory of Coding and Security of Information
University of Sciences and Technology of Oran Mohamed Boudiaf
PoBox 1505 Oran M'Naouer 31000
Corresponding authors: *hadj_94@hotmail.com, a.alipacha@gmail.com, naima.hadjsaid@univ-usto.dz*

Reçu le : 19/11/2020 Accepté le : 02/01/2020

Abstract-*Compressed sensing (CS) is a new signal processing technique, it allows the signal to be sampled at a rate much lower than the Shannon-Nyquist rate,and allows to sample and compress in one step using the sparsity of signal that can represent a signal with fewer number of samples. The signal can be sparse in the original domain or a different domain like the discrete cosine transform DCT, the discrete Fourier Transform DFT, Wavelet transform DWT…etc.the reconstruction of the CS allows recover the original signal with less compression measures. CS has already become a key concept in various fields applied mathematics,computer science,and electrical engineering and it has applied to various fields including radar imaging, the signal extraction…etc.*

In this paper, we present the theoretical bases of CS that divides into two parts first part is the acquisition model or the part of encryption,the second part is the various methods of reconstruction of the CS or the part of decryption.In addition, we give application of CS in cryptography and some others applications that use the CS technique.

Keywords-**Compressive Sensing CS / sparsity / signal sparse /recovery algorithm / minimizationl_1.**

Résumé-*L'acquisition comprimée(AC) est une nouvelle technique de traitement du signal, il permet d'échantillonner le signal à un taux très inférieur au taux de Shannon-Nyquist, et permet d'échantillonner et compresser dans une seule étape en utilisant la parcimonie de signal qui permet de représenter un signal avec moins de nombre d'échantillons. Le signal peut être parcimonie dans le domaine original ou un domaine différent comme la Transformée en cosinus discrète DCT, la Transformée en Fourier discrète DFT, Transformée en ondelettes DWT…etc. la reconstruction de l'AC permet du récupérer le signal original avec moins de mesures de compression. AC est déjà devenu un concept clé dans divers domaines des mathématiques appliquées,l'informatique,et le génie électrique et il est appliqué à divers domaines, y compris l'imagerie par radar, l'extraction de signal…etc.*

Dans cet article nous présentons les bases théoriques de l'AC qui divise en deux parties première partie c'est le modèle d'acquisition ou la partie du chiffrement, et le deuxième partie c'est les différentes méthodes de reconstruction de l'AC ou la partie du déchiffrement, et nous donnons l'application du l'AC dans la cryptographie et quelques d'autres applications qui utilisent la technique de l'AC.

Mots clés- **Acquisition comprimée AC / Parcimonie /signalépars / Algorithme de récupération / la minimisation l_1.**

1. INTRODUCTION

The digital acquisition systems relies on the Shannon-Nyquist theorem that says to avoid any loss of information in a signal, the sampling frequency must be greater than or equal twice the maximum frequency of the signal original.However, for some applications, such as radar and broadband communications the application of this theorem results in sampling rates that are almost beyond the limit of the physical capabilities of analog-to-digital converters[1]. Moreover, for transmission or storage it must use compression thus eliminate most of the coefficients (show in figure 1) to save energy, the bandwidth of the transmission medium and the storage memory.

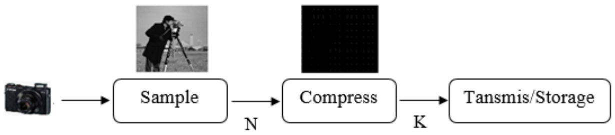

Figure 1:classical method of sampling and signal compression in the digital camera

The recently technique compressive sensing CS (or compressive sampling) introduced by Donoho et Candés et al [2]–[4] is a new signal processing technique, it allows to sample the signal at a rate much lower than the Shannon-Nyquist rate, and allows to sample and compression of signal in one step.

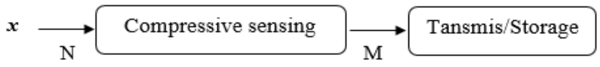

Figure 2: Compressive sensing

CS has already become a key concept in various fields such as radar imaging, signal extraction, laser scanning, medical imaging, surface metrology...etc [5].

CS relies on two principles sparsity and incoherence.

A signal is sparse if it contains only a few non-zero elements or approximately sparse if it contains only a few voluminous elements and if the other elements are almost null[6].Suppose that $\boldsymbol{x}$ a signal vector of$\boldsymbol{R}^{\boldsymbol{N}\boldsymbol{x}\boldsymbol{1}}$, this vector is sparse if it has $\boldsymbol{K}$ non-zero elements with $\boldsymbol{K} << \boldsymbol{N}$.In most of the cases,the measurement signal may have a sparse representation in a particular domain$\boldsymbol{\psi}$ like the discrete cosine transform DCT, the discrete Fourier Transform DFT, Wavelet transform DWT… etc (for example a Dirac spike in the space domain extends into the frequency domain).The minimum number of samples to reconstruct a signal depends on its parsimony and not its bandwidth [6].

If the vector $\boldsymbol{x}$ is not sparse then it can have a sparse representation such as equation (1):

$$\boldsymbol{x} = \boldsymbol{\psi} * \boldsymbol{\alpha} \qquad (1)$$

With $\boldsymbol{\psi}$ a matrix $\boldsymbol{R}^{\boldsymbol{N}\boldsymbol{x}\boldsymbol{N}}$and $\boldsymbol{\alpha}$a vector has only $\boldsymbol{K}$ non-zero elements.

Incoherence expresses the idea that objects with sparse representation in domain $\boldsymbol{\psi}$must dispersed in the field in which they acquired,it indicates that, unlike the signal of interest the sampling/sensing waveforms have an extremely dense representation in$\boldsymbol{\psi}$ [7].

2. ACQUISITION MODEL

The acquisition model shown in figure 3 [8] :

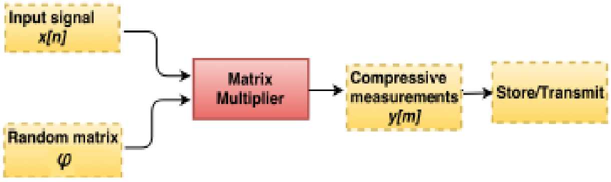

Figure 3: acquisition model

The acquisition model can written mathematically by the equation (2):

$$Y=\emptyset *x= \emptyset *\psi*\alpha= A * \alpha \qquad (2)$$

Where $\boldsymbol{x}$ is signal original$\boldsymbol{R}^{\boldsymbol{N}\boldsymbol{x}\boldsymbol{1}}$, $\boldsymbol{\emptyset}$ matrix $\boldsymbol{R}^{\boldsymbol{M}\boldsymbol{x}\boldsymbol{N}}$ ($\boldsymbol{K} <\boldsymbol{M} <\boldsymbol{N}$) and called measurement matrix, $\boldsymbol{Y}$ is a $\boldsymbol{R}^{\boldsymbol{M}\boldsymbol{x}\boldsymbol{1}}$measurement vector, $\boldsymbol{A}$ is the holographic dictionary and$\boldsymbol{A} = \emptyset * \boldsymbol{\psi}$.

In the equation (2), we assume that the measurements are accurate. However,in any real application,the measured data will invariably corrupted by at least a small amount of noise, since detection devices do not have infinite precision.It is therefore imperative to develop stable recovery algorithms of CS where small disturbances in the data should only cause small disturbances in the reconstruction[9].Taking into account the presence of additive noise during the acquisition phase, the equation (2) becomes equation (3):

$$Y= A * \alpha+\varepsilon \qquad (3)$$

Where $\boldsymbol{\varepsilon} \in \boldsymbol{R}^{\boldsymbol{M}}$is a vector representing the noise.In most of the cases,it considered as a Gaussian white noisewith a zero average and a variance $\boldsymbol{\sigma}^{\boldsymbol{2}}$, $\boldsymbol{N}(\boldsymbol{0}, \boldsymbol{\sigma}^{\boldsymbol{2}}$)[10].

The compressed sensing theory indicates that the sparse signal $\boldsymbol{\alpha}$ may recover by taking$M \geq O(K \log\left(\frac{N}{K}\right))$[6].

For $\boldsymbol{M} << \boldsymbol{N}$ then there exists an infinity of vectors α satisfying the equations (2) and (3),therefore the measurement matrix $\boldsymbol{\emptyset}$ (or in general $\boldsymbol{A}$) must satisfy a certain conditions.

2.1. Mutual coherence

The coherence$\boldsymbol{\mu}$ of the measurement matrix $\boldsymbol{\emptyset}$ and the representation base $\boldsymbol{\psi}$ is:
$\boldsymbol{\mu}(\emptyset, \boldsymbol{\psi}) = \sqrt{\boldsymbol{N}}\boldsymbol{max}_{1\leq k,j\leq N} | < \emptyset_k \boldsymbol{\psi}_j > |$(4)

The coherencemeasures the greatest correlation between any two elements $\boldsymbol{\emptyset}$ and $\boldsymbol{\psi}$.It follows from linear algebra that$\boldsymbol{\mu}(\emptyset, \boldsymbol{\psi}) \in [\mathbf{1}, \sqrt{\boldsymbol{N}}]$.CS mainly concerns low coherence pairs [7].

2.2. Condition of uniqueness

To ensure that two separate signals $\boldsymbol{\alpha}_1$and$\boldsymbol{\alpha}_2$generate two different measurement vectors $\boldsymbol{Y}_1 = \boldsymbol{A}\boldsymbol{\alpha}_1and\boldsymbol{Y}_2 = \boldsymbol{A}\boldsymbol{\alpha}_2(\boldsymbol{Y}_1 \neq \boldsymbol{Y}_2)$.Established the following equation (5):

$$\boldsymbol{K} < \frac{1}{2}\ \textbf{\textit{Spark (A)}} \qquad (5)$$

Where ***Spark (A)*** of a matrix ***A*** is equal to the smallest number of columns of ***A*** that are linearly dependent.Since the value of ***Spark (A)*** varies between two and (M + 1), so ***M>2K***.This theorem guarantee the uniqueness of the representation of a sparse vector,therefore for each measurement vector ***Y***, there is at most one sparse signal $\boldsymbol{\alpha}$ such as$\boldsymbol{Y = A\alpha}$[1].

2.3. Restricted isometry property RIP

A matrix ***A*** satisfied the RIP of order ***K*** if there is constant $\boldsymbol{\delta_k} \in]\mathbf{0}, \mathbf{1}[$called restricted isometry constant (RIC),verifying the equation (6) [11]:

$$(1- \delta_k)||\ \alpha||_2{}^2 \leq ||\ A\alpha||_2{}^2 \leq (1+\delta_k)||\ \alpha||_2{}^2 (6)$$

Where $||\ \boldsymbol{x}||_2 = \sqrt{\sum_{i=1}^{N} \boldsymbol{x}_i^2}$called norm $\boldsymbol{l}_2$.TheRIP check if the measurement matrix ***A*** is close to an isometry (if it preserves the distance between two measurement vectors).In other words.If the measurement matrix satisfies the RIP then the distance between two measurement vectors $\boldsymbol{Y}_1 = \boldsymbol{A}\boldsymbol{\alpha}_1and\boldsymbol{Y}_2 = \boldsymbol{A}\boldsymbol{\alpha}_2$is proportional to the distance between $\boldsymbol{\alpha}_1$and$\boldsymbol{\alpha}_2$, the RIP is an important property that guarantee the reconstruction of the signal.However, it is difficult to verify whether a matrix satisfies the RIP or not[12].

2.4. Choose the measurement matrix

The studies have shown that when measurement matrices are built randomly (like Random Gaussian Matrix) these conditions can be met with a high probability[13]. Recently, deterministic matrices have proposed to facilitate implementation. They have specially designed to have low coherence [14][15][16].

3. RECONSTRUCTIONMODEL

The original signal reconstructed from the ***Y*** measurement vector, the measurement matrix $\boldsymbol{\emptyset}$ and domain $\boldsymbol{\psi}$ during a phase called the reconstruction phase.It work in two steps(figure 4 [8]):

- The first step is to find the vector $\widehat{\boldsymbol{\alpha}}$ corresponding to the solution of the equation 2 (or equation 3 in the case of noise).
- Once $\widehat{\boldsymbol{\alpha}}$ obtained, the final step reconstructs the signal$\widehat{\boldsymbol{x}} = \boldsymbol{\psi} * \widehat{\boldsymbol{\alpha}}$.

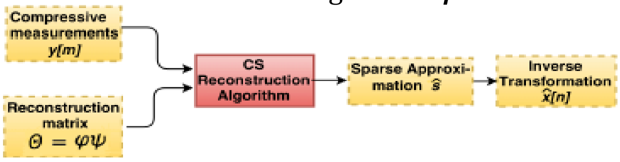
Compressive measurements $y[m]$
Reconstruction matrix $\Theta = \varphi\psi$
CS Reconstruction Algorithm
Sparse Approximation $\hat{s}$
Inverse Transformation $\hat{x}[n]$

Figure 4: Reconstruction model

Since ***M<N*** there are an infinity of vectors α satisfying the equation 2 (or equation 3 in the case of noise), But taking into account the hypothesis that $\boldsymbol{\alpha}$ is sparse in the domain$\boldsymbol{\psi}$.the problem is to solve the minimization $\boldsymbol{l}_0$(the equation7):

$$\min_{\widehat{\alpha}} ||\widehat{\alpha}||_0 \textit{such as } A\widehat{\alpha} = Y \qquad (7)$$

In the case of noise, the equation (7) become equation (8):

$$\min_{\widehat{\alpha}} ||\widehat{\alpha}||_0 \textit{such as } ||Y - A\widehat{\alpha}||_2 \leq b \qquad (8)$$

Where $||x||_0 = \{i : x_i \neq 0\}$called norm $\boldsymbol{l}_0$,and ***b*** represents the noise power expected in observations[1].

Solving this equation requires an exhaustive search for the sparsest solution $\widehat{\boldsymbol{\alpha}}$ and is very complex to implement [11].Several methods have proposed in the literature to work around this problem.They can categorized into three groups [17] :

- Greedypursuit, for example matching pursuit (MP) its extension called Orthogonal Matching Pursuit (OMP).They are iterative methods and generally easy to implement.At each iteration,they select one or more columns of the matrix $\boldsymbol{A}$ according to its correlation with the measurement vector $\boldsymbol{Y}$.Then, they measure an approximation of the signal and update the residual that will be used in the next iteration[18][19][20].
- Convex relaxation, for example basis pursuit (BP).They consist of finding convex minimizations that are approaching the equation (7) (or equation 8 in the case of noise)[21].
- Bayesian inference for example sparse Bayesian learning.

3.1. Matching pursuit (MP)

When the measurement matrix $\boldsymbol{A}$ is an orthogonal base, it is possible to reconstruct an approximation of the signal by selecting one by one the columns of $\boldsymbol{A}$ having a maximum correlation with the residual [1].MP is the simplest version of greedy algorithms.
The MP start by initializing the residual $\boldsymbol{r}$ with the $\boldsymbol{Y}$ measurement vector.It also initialize the approximation of the signal $\widehat{\boldsymbol{\alpha}}$ by a null vector, like in the equation (9)[22]:

$$\boldsymbol{r_0} \leftarrow \boldsymbol{Y} \qquad \widehat{\boldsymbol{\alpha}} \leftarrow \boldsymbol{0} \tag{9}$$

At each iteration $\boldsymbol{k}$, MP select a column of the matrix $\boldsymbol{A}$ having a maximum correlation with the residual:

$$\boldsymbol{\delta_k} = \boldsymbol{arg\ max}\ |\langle \boldsymbol{r_{k-1}}, \boldsymbol{a_i}\rangle| \tag{10}$$

Where $\boldsymbol{\delta_k}$the index of the selected column,$\boldsymbol{r_{k-1}}$is the residual of the previous iteration, $\boldsymbol{a_{i\in\{1,N\}}}$represents the columns of matrix $\boldsymbol{A}$.

Then, the MP calculates a new approximation of the signal and update the residual:

$$\widehat{\boldsymbol{\alpha_k}} = \widehat{\boldsymbol{\alpha_{k-1}}} + \langle \boldsymbol{r_{k-1}}, \boldsymbol{a_{\delta_k}}\rangle \boldsymbol{a_{\delta_k}} \tag{11}$$

$$\boldsymbol{r_k} = \boldsymbol{r_{k-1}} - \langle \boldsymbol{r_{k-1}}, \boldsymbol{a_{\delta_k}}\rangle \boldsymbol{a_{\delta_k}} \tag{12}$$

Where $\widehat{\boldsymbol{\alpha_{k-1}}}$represents the approximation of the signal obtained during the previous iteration,$\boldsymbol{a_{\delta_k}}$is the column of matrix $\boldsymbol{A}$ selected.

Iteration stops when a certain condition met.In the literature, several stopping conditions have proposed [23]:

- Stop after a finite number of iterations.
- Stop when the amplitude of the residual is lower than a predefined threshold.

The disadvantage of this method is that the measurement matrix $\boldsymbol{A}$ is not always orthogonal.In this case, a column of matrix $\boldsymbol{A}$ can selected several times during the selection phase.MP converges exponentially [22].

3.2. Basis Pursuit (BP)

To get around the complexity of the minimization $\boldsymbol{l_0}$methods based on convex relaxation,like norm $\boldsymbol{l_1}$known asBasis Pursuit (BP) introduced by Chen, Donoho and Saunders,relax the problem by replacing the norm $\boldsymbol{l_0}$ with norm $\boldsymbol{l_1}$if matrix $\boldsymbol{A}$satisfies the RIPand use convex solvers to solve the equation (13):

$$\underset{\widehat{\boldsymbol{\alpha}}}{\boldsymbol{min}} \|\widehat{\boldsymbol{\alpha}}\|_{\boldsymbol{1}} \boldsymbol{such\ as\ A\widehat{\alpha} = Y} \tag{13}$$

In the case of noise, equation (13) become equation (14):

$$\underset{\widehat{\boldsymbol{\alpha}}}{\boldsymbol{min}} \|\widehat{\boldsymbol{\alpha}}\|_{\boldsymbol{1}} \boldsymbol{such\ as} \|\boldsymbol{Y} - \boldsymbol{A\widehat{\alpha}}\|_{\boldsymbol{2}} \leq \boldsymbol{b} \tag{14}$$

Where $\|\boldsymbol{x}\|_{\boldsymbol{1}} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} |\boldsymbol{x}|$called norm $\boldsymbol{l_1}$.Interest of norm $\boldsymbol{l_1}$resides in the fact that unlike norm $\boldsymbol{l_0}$it is convex.The equations 13 and 14 reduced to a simple linear programming problem.Many minimizations are then considered[21].

Figure 5 illustrates this fact.In all three cases,we have the same set of solutions represented by a straight line and the solution of the minimization represented by a red dot.Figure 5a shows the minimization of the norm $\boldsymbol{l_0}$, norm $\boldsymbol{l_1}$in Figure 5b reconstructed a good solution, while minimization $l_2$in Figure 5c gives a rough solution [21].

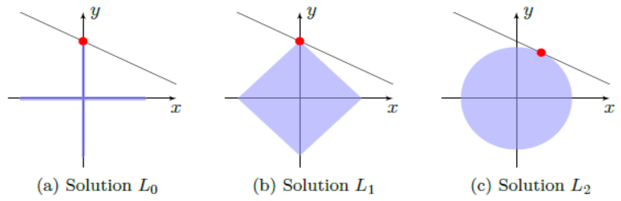

Figure 5: Reconstruction according to different norm

3.3. Greedypursuit VS Convex relaxation

According to the literature, greedy algorithms are easy to implement and potentially fast compared to those based on convex relaxation [24][25]. However, convex relaxation require fewer samples to reconstruct the original signal compared to greedy algorithms [26].

3.4. Basis pursuit denoising (BPDN)

In the literature, the method using the equation 13 called basis pursuit with inequality constraints (BPIC).Another variant of this method called basis pursuit denoising (BPDN)consists of reformulate the problem of the equation (15) [27]:

$$\min_{\widehat{\alpha}} \frac{1}{2}\left|\left|Y - A\widehat{\alpha}\right|\right|^{2}_{2} + \lambda\left|\left|\widehat{\alpha}\right|\right|_{1} \qquad (15)$$

Where $\lambda > 0$the balancing parameter.

4. Application of the compressed sensing

4.1. Compressed sensing in cryptography

One of the important application of CS is cryptography. CS resolves the measurement matrix as a secret key and the compressive measures as an encrypted message.Which makes the CS a technique of simultaneous acquisition, compression and encryption of signals [8].And by taking M>2K guarantee the perfect security of data [28].

4.1.1 Image encryption

Encryption images with CS is one of the most big research that use the new technique CS, many algorithms was developed in last few years such as [29]–[32]. Since the measurement matrix is the key of the encryption, the objective of the research was how to develop this matrix to give the same result as the Gaussian matrix since the result of Gaussian matrix is the best result but this matrix have a large of size and very difficult to change between two points. The study of encryption image by CS show that one of the best methods to generate this matrix isthe chaotic systems since you need only the initial parameters of the chaotic systems as key to send it. The major of algorithms works with the following steps: by transform the plain image to DCT image or DWT image that change the matrix of the plain image to sparse matrix with most of their elements are nulls, then use the chaotic systems to generate the measurement matrix. The last step is applied the CS between the sparse matrix and the measurement matrix to have the cipher image. For more complexity of encryption, the most of the algorithms used scrambling method such as the bloc Arnold to make very hard to decrypt the image without the right key. To recover plain image from the cipher image they used one of the reconstruction algorithm described in section 3 like minimization l_0, minimization l_1...etc.This image encryption are used in various domain such as:

- Data hiding: this method was proposed in [33]–[35], The integration rate has a big boost compared to the method of masking separable data existing in the encrypted image[36].
- image authentication: this method was employed in [37], [38], encrypt a finger image using CS when capturing image, while finger image can only be restored on the authentication server.

4.1.2 Cloud security

The cloud computing have guaranteed confidentiality based on CS [39], [40], Different domain technologies have been synthesized to find the perspective of security, efficiency and complexity aspects. The outsourcing of the sparse reconstruction service to several clouds in parallel has been described in [41],while each cloud has only few information of measurement and asymmetrical support set, the security of the plain image is guaranteed.

4.1.3 Security in 5G system

Security in 5G system based on CS has been proposed in [42], [43],it’s show that the sparse signal that is the principle of CS can be the source of the requirements 5G system and avoid the sampling with the Nyquist method, and that cause the reduce of the complexity and increased reliability.

4.1.4 A simple encryption image with CS

We used DCT domain to transform matrix to sparse matrix, and logistic map as chaotic system to generate measurement matrix and their equation is:

$$\boldsymbol{s_{n+1} = \mu\,(1 - s_n)} \qquad (16)$$

Where s_0 is initial condition, µ the coefficient of parameter and **n** the number of iterations. We tooks_0=0.1, µ=3.9999. The compression ratio with the equation:

$$CR = \frac{T_1 \text{ x } T_2}{e_1 \text{ x } e_2} \qquad (17)$$

Where T_1 ,T_2 the size of the plain image and e_1 ,e_2 the size of the encryption image, in this examples CR≈0.5.

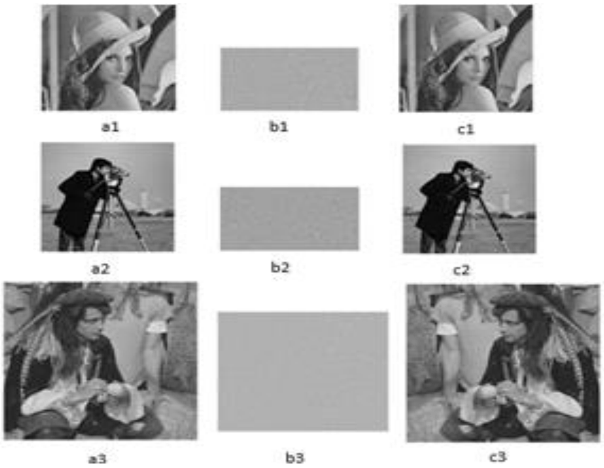

Figure 6: simulations and results of a simple encryption with CS, a(1-4) plain image, b(1-4) cipher image, c(1-4) decrypted image

We calculated the PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index Measurement) with the following equations:

$$PSNR = 10\log\frac{255*255}{(1/M*N)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X(i,j)-Y(i,j)\right)^2}$$

(18)

Where M, N the size of the image and X (i, j) and Y (i, j) are the pixel.

$$SSIM = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \qquad (19)$$

where $C_1 = (k_1 \times L)^2$, $C_2 = (k_2 \times L)^2$, k_1= 0.01 ,k_2 = 0.02, L = 255 , and μ_x , μ_y , σ_x , σ_y , σ_{xy} represent the mean, variances and covariances of the plain image and decrypted image, respectively.

Table 1: PSNRs (dB) and SSIMs for different images

Image(pixels)	PSNR(dB)	SSIM
Lena(256x256)	24.8045	0.5691
Cameraman(256x256)	24.2178	0.5312
Man(512x512)	24.3192	0.5166

4.2. Others Applications of CS

4.2.1 Compressive imaging

-Single-pixel camera: One of the first and very famous architectures illustrating the compressive imagery proposed by Duarte et al [44].

-Radar Imaging Systems: The different types of radar imaging techniques for which CS has used are synthetic aperture radar (SAR) inverse synthetic aperture radar (ISAR), the wall imaging radar (TWR), ground-penetrating radar imaging (GPR) [45]–[48].

4.2.2 Video processing

Among the video processing techniques based on CS: distributed compressed video detection, the sampling of video images is done independently while the reconstruction is done jointly. Detection adaptive video using block-based CS reconstruction and CS streaming for high-speed periodic videos based on coded projections of dynamic events…etc [49][50].

5. CONCLUSION

CS has revolutionized many areas like camera, radar information security, communications networks, biomedical ... etc, one of the most of areas is the cryptography, and by using the measurement matrix as key, the secure of data can be guaranteed. In this paper, we have detailed the basic theory principle ofCS with some reconstruction algorithms and some applications in different fields specifically in the domain of cryptography, and the major of research is how to develop the measurement matrix like with chaotic systems. In addition, for more clearly, we gave a simple example of encryption image by CS using logistic map for generate the measurement matrix. The CS will be the key of revolution network like 5G and cloud scenario…etc, because this technique is better that the existing technique.

References

[1] A. Ravelomanantsoa, « Approche déterministe de l'acquisition comprimée et la reconstruction des signaux issus de capteurs intelligents distribués », PhD Thesis, Université de Lorraine-France, 2015.

[2] E. Candès, J. Romberg, and T. Tao., « Robust uncertainty principles : Exact signal reconstruction from highly incomplete frequency information. IEEE Transactions on Information Theory, 52(2) », p. 489-509, 2006.

[3] E. Candès, et al, « Compressive sampling. Proceedings of the international congress of mathematicians, 3 », p. 1433-1452, 2006.

[4] D. L. Donoho, « Compressed sensing, IEEE Trans. Inform. Theory, vol. 52, no. 4 », p. 1289–1306, avr-2006.

[5] T. B. T. Nguyen, « La programmation DC et DCA en analyse d'image : acquisition comprimée, segmentation et restauration », thesis, Université de Lorraine-France, 2014.

[6] Electrical and Electronic Engineering Department, Islamic Azad University, South Tehran Branch, Tehran, Iran., F. K. Ranjbar, et S. Ghofrani, « Evaluation Compressive Sensing Recovery Algorithms in Crypto Steganography System », *Int. J. Image Graph. Signal Process.*, vol. 8, nº 10, p. 53-63, oct. 2016, doi: 10.5815/ijigsp.2015.10.07.

[7] E. J. Candes et M. B. Wakin, « An Introduction To Compressive Sampling », *IEEE Signal Process. Mag.*, vol. 25, nº 2, p. 21-30, mars 2008, doi: 10.1109/MSP.2007.914731.

[8] M. Rani, S. B. Dhok, et R. B. Deshmukh, « A Systematic Review of Compressive Sensing: Concepts, Implementations and Applications », *IEEE Access*, vol. 6, p. 4875-4894, 2018, doi: 10.1109/ACCESS.2018.2793851.

[9] Y. Xianjun, « Research on compressed sensing and its application in wireless communications », 2014.

[10] T. T. Cai et L. Wang, « Orthogonal Matching Pursuit for Sparse Signal Recovery With Noise », *IEEE Trans. Inf. Theory*, vol. 57, nº 7, p. 4680-4688, juill. 2011, doi: 10.1109/TIT.2011.2146090.

[11] E. J. Candes et T. Tao, « Decoding by Linear Programming », *IEEE Trans. Inf. Theory*, vol. 51, nº 12, p. 4203-4215, déc. 2005, doi: 10.1109/TIT.2005.858979.

[12] A. S. Bandeira, E. Dobriban, D. G. Mixon, et W. F. Sawin, « Certifying the Restricted Isometry Property is Hard », *IEEE Trans. Inf. Theory*, vol. 59, nº 6, p. 3448-3450, juin 2013, doi: 10.1109/TIT.2013.2248414.

[13] E. J. Candes et T. Tao, « Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? », *IEEE Trans. Inf. Theory*, vol. 52, nº 12, p. 5406-5425, déc. 2006, doi: 10.1109/TIT.2006.885507.

[14] *9th International ITG Conference on Systems, Communication, and Coding (SSC 2013): January 21-24, 2013 in Munich, Germany*. Berlin: VDE Verlag GmbH, 2013.

[15] « A Reed-Solomon Code Based Measurement Matrix with Small Coherence », *IEEE Signal Process. Lett.*, vol. 21, nº 7, p. 839-843, juill. 2014, doi: 10.1109/LSP.2014.2314281.

[16] S. Li et G. Ge, « Deterministic Sensing Matrices Arising From Near Orthogonal Systems », *IEEE Trans. Inf. Theory*, vol. 60, nº 4, p. 2291-2302, avr. 2014, doi: 10.1109/TIT.2014.2303973.

[17] H. Song et G. Wang, « Sparse Signal Recovery via ECME Thresholding Pursuits », *Math. Probl. Eng.*, vol. 2012, p. 1-22, 2012, doi: 10.1155/2012/478931.

[18] European Association for Signal Processing et Institute of Electrical and Electronics Engineers, Éd., *2012 proceedings of the 20th European Signal Processing Conference (EUSIPCO 2012): Bucharest, Romania, 27 - 31 August 2012*. Piscataway, NJ: IEEE, 2012.

[19] T. Blumensath et M. E. Davies, *On the Difference Between Orthogonal Matching Pursuit and Orthogonal Least Squares*. 2007.

[20] M. E. Davies et T. Blumensath, « Faster & greedier: algorithms for sparse reconstruction of large datasets », *2008 3rd Int. Symp. Commun. Control Signal Process.*, p. 774-779, 2008.

[21] S. Rousseau, « Feature detection in a multispectral image by compressed sensing », Theses, Université de Poitiers, 2013.

[22] J. A. Tropp, « Greed is Good: Algorithmic Results for Sparse Approximation », *IEEE Trans. Inf. Theory*, vol. 50, nº 10, p. 2231-2242, oct. 2004, doi: 10.1109/TIT.2004.834793.

[23] J. A. Tropp et S. J. Wright, « Computational Methods for Sparse Solution of Linear Inverse Problems », *Proc. IEEE*, vol. 98, nº 6, p. 948-958, juin 2010, doi: 10.1109/JPROC.2010.2044010.

[24] J. A. Tropp et A. C. Gilbert, « Signal Recovery From Random Measurements Via Orthogonal Matching Pursuit », *IEEE Trans. Inf. Theory*, vol. 53, nº 12, p. 4655-4666, déc. 2007, doi: 10.1109/TIT.2007.909108.

[25] S. Kunis et H. Rauhut, « Random Sampling of Sparse Trigonometric Polynomials, II. Orthogonal Matching Pursuit versus Basis Pursuit », *Found. Comput. Math.*, vol. 8, nº 6, p. 737-763, déc. 2008, doi: 10.1007/s10208-007-9005-x.

[26] T. T. Do, L. Gan, N. Nguyen, et T. D. Tran, « Sparsity adaptive matching pursuit algorithm for practical compressed sensing », in *2008 42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2008, p. 581-587, doi: 10.1109/ACSSC.2008.5074472.

[27] Z. Ben-Haim, Y. C. Eldar, et M. Elad, « Coherence-Based Performance Guarantees for Estimating a Sparse Vector Under Random Noise », *IEEE Trans. Signal Process.*, vol. 58, nº 10, p. 5030-5043, oct. 2010, doi: 10.1109/TSP.2010.2052460.

[28] M. Ramezani Mayiami, B. Seyfe, et H. G. Bafghi, « Perfect secrecy via compressed sensing », in *2013 Iran Workshop on Communication and Information Theory*, Tehran, 2013, p. 1-5, doi: 10.1109/IWCIT.2013.6555751.

[29] J. Chen, Y. Zhang, L. Qi, C. Fu, et L. Xu, « Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression », *Opt. Laser Technol.*, vol. 99, p. 238-248, févr. 2018, doi: 10.1016/j.optlastec.2017.09.008.

[30] Q. Xu, K. Sun, C. Cao, et C. Zhu, « A fast image encryption algorithm based on compressive sensing and hyperchaotic map », *Opt. Lasers Eng.*, vol. 121, p. 203-214, oct. 2019, doi: 10.1016/j.optlaseng.2019.04.011.

[31] N. Zhou, H. Li, D. Wang, S. Pan, et Z. Zhou, « Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform », *Opt. Commun.*, vol. 343, p. 10-21, mai 2015, doi: 10.1016/j.optcom.2014.12.084.

[32] N. Zhou, S. Pan, S. Cheng, et Z. Zhou, « Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing », *Opt. Laser Technol.*, vol. 82, p. 121-133, août 2016, doi: 10.1016/j.optlastec.2016.02.018.

[33] D. Xiao et S. Chen, « Separable data hiding in encrypted image based on compressive sensing », *Electron. Lett.*, vol. 50, nº 8, p. 598-600, avr. 2014, doi: 10.1049/el.2013.3806.

[34] G. Hua, Y. Xiang, et G. Bi, « When Compressive Sensing Meets Data Hiding », *IEEE Signal Process. Lett.*, vol. 23, nº 4, p. 473-477, avr. 2016, doi: 10.1109/LSP.2016.2536110.

[35] M. Li, D. Xiao, et Y. Zhang, « Reversible Data Hiding in Block Compressed Sensing Images », *ETRI J.*, vol. 38, nº 1, p. 159-163, févr. 2016, doi: 10.4218/etrij.16.0114.0242.

[36] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, et X. He, « A Review of Compressive Sensing in Information Security Field », *IEEE Access*, vol. 4, p. 2507-2519, 2016, doi: 10.1109/ACCESS.2016.2569421.

[37] H. Suzuki, M. Takeda, T. Obi, M. Yamaguchi, N. Ohyama, et K. Nakano, « Encrypted sensing for enhancing security of biometric authentication », in *2014 13th Workshop on Information Optics (WIO)*, Neuchatel, 2014, p. 1‑3, doi: 10.1109/WIO.2014.6933292.

[38] H. Suzuki, M. Suzuki, T. Urabe, T. Obi, M. Yamaguchi, et N. Ohyama, « Secure biometric image sensor and authentication scheme based on compressed sensing », *Appl. Opt.*, vol. 52, nº 33, p. 8161, nov. 2013, doi: 10.1364/AO.52.008161.

[39] L.-W. Kang, K. Muchtar, J.-D. Wei, C.-Y. Lin, D.-Y. Chen, et C.-H. Yeh, « Privacy-preserving multimedia cloud computing via compressive sensing and sparse representation », in *2012 International Conference on Information Security and Intelligent Control*, Yunlin, Taiwan, 2012, p. 246‑249, doi: 10.1109/ISIC.2012.6449752.

[40] C. Wang, B. Zhang, K. Ren, et J. M. Roveda, « Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud », *IEEE Trans. Emerg. Top. Comput.*, vol. 1, nº 1, p. 166‑177, juin 2013, doi: 10.1109/TETC.2013.2273797.

[41] Y. Zhang, J. Zhou, L. Y. Zhang, F. Chen, et X. Lei, « Support-Set-Assured Parallel Outsourcing of Sparse Reconstruction Service for Compressive Sensing in Multi-clouds », in *2015 International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec)*, Hangzhou, China, 2015, p. 1‑6, doi: 10.1109/SocialSec2015.10.

[42] G. Wunder, H. Boche, T. Strohmer, et P. Jung, « Sparse Signal Processing Concepts for Efficient 5G System Design », *IEEE Access*, vol. 3, p. 195‑208, 2015, doi: 10.1109/ACCESS.2015.2407194.

[43] Z. Gao, L. Dai, S. Han, C.-L. I, Z. Wang, et L. Hanzo, « Compressive Sensing Techniques for Next-Generation Wireless Communications », *IEEE Wirel. Commun.*, vol. 25, nº 3, p. 144‑153, juin 2018, doi: 10.1109/MWC.2017.1700147.

[44] M. F. Duarte *et al.*, « Single-pixel imaging via compressive sampling », *IEEE Signal Process. Mag.*, vol. 25, nº 2, p. 83‑91, mars 2008, doi: 10.1109/MSP.2007.914730.

[45] V. M. Patel, G. R. Easley, D. M. Healy, et R. Chellappa, « Compressed Synthetic Aperture Radar », *IEEE J. Sel. Top. Signal Process.*, vol. 4, nº 2, p. 244‑254, avr. 2010, doi: 10.1109/JSTSP.2009.2039181.

[46] L. Zhang *et al.*, « Resolution Enhancement for Inversed Synthetic Aperture Radar Imaging Under Low SNR via Improved Compressive Sensing », *IEEE Trans. Geosci. Remote Sens.*, vol. 48, nº 10, p. 3824‑3838, oct. 2010, doi: 10.1109/TGRS.2010.2048575.

[47] Qiong Huang, Lele Qu, Bingheng Wu, et Guangyou Fang, « UWB Through-Wall Imaging Based on Compressive Sensing », *IEEE Trans. Geosci. Remote Sens.*, vol. 48, nº 3, p. 1408‑1415, mars 2010, doi: 10.1109/TGRS.2009.2030321.

[48] A. C. Gurbuz, J. H. McClellan, et W. R. Scott Jr., « Compressive sensing for subsurface imaging using ground penetrating radar », *Signal Process.*, vol. 89, nº 10, p. 1959‑1972, oct. 2009, doi: 10.1016/j.sigpro.2009.03.030.

[49] S. Mun et J. E. Fowler, « Residual Reconstruction for Block-Based Compressed Sensing of Video », in *2011 Data Compression Conference*, Snowbird, UT, USA, 2011, p. 183‑192, doi: 10.1109/DCC.2011.25.

[50] T. T. Do, Yi Chen, D. T. Nguyen, N. Nguyen, L. Gan, et T. D. Tran, « Distributed compressed video sensing », in *2009 16th IEEE International Conference on Image Processing (ICIP)*, Cairo, Egypt, 2009, p. 1393‑1396, doi: 10.1109/ICIP.2009.5414631.