Open access • Proceedings Article • DOI:10.1109/IEMBS.2010.5627119

Compressive sensing: From "Compressing while Sampling" to "Compressing and Securing while Sampling" — Source link

Amir M. Abdulghani, Esther Rodriguez-Villegas

Institutions: Imperial College London

Published on: 01 Jan 2010 - International Conference of the IEEE Engineering in Medicine and Biology Society

Topics: Multidimensional signal processing, Sampling (signal processing), Signal reconstruction, Signal and Signal processing

32nd Annual International Conference of the IEEE EMBS
Buenos Aires, Argentina, August 31 - September 4, 2010

Compressive Sensing: From "Compressing while Sampling" to "Compressing and Securing while Sampling"

Amir M. Abdulghani, *Student Member, IEEE* and Esther Rodriguez-Villegas, *Senior Member, IEEE*

***Abstract*—In a traditional signal processing system sampling is carried out at a frequency which is at least twice the highest frequency component found in the signal. This is in order to guarantee that complete signal recovery is later on possible. The sampled signal can subsequently be subjected to further processing leading to, for example, encryption and compression. This processing can be computationally intensive and, in the case of battery operated systems, unpractically power hungry. Compressive sensing has recently emerged as a new signal sampling paradigm gaining huge attention from the research community. According to this theory it can potentially be possible to sample certain signals at a lower than Nyquist rate without jeopardizing signal recovery. In practical terms this may provide multi-pronged solutions to reduce some systems computational complexity. In this work, information theoretic analysis of real EEG signals is presented that shows the additional benefits of compressive sensing in preserving data privacy. Through this it can then be established generally that compressive sensing not only compresses but also secures while sampling.**

Keywords: Compressive Sensing, Data Security, Encryption, Privacy Preservation, Power efficient, Wireless Systems, EEG.

I. Introduction

Guaranteeing data security and privacy are extremely crucial issues in most engineering systems and processes dealing with personal data. Under the UK Data Protection Act 1998 [1], records which contain physical or mental health information of a person such as clinical notes, laboratory reports, radiographs, imaging records, monitoring equipment outputs etc., are generally held under legal and ethical obligations of confidentiality [2].

In general, transmission of data over non-secure channels, such as wireless links, poses major risks to data security. Therefore, when designing portable wireless health monitoring devices confidentiality and security aspects should be given considerable attention. One of the methods for securing sensitive data is through encryption [3]. Unfortunately though, this is a computationally intensive process, which in the case of portable embedded systems can have significant impact in their battery life.

A. M. Abdulghani is with the Department of Electrical and Electronic Engineering, Imperial College London SW7 2AZ, UK, on study leave from the Sultan Qaboos University, Oman, (e-mail: amirm@imperial.ac.uk).

E. Rodriguez-Villegas is with the Department of Electrical and Electronic Engineering, Imperial College London SW7 2AZ, UK, (e-mail: e.rodriguez@imperial.ac.uk).

The research leading to these results has received funding from the European Research Council under the European Community's 7th Framework Programme (FP7/2007-2013) / ERC grant agreement no 239749

Compressive sensing has recently emerged as a new signal sampling paradigm. It is based on randomly sampling certain signals which meet a series of criteria to effectively achieve a sub-Nyquist sampling rate. From a wireless portable system perspective this can lead to advantages in terms of data rate and potentially power consumption [4].

This paper explores a further potential benefit of compressive sensing: its inherent capability to provide a certain level of security in the compressed data, without adding any extra computational cost. The paper explores the privacy preservation properties of compressive sensing when applied to scalp electroencephalography (EEG) brainwave signals. The relevance of using compressive sensing in these signals is double: On one hand it has been previously reported in [5] that EEG signals meet the necessary requirements to ensure reconstruction after compression when projected in certain basis. Hence compressive sensing appears as a very attractive technique to reduce the power consumption and thus the size of future miniaturized EEG systems, which could be used in a variety of applications ranging from long term medical monitoring [6] to brain computer interfaces [7]. On the other hand, advances on brainwave interpretation research could lead to situations in the future in which sensitive personal information, not only of medical nature, could potentially be extracted from them. This would make privacy preservation even more of an important issue in the design of the whole EEG system.

The paper starts with a brief introduction to the compressive sensing theory. Since compressive sensing inherently involves a randomization process its performance is compared to two randomization techniques commonly used in data mining for privacy preservation. These techniques are presented in Section III together with a brief discussion of some of their potential problems. This is followed in Section IV by a description of the metric that will subsequently be used to evaluate performance. Section V presents the quantitative comparison including results for additive and multiplicative randomization (both of them used in data mining although known to be not very strong in terms of privacy preservation); AES encryption (a widely used symmetric block cipher); and compressive sensing. Finally Section VI presents some of the conclusions that can be extracted from this work.

II. Compressive Sensing

The concept of compressive sensing [8] is based on the fact that there is a difference between the rate of change of a

signal and the rate of information in the signal. Traditional Nyquist sampling, putting the signal into the digital domain ready for wireless transmission, is based on the former. The Nyquist theorem states that it is necessary to sample the signal at a rate at least twice the maximum rate of change present. A conventional compression algorithm would then be applied to all of these samples taken to remove any redundancy present, giving a reduced number of bits that represent the signal.

In contrast, compressive sensing exploits the information rate within a particular signal. Redundancy in the signal is removed during the sampling process itself, leading to a lower effective sampling rate. Provided certain conditions are satisfied [9], sampling at a sub-Nyquist rate the signal can still be accurately recovered.

To illustrate this, consider an EEG signal of interest x which is a vector of N digital samples; i.e. x[n] where n =1, 2 … N. Then assume that this signal can be represented by a projection onto a different basis set:

$$x = \sum_{i=1}^{N} s_i \Psi_i \text{ or } \mathbf{x} = \mathbf{\Psi s} \tag{1}$$

where $\mathbf{s}$ is a $N\times1$ basis function vector and $\mathbf{\Psi}$ is a $N\times N$ basis matrix. The matrix $\mathbf{s}$ can be calculated from the inner product of $\mathbf{x}$ and $\mathbf{\Psi}$:

$$s_i = \langle \mathrm{x}, \Psi_i \rangle \tag{2}$$

For example, if $\mathbf{\Psi}$ is the Fourier basis set of complex exponential functions, $\mathbf{s}$ is the Fourier transform of $\mathbf{x}$ and both $\mathbf{s}$ and $\mathbf{x}$ represent the signal equivalently, but in different domains. In compressive sensing $\mathbf{\Psi}$ is chosen so that $\mathbf{s}$ is sparse – a vector is K-sparse if it has K non-zero entries and the remaining $N–K$ entries are all zero. $\mathbf{s}$ is thus a more *compact* representation of the signal than the original $\mathbf{x}$. Similar to this projection, assume that $\mathbf{x}$ can be related to another signal $\mathbf{y}$:

$$\mathbf{y} = \mathbf{\Phi x} \tag{3}$$

where $\mathbf{y}$ is a $M\times1$ vector and $\mathbf{\Phi}$ is a matrix of dimensions $M\times N$ where $M<N$. Thus:

$$\mathbf{y} = \mathbf{\Phi\Psi s} \tag{4}$$

Provided that $\mathbf{\Phi}$ is correctly chosen so that no significant information is lost during the reduction in dimensionality, it is possible to use $\mathbf{\Phi}$ to sample the sparse signal $\mathbf{s}$, rather than the original signal $\mathbf{x}$ to give an output vector $\mathbf{y}$ which has only M entries rather than the original N. If $M<N$ data compression is thus achieved, and the signal $\mathbf{y}$ would be transmitted from the portable EEG unit. It can be shown [9] that this technique is possible if $\mathbf{\Phi}$ and $\mathbf{\Psi}$ are incoherent; that is if the elements of $\mathbf{\Phi}$ and $\mathbf{\Psi}$ have low correlation.

Given a compressed measurement $\mathbf{y}$ at the receiver, the signal $\mathbf{x}$ can be reconstructed by solving the L1 problem:

$$\min_{s \in \Re^N} \|s\|_{l1} \text{ subject to } y_i = \langle \Phi_i, \Psi s \rangle \tag{5}$$

which finds the vector $\mathbf{s}$ with the lowest L1 norm that satisfies the observations made. This is then easily converted back into $\mathbf{x}$. In general, the L1 minimization problem is non-trivial and computationally complex, but there is no need for this to run online in the portable EEG unit. The EEG signal $\mathbf{x}$ will be sampled as signal $\mathbf{y}$, and these samples wirelessly transmitted to a base station which will then regenerate $\mathbf{x}$ from $\mathbf{y}$ offline. The fact that compressive sensing based data compression has all of its computational complexity in the backend, where power and size constraints are not as stringent is a major factor motivating this work.

III. Preserving Privacy through Randomization

In principle, privacy preservation through random perturbation is achieved through modification of data values in a random style after which the original data should remain recoverable at its legitimate destination. Based on this, there are different methods to modify the signal original values. An example could be the value distortion method [10] in which the original data x_i is distorted to:

$$x_i + z \tag{6}$$

where z is an arbitrary function. Similarly, in case of multiplicative distortion, the original data x_i is distorted to:

$$x_i \times z \tag{7}$$

Uniform and Gaussian distributions with mean 0 have been considered for z , out of which the latter has been proven to provide considerably higher privacy at superior confidence levels [10]. Unfortunately, although these methods can help, randomization can also be easily removed using different signal processing techniques such as probabilistic analysis. In [11] it has been shown that random-data distortion preserves little data privacy. Characteristics of random processes can easily be revealed, especially when the original data has some definite trend, which may lead to privacy breach. An advantage of compressive sensing versus these techniques is that the original signal does not only undergo multiplicative matrix based randomization but dimensionality reduction as well. Hence, if compressive sensing is performed appropriately- by, for example, choosing a Gaussian random measurement matrix in the measurement vector- the data will exhibit almost no definite trend.

Visualization of the level of randomization achieved through Compressive Sensing is presented in Fig. 1. These plots demonstrate that once the data is compressively sensed it changes completely, not only in time but frequency domain as well.

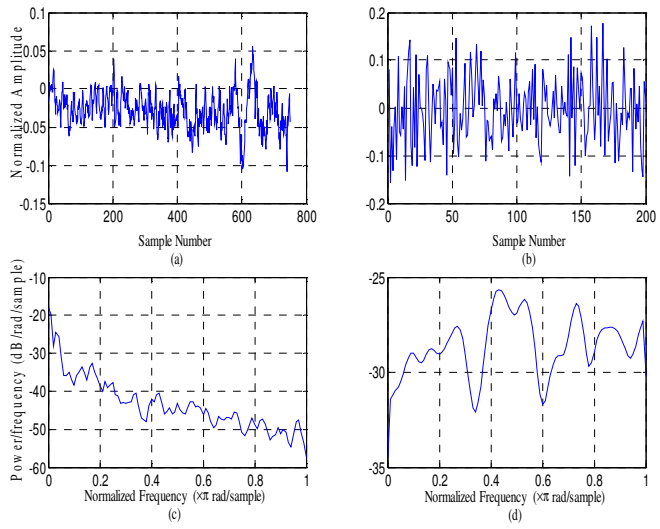

Fig. 1. (a) Original EEG Data (b) Compressively sensed for transmission (c, d) Corresponding Welch Spectrums

IV. Measure of Privacy

Many methods have been proposed in the literature to measure the level of privacy. The one used in this paper was proposed in [12] and is based on Shannon's information theory [13]. The level of privacy is quantified measuring the similarity between the original and the modified signals, through a metric called mutual information, which is analytically defined as:

$$I(A;B) = \sum_{b\epsilon B}\sum_{a\epsilon A} p(a,b)\log\left(\frac{p(a,b)}{p(a)p(b)}\right) \quad (8)$$

where A and B represent the two signals; $p(a,b)$ is their joint probability function; and $p(a), p(b)$ are their respective marginal probability density functions.

Since the mutual information measures common information between A and B, if these two variables were fully independent their joint probability density would be equal to the product of their marginal probability density functions, i.e.

$$p(a,b) = p(a) \times p(b) \quad (9)$$

and

$$\log\left(\frac{p(a,b)}{p(a)p(b)}\right) = \log\left(\frac{p(a)p(b)}{p(a)p(b)}\right) = 0 \quad (10)$$

This would imply that $I(A;B) = 0$ and hence there is nothing in common between A and B. In general, even if zero cannot be achieved the closer the mutual information is to this value, the higher the level of privacy provided by the encryption technique.

V. Analysis and Results

Mutual information was calculated following the methods described in [14], some of which were previously also used on human and animal EEG signals [15, 16]. Three different sets of 21 channel EEG data with 5 minutes per channel were used for comparison. Four different privacy preservation methods were compared: (i) additive randomization, (ii) multiplicative randomization (iii) Advanced Encryption Standard (AES) algorithm [17] and (iv) compressive sensing. For the AES method, the EEG data was formatted, and then encrypted using AES toolbox [18]. Mutual information was then estimated between the formatted unencrypted and encrypted data.

The estimated mutual information for all four cases is shown in Fig. 2. The average of the estimated mutual information over all 21 channels and respective variances have been summarized in Table 1. Since this study was focused on privacy preservation as opposed to signal compression an N×N measurement matrix was used for compressive sensing. Note, that any reduction of dimensionality leading to compression could only lead to an improvement on the results presented here.

Table 1
Comparison of (i) additive, (ii) multiplicative (iii) AES encrypted and (iv) compressive sensing based data randomizations of real EEG data

EEG Channels: C3, C4, Cz, F3, F4, F7, F8, Fp1, Fp2, Fz, O1, O2 , P3, P4, Pg1, Pg2, Pz, T3, T4, T5, T6

Mutual Information (Nats)				
Subject 1				
	Additive	Multiplicative	AES	CS
Average	1.474	0.19	0.008	0.069
Variance	1.278	0.034	0	0.001
Subject 2				
	Additive	Multiplicative	AES	CS
Average	0.937	0.093	0.014	0.08
Variance	0.309	0.007	0	0.001
Subject 3				
	Additive	Multiplicative	AES	CS
Average	1.273	0.141	0.01	0.101
Variance	0.097	0.003	0	0.001

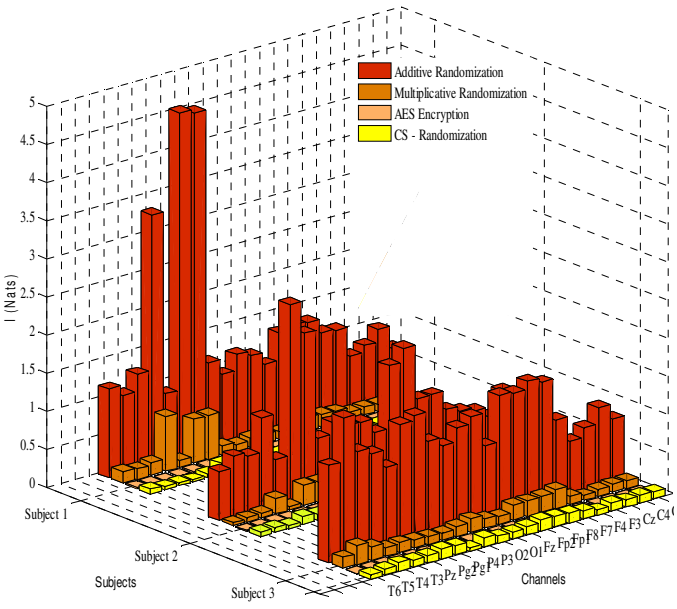

Fig. 2. Level of Privacy Comparison of (i) Additive, (ii) Multiplicative (iii) Measurement Matrix(CS based) Randomizations and (iv) AES Encrypted EEG data

From the results in Table 1 it can be seen that the privacy achieved through compressive sensing based data randomization is significantly closer to AES encryption than to additive and multiplicative randomization. The original and compressively sensed measurement vectors render almost complete statistical independence hence providing high levels of data privacy.

VI. Discussion and Conclusions

In compressive sensing the original data is not only multiplicatively randomized. A dimension reduction is also achieved through setting appropriate dimensions of the random measurement matrix. This inherent multi-dimensional projection perturbation feature makes it harder to breach the privacy as the information related to the level of dimension reduction is not transmitted over the intermediary non-secure transmission link. All these features of compressive sensing not only help in achieving compression, but random encryption while sampling too.

In this work, secrecy properties of compressive sensing for noisy and compressible signals have been explored. Further future analysis could be carried out looking at the levels of privacy achievable in case of jointly sparse signals. Besides, the manner in which compressive sensing is used in a specific application/system is crucial for the level of data security achievable. If the random measurement matrix can be generated more often instead of just using one random measurement matrix the system's privacy could be enhanced. However, this would be at the expense of increased computational costs. An appropriate tradeoff between security and implementation cost should be found taking into account application specific variations to fully exploit the characteristics of compressive sensing. Research in this arena can change the way people perceive compressive sensing today, viz. "Compressing while Sampling" to "Compressing and Securing while sampling".

Acknowledgments

The authors would like to thank the National Society of Epilepsy UK for providing the EEG data. Authors would also like to thank Alexander J. Casson for his positive feedback.

References

[1] Data Protection Act 1998, http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

[2] Department of Health, Confidentiality: NHS Code of Practice, November 2003. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

[3] E. Smith and J.H. Eloff, Security in health-care information systems—current trends, International Journal of Medical Informatics, 54, pp. 39–54, April 1999.

[4] A. M. Abdulghani , A. J. Casson and E. Rodriguez-Villegas, Quantifying the feasibility of compressive sensing in portable electroencephalography systems, in Foundations of Augmented Cognition, Neuroergonomics and Operational Neuroscience, vol. 5638, pp. 319-328, 2009.

[5] S. Aviyente, Compressive sampling framework for EEG compression, IEEE/SP 14th Workshop on Statistical Signal Processing, pp. 181–184, 2007.

[6] E. Waterhouse, New horizons in ambulatory electroencephalography, IEEE Engineering in Medicine and Biology Magazine, vol. 22, no. 3, pp. 74–80, 2003.

[7] G. E. Birch, S. G. Mason and J F Borisoff, Current trends in brain-computer interface research at the Neil squire foundation, IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 11, no. 2, pp. 123-126, 2003.

[8] D. Donoho, Compressive sampling, IEEE Transactions on Information Theory, vol. 52, no. 4, pp. 1289-1306, 2006.

[9] J. Candès, M. Wakin, People hearing without listening: an introduction to compressive sampling, In IEEE Signal Processing Magazine. vol. 25, no. 2, pp. 21-30, 2008.

[10] R. Agrawal and R. Srikant, Privacy-preserving data mining, In Proceedings of the ACM SIGMOD Conference on Management of Data, Dallas, TX, ACM, May 14-19 2000.

[11] H. Kargupta, S. Datta, Q. Wang, K. Sivakumar, Random-data perturbation techniques and privacy-preserving data mining, Knowledge and information systems, vol. 7, no. 4, pp. 387–414, 2005.

[12] D. Agrawal and C. C. Aggarwal, On the design and quantification of privacy preserving data mining algorithms, Proceedings of the 20th Symposium on Principles of Database Systems, Santa Barbara, California, USA, May 2001.

[13] C. E. Shannon. Communication theory of secrecy systems, Bell System Technical Journal, vol. 28 no.4, pp. 656–715, 1949.

[14] R. Moddemeijer, On Estimation of Entropy and Mutual Information of Continuous Distributions, Signal Processing, vol. 16, no. 3, pp. 233-246, 1989.

[15] N. J. I. Mars et al., Propagation of seizure activity in kindled dogs, Electroencephalography and Clinical Neurophysiology, vol. 56, pp. 194-209, 1983.

[16] N. J. I. Mars et al., Spread of epileptic seizure in humans, Epilepsia, vol. 26, pp. 85-94, 1985.

[17] National Institute of Standards and Technology: Specification for the Advanced Encryption Standard (AES), 2001.

[18] J. J. Buchholz, Matlab Implementation of the Advanced Encryption Standard, December 19, 2001. http://buchholz.hs-bremen.de