

A two-class information concealing system based on compressed sensing

Original

A two-class information concealing system based on compressed sensing / Cambareri, Valerio; Haboba, Javier; Pareschi, Fabio; Rovatti, Riccardo; Setti, Gianluca; Wong, Kwok-wo. - STAMPA. - (2013), pp. 1356-1359. (Intervento presentato al convegno IEEE International Symposium on Circuits and Systems tenutosi a Beijing nel May 2013) [10.1109/ISCAS.2013.6572106].

Availability:

This version is available at: 11583/2696817 since: 2021-09-23T23:51:17Z

Publisher:

IEEE

Published

DOI:10.1109/ISCAS.2013.6572106

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

IEEE postprint/Author's Accepted Manuscript

©2013 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

A Two-Class Information Concealing System based on Compressed Sensing

Valerio Cambareri^{*,†}, Javier Haboba[†], Fabio Pareschi^{†,‡}, Riccardo Rovatti^{*,†}, Gianluca Setti^{†,‡}, Kwok-wo Wong[§]

^{*} DEI – University of Bologna, viale Risorgimento 2, Bologna, Italy. {valerio.cambareri, riccardo.rovatti}@unibo.it

[†] ARCES – University of Bologna, via Toffano 2/2, Bologna, Italy. jhaboba@arces.unibo.it

[‡] ENDIF – University of Ferrara, via Saragat 1, Ferrara, Italy. {fabio.pareschi, gianluca.setti}@unife.it

[§] Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong Special Administrative Region, China. itkwwong@cityu.edu.hk

Abstract—We elaborate on the possibility of exploiting the (pseudo)random projection operator, which is at the heart of the most common architecture for compressed sensing, to prevent access to the acquired information by unauthorized receivers. In low-resource applications, this approach may make dedicated cryptographic layers unnecessary when the security requirement is not particularly high. Beyond proving that the proposed system is at least asymptotically immune to straightforward statistical attacks, we also exploit the sensitivity of compressed sensing recovery algorithms to the complete knowledge of the projection matrix to introduce two-class protection. The encoding is such that first-class decoders can retrieve the signal to its full resolution while second-class decoders are able to retrieve only a degraded version of the same signal. Examples are given with reference to ECG signal acquisition.

I. INTRODUCTION

Multi-class information broadcasting policies are found in many technologies such as navigation systems, digital video broadcasting of restricted access content and software radio. In these applications the ability to distinguish between user classes is an advisable feature. As an example, in the Global Positioning System (GPS) two different user classes share the same physical layer infrastructure: the Precise Positioning Service [1] transmits high precision data restricted for military use, while Standard Positioning [2] is open for civilian use but operates with significantly lower accuracy.

The key to differentiating information content between multiple user classes commonly entails the use of pseudorandom number generators (PRNG) as the base of more advanced cryptographic algorithms. In these terms, low-cost concealing of analog signal sources may take advantage of Analog-to-Information (A2I) conversion by Compressed Sensing (CS), which is based on generating projections of the analog signal along (pseudo)random directions [3].

Compressed Sensing [4, 5] is a signal processing paradigm that has recently gained interest due to the possibility of acquiring a signal from significantly less measurements than its Nyquist rate samples. The main prior condition to efficiently perform CS of a signal is that it has a *sparse* representation, i.e., it may be expressed as a linear combination of some known basis waveforms with very few nonzero/non-negligible coefficients. It is the number of nonzero coefficients rather than the apparent dimensionality of the signal that controls the number of measurements required to encode it and perform reconstruction at the decoder side [6, 7].

The intrinsic exploitation of randomness in A2I converters makes them appealing for simultaneous information acquisition, compression, and concealing directly at the physical interface between the analog and the digital world.

In this paper we propose a CS system based on the parallel Random Modulation Pre-Integration (RMPI) converter [3] that is able to distinguish first-class and second-class decoders; the former completely know the pseudorandom vectors used in the encoding and are capable of reconstructing the signal at maximum resolution (minimum reconstruction noise); the latter know a version of the same vectors altered by a random perturbation whose magnitude controls the amount of non-recoverable information at the decoder.

From a cryptographic perspective, the analog input signal is the *plaintext*, the measurements are the *ciphertext* and the pseudorandom encoding is the *encryption algorithm*, of which the initial state is the *private key*. This paper does not aim to prove whether CS is a cryptographically secure algorithm or not; it rather shows an information concealing system which makes signal recovery from ciphertext computationally hard, and recovery relying on incomplete knowledge of the key affected by an arbitrarily high amount of noise.

As a proof of concept, this two-class scheme is applied to electrocardiographic signals (ECGs): the first-class receiver is designed to decode the complete signal profile and reproduce all its features with low reconstruction noise, while the second-class receiver is able to observe only basic features such as the heart rate, but cannot detect sensitive information such as cardiac cycle anomalies due to a pathologic condition.

II. TWO-CLASS CONCEALING BY COMPRESSED SENSING

Let $x \in \mathbb{R}^n$ be a signal in an n -dimensional vector space; we say x is k -sparse w.r.t. a basis $\Psi_{n \times n}$ (or a dictionary $\Psi_{n \times p}$, $p \geq n$) if $x = \Psi\alpha$, where $\alpha \in \mathbb{R}^n$ has $k \ll n$ nonzero coefficients. CS essentially states that if x is k -sparse, then it can be recovered from only $m < n$ linear projections, where m depends on the sparsity k and the dimensionality n [5]. In particular, if $\Phi_{m \times n}$ is a matrix with independent and identically distributed (i.i.d.) entries belonging to a wide class of possible random variables, the needed measurements can be found in the vector $y = \Phi x = \Phi \Psi \alpha$.

When x is a window of n Nyquist rate samples of an analog signal $x(t)$ which is known to be sparse in a basis Ψ , there are a number of architectures that implement CS of $x(t)$, among

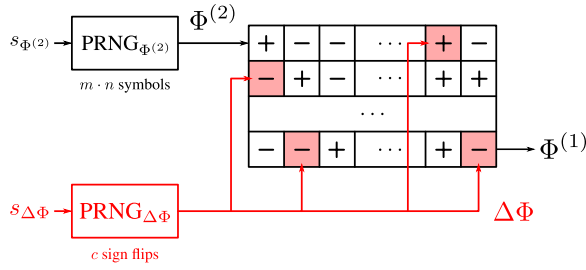


Fig. 1. Measurement matrix generator architecture

which the most straightforward is the RMPI converter [3]. In order to recover x from y under the prior that x is k -sparse, one may solve the well-known $\min \ell_1$ optimization problem (see [4]): $\min \sum_{j=0}^{n-1} |\alpha_j|$ s. t. $y = \Theta\alpha$, where $\Theta = \Phi\Psi$. This is a linear programming (LP) problem that can be solved very efficiently by standard means.

From a more architectural point of view, the RMPI encoder is an array of m analog inner products between the signal $x(t)$ and the rows of Φ ; the decoder is a standard LP solver which takes the matrix Θ and the encoded message y as inputs and, if the m projections have raked enough information from the input signal, it outputs the sparsest approximation $\hat{\alpha}$ to α .

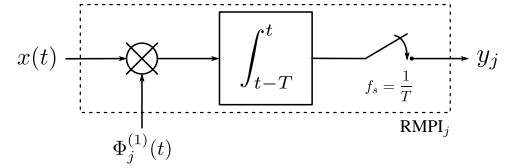
To understand how effective two-class information concealing can be embedded in such a system note that the encoder and the decoder must agree on an initial state of the PRNG generating Φ (it is known that Φ can be as simple as a collection of antipodal pseudorandom symbols) so that any decoder who knows the seed knows Φ . On the contrary, a decoder ignoring Φ will not be solving the same instance of the LP problem, and reconstruction errors will be unavoidable. We exploit this encoder/decoder agreement to conceal information by introducing a controlled mismatch in the matrix Φ for lower-class receivers.

The two-class system works as follows. We encode x with a measurement matrix generated by combining two random sources, one being an i.i.d. stream of $m \cdot n$ antipodal symbols, the other being a pseudorandom set C of positions in the symbol buffer, of cardinality $|C| = c \ll m \cdot n$. First the symbol buffer is filled by the pseudorandom stream generating the matrix $\Phi^{(2)}$. Then, the symbols at the positions contained in C are flipped by changing their sign. The altered buffer is then used to obtain the matrix $\Phi^{(1)}$ that can be expressed as $\Phi^{(1)} = \Phi^{(2)} + \Delta\Phi$, where $\Delta\Phi$ is the *perturbation matrix* of elements

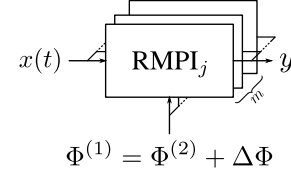
$$\Delta\Phi_{j,k} = \begin{cases} -2\Phi_{j,k}^{(2)}, & (j,k) \in C \\ 0, & (j,k) \notin C \end{cases}$$

chosen uniformly at random. A thorough analysis of perturbations in CS can be found in [8]. For our purposes, it is enough to say that if the entailed PRNGs are a good approximation of i.i.d. symbol sources, the two matrices $\Phi^{(1)}$ and $\Phi^{(2)}$ are statistically indistinguishable and satisfy the classical assumptions [5] ensuring recovery of the original signal from the measurements they produce.

The seeds of the PRNGs generating $\Phi^{(2)}$ and $\Delta\Phi$ define the *first-class* user key $K_1 = (s_{\Phi^{(2)}}, s_{\Delta\Phi})$, while the *second-class* key is $K_2 = (s_{\Phi^{(2)}})$. The complete matrix generator is



(a) j th RMPI channel



(b) Two-Class Encoder

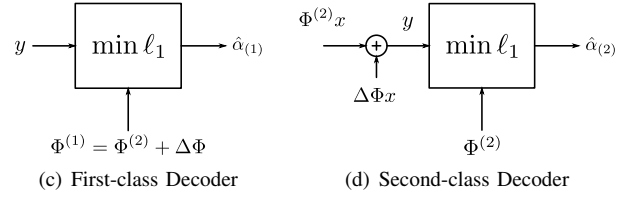


Fig. 2. Two-class Encoder/Decoder Architecture

depicted in Fig. 1 and must be present at both the encoder and the first-class decoder side; since second-class users only know $s_{\Phi^{(2)}}$, the lower PRNG is missing in second-class decoders.

The CS encoder is depicted in Fig. 2(b); it transmits the compressed measurements y encoded with $\Phi^{(1)}$. The acquisition is performed by m parallel RMPI channels, whose j th instance (see Fig. 2(a)) modulates $x(t)$ by the waveform $\Phi_j^{(1)}(t)$ (the j th row of $\Phi^{(1)}$). The first-class decoder, depicted in Fig. 2(c), receives the measurements y and, since it knows K_1 , it solves the $\min \ell_1$ problem given the constraint $y = \Phi^{(1)}x$; if there are no other noise sources and the m measurements carry sufficient information, the reconstruction $\hat{\alpha}$ will be exact, yielding $\hat{x} = \Psi\hat{\alpha}$ with low or no reconstruction noise w.r.t. x . The second-class decoder (in Fig. 2(d)) receives $y = (\Phi^{(2)} + \Delta\Phi)x = \Phi^{(2)}x + \nu_{\Delta\Phi}$, where $\nu_{\Delta\Phi} = \Delta\Phi x$ is equivalent to additive colored noise since $\Delta\Phi$ is unknown to this decoder. From [7] we know that in presence of additive noise the reconstruction error cannot be bounded but proportionally to $\|\nu_{\Delta\Phi}\|_2^2$ so the second-class receiver will be, in general, affected by a higher reconstruction noise.

The energy $\|\nu_{\Delta\Phi}\|_2^2$ of $\nu_{\Delta\Phi}$ is controlled by the number c of flipped positions in $\Phi^{(1)}$ w.r.t. $\Phi^{(2)}$. Hence, increasing c is expected to raise the average reconstruction noise of the second-class receiver. We have to choose c such that the noise threshold for second-class users in the selected application agrees with the specifications.

We cannot prevent the second class receiver from improving its reconstruction quality by denoising. According to experimental results, simple attacks such as trivial noise filtering do not improve the reconstruction quality; however, more complex attacks based on signal priors may have some effect at the expense of much higher computational effort.

Eavesdroppers, i.e., malicious receivers trying to decode the concealed signal, do not know any of the two seeds and are

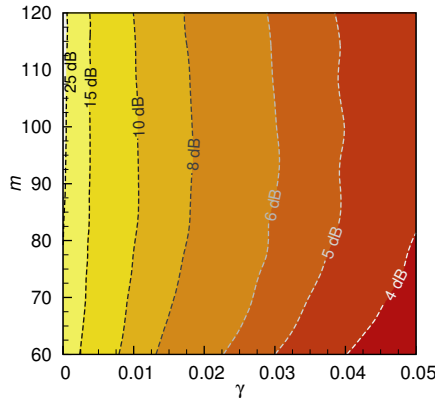


Fig. 3. Design space for the proposed two-class ECG compressed sensing system when the input signal has an intrinsic SNR of 30 dB. The contour plot shows the ARSNR_{dB} performance after min ℓ_1 decoding when we vary the number of measurements m and the ratio of corrupted entries γ .

therefore unable to obtain the projection matrix and use it for signal recovery. A few contributions exist (e.g., [9]) trying to clarify the strength of this protection and some novel insight on this is given in the final part of this paper. By now we exemplify the two-class concealing scheme by addressing a sample application.

III. APPLICATION TO HEART PATIENT MONITORING

In our sample application the ECG trace of a heart patient is acquired by RMPI-A2I and must be transmitted to monitoring devices ensuring privacy. Low-level monitoring (second-class receivers) is only interested in heartbeat measurement but must not have access to detailed data. High-level monitoring (first-class receivers) must have access to a full resolution heartbeat trace for possible medical diagnosis.

The interpretation of ECGs is out of the scope of this paper. It suffices to say that relevant informations are associated to the position of the five peaks usually indicated with the letters P, Q, R, S and T [10].

In this case, the idea is that first-class users must be able to appreciate the exact position and shape of all peaks, while second-class receivers are able to reconstruct only a perturbed version of the trace in which all the peaks but the highest one can be precisely identified.

Starting from the dictionary Ψ used in [11] and from synthetic ECGs generated as in [12] with an additional Gaussian noise at -30 dB, we may compute the performance contour plot in Figure 3; in that plot, the average reconstruction SNR, $\text{ARSNR}_{\text{dB}} = 20 \log_{10} \mathbf{E}_x [\|x\|_2 / \|\hat{x} - x\|_2]$ is reported as a function of the number of measurements m and the relative perturbation magnitude $\gamma = c/(m \cdot n)$ for $n = 250$. The reconstruction is performed over 250 synthetic ECG instances per (γ, m) pair by linear programming using ILOG CPLEX.

Clean ECGs require an ARSNR of at least 20 dB. From Figure 3, this is ensured by setting $m = 80$ and $\gamma = 0$. To corrupt information about the lower peaks $\{P, Q, S, T\}$, we will allow second-class receivers to reconstruct the same ECGs with an ARSNR not higher than 6 dB. For $m = 80$, this is achieved with $\gamma = 0.03$.

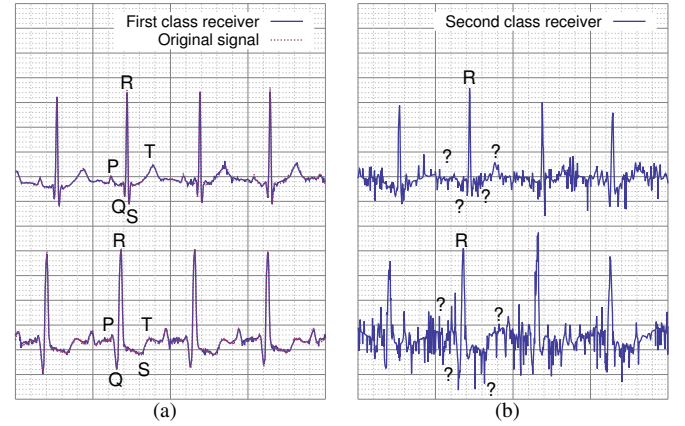


Fig. 4. (a) First-class receiver signal reconstruction compared with the original signal. The position of the PQRST peaks is clearly identifiable and the healthy ECG (top) can easily be distinguished from the pathological one (bottom). (b) Second-class receiver signal reconstruction, where only the R peaks are identifiable; the healthy (top) and pathological (bottom) ECGs cannot be distinguished.

A sample performance of a system designed with the above parameters is depicted in Figure 4, where two ECG traces coming from public databases [13] have been considered. In Figure 4(a) we depict two signals decoded by the first-class receiver, one from a healthy patient (top) and the other from a patient affected by cardiac insufficiency (bottom), compared with the original signal. The position of the peaks is well identifiable both in the healthy case (SNR = 19.6 dB) and the pathological case (SNR = 23.6 dB) reconstructions, and the two traces are clearly distinguishable from each other.

In the signal available to second-class receivers (Figure 4(b)) information on the peak position except for the QRS complex is severely corrupted by reconstruction noise, making distinction between healthy and ill patients virtually impossible. In this case, the healthy patient trace is reconstructed with SNR = 5.0 dB, the pathological case with SNR = 6.3 dB.

IV. SHANNON SECURITY AND COMPRESSED SENSING

The aim of this section is to give a hint on the security of the proposed system. Despite the fact that it is designed to work in simple and low-cost applications, a certain amount of security is nevertheless ensured. An extensive analysis of possible attacks leveraging on some kind of side information is possible but incompatible with the scope of this communication. For this reason we here concentrate on the most basic requirement of security.

According to Shannon's definition, a prerequisite of all secure systems is that the statistical properties of the ciphertext (the measurements) must be independent of the plaintext (the signal to acquire) [14], i.e. any statistical analysis of the encrypted message alone gives no information on the original message.

Previous works have studied secrecy in compressed sensing [9] and immediately clarified that the Shannon prerequisite cannot be fulfilled in general due to the linearity of the projection operator used to obtain the measurements. In particular, we will see that linearity makes eavesdroppers able to detect

energy-related information. Yet, we are also able to prove that, at least asymptotically, such information is the only percolating through our encoding.

More formally, let us consider a sequence of systems with increasing n in which the projection matrices $\Phi_{m \times n}$ are made of i.i.d. entries with zero mean, variance $\sigma_n^2 = 1/n$ and bounded absolute third-order moment $\mu_n^3 \leq M$ for some $M > 0$ (for example i.i.d. antipodal symbols $\pm 1/\sqrt{n}$). These systems acquire a bounded signal x with $|x_l| \leq X$ and finite power $W = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{l=0}^{n-1} x_l^2 < \infty$.

The j th measurement is $y_j = \sum_{l=0}^{n-1} \phi_{j,l} x_l = \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} z_{j,l}$ with $z_{j,l} = \sqrt{n} \phi_{j,l} x_l$. Regardless of j , the sequence $z_{j,l}$ is made of independent random variables with zero mean and such that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{l=0}^{n-1} \mathbf{E}[z_{j,l}^2] = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{l=0}^{n-1} x_l^2 = W$$

and

$$0 \leq \lim_{n \rightarrow \infty} \frac{1}{n^{3/2}} \sum_{l=0}^{n-1} \mathbf{E}[|z_{j,l}|^3] \leq \lim_{n \rightarrow \infty} \frac{1}{n^{3/2}} \sum_{l=0}^{n-1} M X^3 = 0$$

Hence, by the Central Limit Theorem, every y_j asymptotically distributes as a zero-mean Gaussian with variance equal to the power W of the signal to acquire.

Yet, in the same asymptotic conditions, any two signals with the same power will be statistically indistinguishable given the measurements, thus ensuring Shannon security whenever power information is not substantial, e.g., when all the realizations to acquire at a given time window have (or can be made to have) approximately the same energy.

To numerically illustrate this property, we consider the two ECG traces from which the windows in Fig. 4(a) were taken and extract $n = 50, 100, 150, \dots, 2500$ samples from each of them. For each n , the two sample collections are normalized to unit energy and projected along 10^8 i.i.d. antipodal vectors. To model what would happen in a real implementation, measurements are quantized in 8-bit words ($B = 2^8$ bins). Quantization levels are optimized assuming a Gaussian distribution to have a maximum-entropy digital encoding. This provides us with $N = 10^8$ samples from the distributions of the digital words y', y'' encoding two different ECG signals x', x'' . These samples are used to estimate the Kullback-Leibler divergence $D(y' || y'')$ [15] that is plotted in Figure 5 against the value of n .

As a reference, we also report the theoretical expected value of the divergence estimated using two sets of N samples coming from the same discrete uniform distribution, i.e., $\beta = (B - 1)/(N \ln 2) \simeq 3.67 \times 10^{-6}$ bit.

It is clear that the measurements of the two signals become statistically indistinguishable for n above few hundreds, since the number of bits of information that can be apparently inferred from their differences ($\leq 10^{-5}$ bit for $n > 500$) is mainly due to estimation uncertainties and cannot support straightforward statistical attacks.

V. CONCLUSION

We have proposed a compressed sensing system that selectively hides information content by introducing a controlled

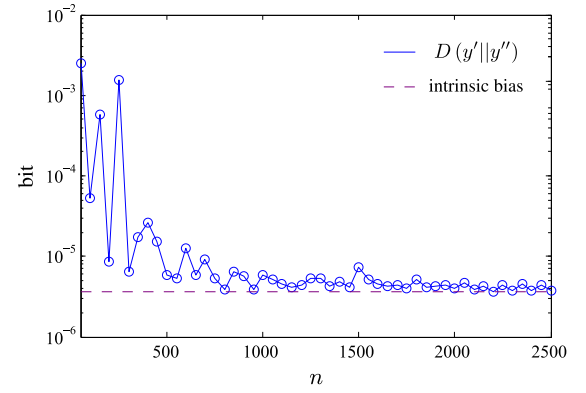


Fig. 5. Estimated Kullback-Leibler divergence between the probability distributions of two 8-bit measurements corresponding to different original signals.

amount of perturbations in the measurement matrix. This system may find application whenever one wants to perform simultaneous sensing, compression and information concealing directly in the analog domain, before the signal is digitized. The system was shown to be asymptotically secure in the Shannon sense except for the signal power.

REFERENCES

- [1] U.S. Department of Defense, "GPS Precision Positioning Service (PPS) Performance Standard," 2007, Available at <http://www.gps.gov/technical/ps/>.
- [2] —, "GPS Standard Positioning Service (SPS) Performance Standard," 2008, Available at <http://www.gps.gov/technical/ps/>.
- [3] J. N. Laska, S. Kirolos, M. F. Duarte, T. S. Ragheb, R. G. Baraniuk, and Y. Massoud, "Theory and Implementation of an Analog-to-Information Converter using Random Demodulation," in *Proceedings of 2007 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2007, pp. 1959–1962.
- [4] D. L. Donoho, "Compressed Sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
- [5] E. J. Candes and M. B. Wakin, "An Introduction to Compressive Sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, Mar. 2008.
- [6] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.
- [7] E. J. Candes, J. K. Romberg, K. Justin, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics*, vol. 59, no. 8, pp. 1207–1223, Aug. 2006.
- [8] M. Herman and T. Strohmer, "General deviants: An analysis of perturbations in compressed sensing," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 342–349, 2010.
- [9] Y. Rachlin and D. Baron, "The Secrecy of Compressed Sensing Measurements," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Sep. 2008, pp. 813–817.
- [10] D. Dubin, *Rapid Interpretation of EKG's*, 6th ed. Cover Pub. Co, Oct. 2000.
- [11] M. Mangia, R. Rovatti, and G. Setti, "Rakeness in the Design of Analog-to-Information Conversion of Sparse and Localized Signals," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 5, pp. 1001–1014, May 2012.
- [12] P. McSharry, G. Clifford, L. Tarassenko, and L. Smith, "A dynamical model for generating synthetic electrocardiogram signals," *IEEE Transactions on Biomedical Engineering*, vol. 50, no. 3, pp. 289–294, 2003.
- [13] A.L. Goldberger *et al.*, "Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. 215–220, 2000.
- [14] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
- [15] S. Kullback, *Information theory and statistics*. Dover publications, 1997.