Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols

Alejandro Calleja, Pedro Peris-Lopez, Juan E. Tapiador

▶ **To cite this version:**

Alejandro Calleja, Pedro Peris-Lopez, Juan E. Tapiador. Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols. 9th Workshop on Information Security Theory and Practice (WISTP), Aug 2015, Heraklion, Crete, Greece. pp.36-51, 10.1007/978-3-319-24018-3_3 . hal-01442552

HAL Id: hal-01442552
https://inria.hal.science/hal-01442552

Submitted on 20 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-based Protocols

Alejandro Calleja[1] , Pedro Peris-Lopez[1] and Juan E. Tapiador[1]

Universidad Carlos III de Madrid, Avenida de la Universidad 30,
28911, Leganes, Madrid, Spain

Abstract. Inter-Pulse Intervals (IPIs) have been proposed as a source of entropy for key generation and establishment algorithms in Implantable Medical Devices (IMDs) and Body Area Networks (BANs). Most of the proposed protocols built on top of this biometric feature assume that reliable measures of the IPIs are only available to devices maintaining physical contact with the user. However, computer vision techniques have proved to be able to obtain estimates of heart timings from a video recording of the user's face. In this paper, we study the impact of these techniques on IPI-based authentication protocols, comparing a heart signal captured using a traditional contact-based approach against a signal retrieved using such a contactless technique. One key finding is that quantization is a crucial step in the process and we report our empirical assessment of the main approaches proposed so far. Our results show that up to 70% of the information obtained by means of the contact-based method can be also obtained through contactless techniques.

Keywords: Implantable Medical Devices, Inter-Pulse Intervals, IMD Security, Security Protocols

1 Introduction

Implantable Medical Devices (IMDs) allow physicians to treat medical conditions such as heart or neurodegenerative diseases. Similar kind of devices are increasingly being used in Wireless Body Area Networks (WBANs), in which wireless sensors deployed over the patient are able to monitor her physical status. The current trend in the design of this sort of devices is making totally unnecessary the intervention of patients, thus facilitating the remote operation by the physician with the aim of programming them or performing diagnostic tasks. As this family of devices evolves and becomes more sophisticated, new challenges arise concerning their security and more efficient protection mechanisms are demanded [1]. For instance, the inclusion of wireless radio communication capabilities in IMDs has given rise to several concerns regarding the privacy and integrity of information exchanged between the physician and the device.

As the patient's privacy and physical safety are the main assets involved, security plays a vital role for these new technologies. Several authors have shown

the potential risks derived from deploying security-lacking protocols in these scenarios, including the modification of the implant's operational parameters or the leakage of the patient's private information [2–4]. It is also worth mentioning that IMDs suffer from important limitations regarding their computational capabilities and energy consumption, which so far has hindered the use of strong and well-known security protocols, for example those based on public-key cryptography algorithms [1]. This has motivated experts to seek more lightweight alternatives in the field of biometry. Specifically, one of the most promising approaches so far relies on the use of the Inter-Pulse Intervals (IPIs) obtained from the patient's heart signals via electrocardiography (ECG) or photoplethysmography (PPG). The use of this information comes supported mainly by the high degree of entropy contained in IPIs [5–8] and by the simplicity and consistency in the measuring process, which allows the retrieval of nearly the same values in different body parts. Overall, this fact makes such signals very resilient against noise.

All the proposed protocols built on top of this feature assume that IPIs cannot be retrieved if there is no physical contact between the patient and a measuring device (i.e., a set of electrodes). This peculiarity has been proposed as an additional security warranty, since if a potential attacker is not touching the patient, she will be unable of authenticating herself against the implanted device or the WBAN and, therefore, unable to inject fraudulent information or modifying the applied therapies. Nevertheless, driven by the rise of telemedicine, new techniques with the ability to retrieve heart signals such as ECG or PPG without establishing physical contact with patients have emerged [9, 10]. These techniques are roughly based on the amount of light reflected by the human skin when the blood flows through capillaries located near the skin surface. The variations in the reflected light are totally imperceptible to the human eye, but could be enhanced and magnified using video processing and computer vision techniques [10]. Despite the fact that these techniques could threaten the need of physical contact assumed in IPI-based protocols, to the best of our knowledge their potential impact has not been yet explored.

In this paper, we study how contactless techniques developed to retrieve heart signals that can be used as the basis for security protection mechanisms on-board of IMDs. To do so, we present a comparison of heart signals obtained by means of a contact-based and a contactless method. Our approach uses commodity hardware to show that, following a process akin to those presented in related works, it is possible to extract nearly equal IPIs using both methods. Particularly, our final results show that up to 70% of the information contained in the signal obtained through the contact method can be extracted from the signal retrieved using the contactless technique.

The rest of this paper is structured as follows. In Section 2 an overview of cardiac signals and feature extraction is introduced. Section 3 presents our proposal, attending to important aspects such as signal retrieval, preprocessing, and feature extraction. The experimental setting and our results are presented in Section 4. In Section 5, we discuss the applicability of our approach and the

potential impact to the IPI-based protocols proposed so far. Finally, in Section 5 we present our conclusions and future research lines.

2 Background

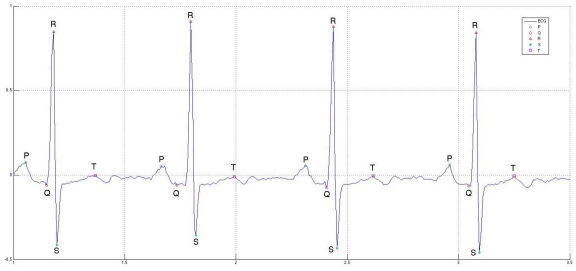
During the past few years, several biometric features have been proposed to be used in human identification and other security-related scenarios. For instance, biometric traits like fingerprints, the voice pitch, or iris pigmentation have been successfully used as verification or identification mechanism [11–13]. The rise of mobile health services and telemedice have forced the experts to seek new biometric features that could be measured in a more continuous and ubiquitous way, i.e., without requiring the interruption of the patient's activity. Furthermore, as many kinds of WBANs and IMDs exist, it is desirable for a candidate biometric trait to be accessible in almost every part of the body. Nowadays, the most promising features are those related to the heart activity, particularly those related to the Heart Variability (HV), i.e., the variation in the time intervals between heartbeats, which can be measured by the analysis of different cardiac biosignals such as the ECG or the PPG.

The ECG signal describes the variations in the electrical activity of the heart within a time interval. An ECG graph can be used to obtain a clear representation of the HV through the analysis of the QRS complex, a set of waves representing the fluctuations of electrical potential due to depolarization of heart muscles during a heartbeat. As depicted in Figure 1(a), the QRS complex is composed by the superposition of several waves (Q, R, and S) with different amplitudes and duration. The ECG signal can be retrieved by using a set of sensors or electrodes attached to different body parts and connected to a measuring device that interprets and stores the collected data. Nowadays it is possible to find small and wearable versions of these devices, resulting in a measuring process that does not interfere with the normal activity of the patient [14].

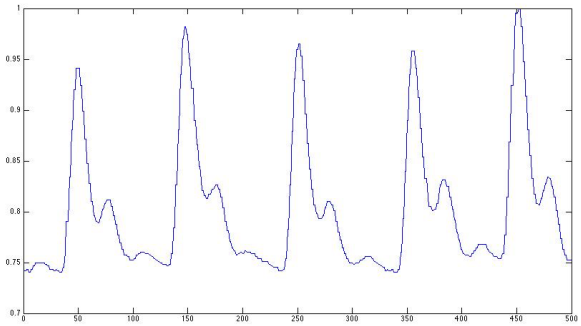
On the other hand, the photoplethysmogram (PPG) signal, also known as pulse signal, describes the variation in the amount of blood flowing in a certain body area during a time interval. Like the ECG signal, a PPG signal can be retrieved using a sensor attached to some body parts such as a finger, an earlobe, or the forehead. The PPG is obtained by illuminating the skin with a light pulse and measuring the amount of reflected or absorbed light, which varies depending on the volume of blood that flows in a given instant. These variations can be represented in a graph such as the one depicted in Figure 1(b). As it can be seen, the PPG also contains local maxima similar to those that can be observed in the ECG graph. This means that the same heartbeat (i.e., the R peak) can be detected in both signals.

2.1 The Inter-pulse Interval Feature

Depending on the purpose of the biometric system, one-to-one or one-to-many comparisons are performed for verification and identification, respectively. In



(a) ECG



(b) PPG

Fig. 1. Example of ECG and PPG signals.

these comparisons, it is unusual to compare all the raw-biometric material, but rather a set of features extracted from it. For instance, when using fingerprints, it is possible to extract many features such as the fingerprint size, its shape, or the distance between ridges. Instead of using the whole set of features, only a subset is commonly employed. This is done because using all extracted features could affect the protocol performance, for instance by increasing the probability of false positives or negatives. Therefore, the common approach is to choose a representative set of features and build a robust protocol on top of them.

In the case of the cardiac signals, several authors have shown the existence of certain features that can be used for security purposes due to their randomness [5–7]. This is the case of the Inter-Pulse Intervals (IPIs). An IPI is the temporal distance between two heartbeats (i.e., the inverse of the heart rate). Thus, given a cardiac signal, an IPI can be extracted by just measuring the temporal distance between two R peaks, which are correlated with the heartbeats. As said before, a heartbeat is detectable in both the ECG and the PPG signal, so the IPI feature can be extracted from these two signals.

Since the R wave is the most prominent in the QRS complex, its detection is easier than in the case of other signal features. This greatly simplifies the measuring process, given the fact that it relaxes the need of having a large set

of sensors attached in order to obtain a reliable dataset. In practical terms, just one or three electrodes would suffice for the acquisition of the PPG and ECG signals, respectively.

2.2 Digitalization

In order to use the retrieved IPI, it must be digitally represented using an encoding process. Digitalization is approached in previous works by means of a quantization algorithm. The use of one quantizer or another will affect the overall system performance. Quantization consists in mapping the image set of an analog and continuous signal (representing, for example, a voltage signal) into a small set of discrete values. Combining this process with a subsequent binary codification, it is possible to obtain a digital representation of an analog signal. It is important to note that the quantization process introduces a noise component due to the rounding errors between the real values and the approximated discrete values. The amount of noise varies depending on several parameters such as the quantization step (i.e., the distance between the discrete values the real values are mapped to) or the quantization algorithm employed.

Choosing a particular quantization algorithm and its parameters is a crucial step in the development of IPI-based protocols, as this will affect the amount and the quality of the obtained digital representation. Surprisingly, despite this fact, only a few of the publications in this field explain in detail the particular quantization process used. Furthermore, even those works that facilitate details about the process usually only provide details about the precision used in the encoding process, i.e., the number of bits used to encode the quantized values. In Section 3.3, the quantification alternatives included in our study are described in detail.

3 Biosignal retrieval: physical contact vs contactless

The high levels of entropy that can be found in the IPIs of cardiac signals make it a very attractive feature to be used in the generation of shared keys between an IMD and a programmer device. Besides, as the extraction of IPIs requires physical contact, it prevents that this information could be retrieved by a third party without the implant owner noticing it. However, this last assumption has been overridden by contactless biosignal retrieval techniques such as the one mentioned above. Thus, if it is possible to achieve a similar signal resolution using contactless techniques as that achieved with contact-based ones, this would mean that an attacker might try to defeat the security of IPI- based protocols without needing physical contact with the user.

With the aim of exploring the impact of this threat, we carried out an effective comparison between two heart signals retrieved by both methods. The first will be retrieved by a traditional contact-based technique. Specifically, we use a pulse sensor similar to the ones used in medical environments to obtain a PPG signal. The second signal will be recorded using a contactless method. In our case,

we will use a heart rate monitor software based on real time video analysis to estimate heart variability. This signal will be compared against the first one, which will be considered as a control signal, extracting the same features and measuring their similarity.

To extract the features from the signals, we followed a procedure similar to the one proposed by previous works on IPI-based protocols. First, we identify the R peaks in both signals with the aim of detecting when a heartbeat happens. The number of heartbeats identified on each signal will be used as a preliminary metric of similarity. After this, we calculate the IPIs on both signals and apply a quantization algorithm in order to get their binary representations. After that, we use traditional techniques such as Hamming distance and entropy analysis to measure the similarity between both signals at low level.

Our final goal is to measure the impact of contactless biosignal retrieval techniques on security solutions for IMDs. To do so, we have followed a similar approaches to the one described for the paring stages of protocols such as IMD-Guard [15] or H2H [8]. The following sections present a more detailed description of the experimental process and the obtained results.

3.1 Signal Acquisition

The signal retrieval process has been carried out by using commodity hardware and software. In order to capture the control signal, we have used a DIY pulse sensor[1] attached to an `Arduino` microcontroller [2], which acts as interface between the sensor and the computer used for storing the signal. The sensor is supposed to be placed in an area where the blood flow could be easily measured, such as a fingertip or an earlobe. The microcontroller was loaded with a program that reads every 50 ms the analog input to which the sensor is connected and sends it to the computer through its serial interface. The sensor circuitry roughly consists of a LED that emits a light pulse and a light-dependent resistor that changes its value depending on the amount of light that it receives from the environment. As explained above, the amount of light reflected by the skin changes when a heartbeat happens. In this way, it is possible to get an approximation of the blood flow and the HV. The computer to which the microcontroller is connected runs a simple process that periodically reads the serial port and saves the read data.

On the other hand, the contactless signal has been taken using the built-in webcam of an Apple MacbookPro laptop. The camera is used as a real-time video source for an open-source pulse monitor software that is able to approximate the patient's PPG signal. This software locates the forehead of the subject using the `OpenCV`[3] computer vision library and performs spectral power analysis to approximate the heart rate and its corresponding PPG signal. In our setup, the subject is located in front of the camera, at a distance of around 50 cm from the

[1] http://pulsesensor.myshopify.com/
[2] http://www.arduino.cc/
[3] http://opencv.org/

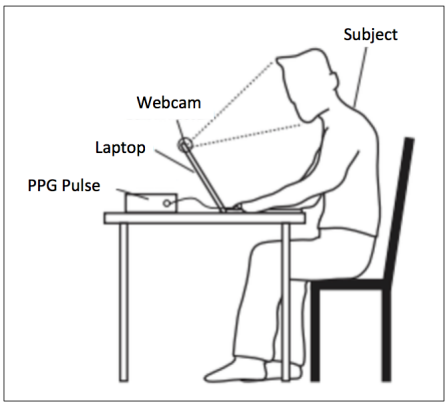


Fig. 2. Experimental Setup

laptop. The recorded video resolution is 640x480 pixels at a frame rate of 30 fps and the color scheme used is RGB with 8 bits per channel. This software has been slightly modified for the purpose of our experimentation.

3.2 Preprocessing

The experimental setup described before, sketched in Figure 2, has been used for retrieving 13 pairs of samples from subjects of ages between 20 and 40 years old with no known heart condition and Caucasian skin tone. All signals have a length of 60 seconds. The frequency of the sensor signal is 100 Hz while the frequency of the webcam signal is 14.7 Hz.

Once the two raw signals were gathered, a preprocessing stage is needed prior to the detection of the R-peaks. As a first step, both signals were resampled to the same frequency. In this case, we decided to resample the signal sampled at the highest frequency (the sensor signal) to the lowest one in order to reach the same temporal resolution in both of them. Following this approach, the sensor signal has been resampled to 14.7 Hz. The next step was to apply a filtering strategy to reduce in both signals the noise components introduced during the measuring process. A low-pass filter with a 3 Hz threshold frequency was applied in order to remove higher frequencies. This parameter has been tuned according to the highest heart rate considered, which is 180 heartbeats per minute. After filtering, the next step is to identify the R-peaks in both signals for further digitalization and comparison. Figure 3 depicts the result of applying the filtering process, where the red dots represent the heartbeats detected on each graph—webcam on top and PPG sensor at the bottom.

As it can be seen in Fig. 3, in the case of the PPG sensor all the R-peaks corresponding a heartbeat have been detected. However, in the webcam case it is easy to observe the presence of false peaks (red dots located very close each other) or real peaks not marked with a red dot (the distance between two

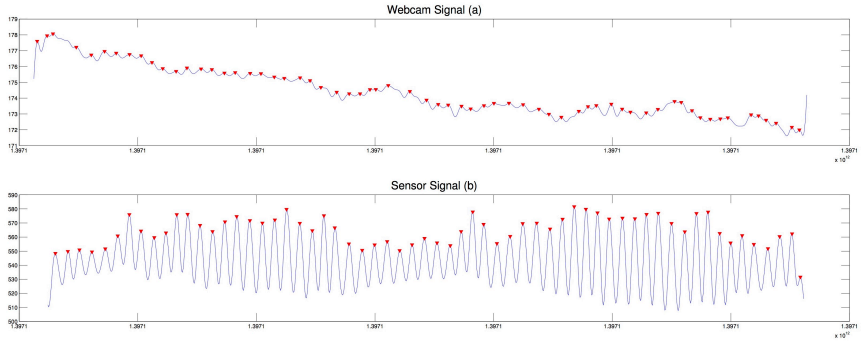


Fig. 3. Processed signals with marked peaks

Table 1. R-peaks (beats) detected on each sample.

Sample	Beats Webcam Signal	Beats Sensor Signal	Error
sample 1	62	64	2
sample 2	68	71	3
sample 3	59	59	0
sample 4	63	60	3
sample 5	60	62	2
sample 6	60	59	1
sample 7	66	65	1
sample 8	69	69	0
sample 9	62	60	2
sample 10	85	81	4
sample 11	61	65	4
sample 12	69	70	1
sample 13	68	69	1
Mean Error	-	-	1.69

marked peaks is anomalously wide). This translates into a different number of heartbeats detected on the retrieved signal pairs. In fact, in only 2 of the 13 subjects we obtained a perfect match in the number of detected beats. In Table 1 we show a comparative analysis between the number of heartbeats detected in both signals. In most cases, although the number of beats is different, the mean error is lower than 2 heartbeats, which is lower than previously reported results [9]. Even though this is by no means a concluding evidence of its similarity, it shows a certain degree of closeness between both signals.

More preprocessing can be applied to the webcam signal to match as much as possible the peaks detected by the PPG signal. We implemented a simple algorithm to find hidden peaks (i.e., those that were not initially detected) and to discard false peaks (i.e., those located very close to each other). The procedure is described next. First, the IPI vector is extracted from the webcam signal and the mean value ($meanIPI$) is computed. We next compare $meanIPI$ to each IPI and, if the rate between the $meanIPI$ value and the detected IPI is bigger than a predefined experimental value N, we conclude that there is a hidden beat that has not been detected, so a new IPI is added to the extracted IPI vector. This new IPI has the value $meanIPI$. Otherwise, if the rate is lower than another

Table 2. Average IPI values and and average IPI differences.

Sample	Mean IPI value PPG Sensor	Mean IPI value Webcam	Difference(s)
sample 1	1.0296	1.198	0.2188
sample 2	0.928	0.9394	0.1364
sample 3	1.0092	1.0681	0.2348
sample 4	0.9884	0.9685	0.3506
sample 5	0.9525	1.025	0.2512
sample 6	1.0071	1.038	0.1694
sample 7	0.9855	1.0167	0.1570
sample 8	0.8576	0.8924	0.2649
sample 9	0.9148	0.958	0.1684
sample 10	0.6756	0.7032	0.0676
sample 11	0.9137	0.9973	0.1951
sample 12	0.8472	0.9048	0.1570
sample 13	0.8586	0.8816	0.1182

experimental factor M, then we conclude that one of the heartbeats from which the IPI has been extracted is not real. In this case, the first heartbeat of the pair is deleted and the IPI vector is recalculated.

By applying this algorithm and tuning the $\{N, M\}$ parameters, the same number of heartbeats can be found in both signals. In order to measure the error of approximating the IPI locations, we have performed a preliminary comparison between the mean of the IPI values for each sample and then computed the mean error between both signals. Table 2 shows the result of this comparison. The mean and standard deviation of the difference between the mean IPI obtained using the camera signal and using the PPG sensor are 0.191 and 0.073, respectively. As these are very small values, we consider them as another preliminary evidence of the similarity between both sources of features.

3.3 Quantization

Having the same number of heartbeats (and thus the same number of IPIs) in both signals, the next step was to encode the signals into their binary representation. To proceed with the quantization process, we first studied different available alternatives: scalar, uniform, and dynamic quantization.

A scalar quantizer is the simplest type of quantization algorithm. It consists of a direct mapping from the input values (in this case, the time intervals between heartbeats) into a set of integers. The parameters of this algorithm are the codebook and the set of boundary points. The set of boundary points contains the values to which the input values will be rounded. That is, it contains values between the minimum and the maximum input values incremented by a quantization step obtained as a result of dividing the distance between limit values by the number of codes considered. The smaller this step is, the less quantization error will appear in the final result. The codebook contains the different values associated to each boundary point. The cardinality of these two sets depends on the desired characteristics of the output value. In order to emulate the approaches followed by previous works on IPI-based protocols [15], we encoded

each quantized value as an 8-bit unsigned integer, so $2^8 = 256$ codes have been used.

On the other hand, an uniform quantizer unifies the process of quantizing and encoding the output value. It follows a similar approach to the scalar quantizer algorithm and, as a final step, it maps the output value into an integer of the desired precision. The parameters of this algorithm are the maximum and minimum input value and the precision of the desired encoded output value. In our case, we established this parameter to 8 bits as explained above.

Finally, we also implemented the quantization algorithm employed by Rostami et al. in the H2H protocol [8], known as dynamic quantization. This algorithm assumes that the perturbation of the signal (i.e., the remainder of subtracting the signal baseline) can be modeled with a normal distribution with mean $\mu = 0$ and a standard deviation of σ. Knowing this, the Normal Cumulative Distribution Function (NCDF) is calculated for each value in the raw signal. This yields a set of values between 0 and 1 that allows us to multiply them by a roof factor to obtain values between this threshold and 0. We set this roof factor to 256 (2^8) in order to have the same resolution than in the other quantizers. Finally, the quantized values were encoded as 8-bit unsigned integers.

Once the IPI values are quantized using one of the three mentioned algorithms, its Gray code representation is calculated. This is done with the aim of eliminating (or, at least, reducing) the differences between the contact and contactless signals.

4 Results and Discussion

To analyze and measure the similarity between the PPG sensor and the webcam signals, we performed two experiments. In the first experiment, we evaluate the similarity of both signals by comparing the decimal digits of each IPI. To do so, we have grouped the decimal digits of the IPIs in four groups: two first decimal digits, three first decimal digits, second and third decimal digits, and third and fourth decimal digits. For each group, we have converted the digits into an unsigned integer, then transformed it into its 8-bit binary representation (10 bits in the case of the second group, as it includes values from 0 to 999), and finally computed the Hamming Distance (HD) between the value obtained from the PPG sensor and the value captured from the webcam. We have computed an overall similarity value (i.e., % of bits that are equal for all IPI decimals in each sample) for each sample. The results are shown in Table 3 and clearly show a similarity higher to the one that would be obtained by pure chance between both signals.

In the second experiment, we applied the quantization algorithms explained in previous subsections to obtain the binary representations of the IPI values. We have conducted the same experiment for the three different quantization algorithms. We quantized all the IPI values of each sample (the IPI values were previously normalized) and then converted them to their binary representation. This process was applied to all samples of all signals captured by both devices.

Table 3. Signal similarity of InterPulse Intervals (IPIs) at digit level

sample	2 first decimals	3 first decimals	2nd and 3rd	3rd and 4th
Sample 1	56.96%	51.80%	57.50%	65.36%
Sample 2	62.31%	55.67%	56.71%	63.61%
Sample 3	58.40%	56.37%	61.20%	61.20%
Sample 4	63.98%	51.52%	56.77%	57.41%
Sample 5	56.14%	44.90%	51.63%	61.68%
Sample 6	59.91%	54.48%	63.14%	65.51%
Sample 7	61.71%	52.18%	54.29%	65.82%
Sample 8	59.74%	48.67%	57.16%	61.94%
Sample 9	59.11%	48.81%	54.66%	62.92%
Sample 10	69.68%	59.10%	63.59%	65.93%
Sample 11	56.05%	56.40%	54.88%	61.71%
Sample 12	64.67%	58.84%	59.96%	58.51%
Sample 13	65.99%	58.08%	58.63%	60.29%
Overall	61.13%	53.60%	57.70%	62.45%

Table 4. Percentages of similar bits and entropy values obtained with the dynamic quantizer for all samples.

		Entropy	
Bit	**Hit Probability (%)**	**Sensor**	**Webcam**
1 (MSB)	62.157	0.979	0.946
2	65.071	0.947	0.959
3	49.88	0.991	0.951
4	55.741	0.781	0.959
5	47.010	0.905	0.977
6	49.880	0.997	0.961
7	51.555	0.657	0.983
8 (LSB)	52.990	0.9290	0.999
Last 4 bits	50.358	0.959	0.999
Overall	54.41	0.990	0.999

Finally we computed an overall similarity measure between the binary representations of both IPI strings (PPG sensor and webcam) belonging to all the samples in our dataset. For a better understanding of what exactly is happening here, we have also computed the similarity at the bit level (Hit Probability). Table 4 and Table 5 summarize the similarity and entropy results obtained for all the signals using the dynamic and the scalar quantizers. Due to space reasons, we do not include the results obtained with the uniform quantizer, as they are very similar to those obtained with the dynamic quantizer.

As it can be observed, the best results are obtained with the scalar quantizer. Even when the entropy is high, the Hit Probability is over 60% for the majority of the bits, including the four Least Significant Bits (LSB), which is particularly remarkable as these bits have been pointed out by previous works as the most suitable for cryptographic purposes due to their high degree of randomness [5]. In the case of the dynamic quantizer, it is evident that the results do not improve a blind guessing approach for the last four bits, although it is possible to observe a higher hit ratio in certain high entropic bits, for instance in the most significant bit. Though we are not completely guessing the bits, these results show that the webcam provides insights about the heart beat of the subjects. In the case of the scalar quantizer, the percentage of equal bits is 70% (overall value), which

Table 5. Percentages of similar bits and entropy values obtained with the scalar quantizer for all samples.

		Entropy	
Bit	**Hit Probability (%)**	**Sensor**	**Webcam**
1 (MSB)	70.095	0.714	0.868
2	61.483	0.941	0.689
3	61.004	0.898	0.762
4	62.918	0.929	0.709
5	58.688	0.959	0.816
6	94.976	0.143	0.228
7	82.775	0.0.266	0.593
8 (LSB)	70.095	0.719	0.764
Last 4 bits	76.883	0.718	0.657
Overall	70.37	0.782	0.708

again supports the hypothesis of signal similarity between the PPG sensor and the heartbeats derived from the webcam.

5 Applicability and Impact

We next analyze the potential impact of our results in a recently proposed ECG-based protocol in which IPI values are extracted from ECG chunks. In particular, we focus our efforts in the H2H (*Heart-2-Heart*) scheme proposed in 2013 by Rostami et al. [8]. In H2H, the authors developed cryptographic authentication and pairing protocols for IMDs such as pacemakers or Holter monitors. The proposed protocol is based on a comparison between a set of IPIs obtained from the implanted device (α) and another set of IPIs simultaneously taken by an external programmer (β). If both sets are nearly equal, the programmer is authenticated to the IMD and, hence, both are able to interchange commands.

As ECG signals contain a certain amount of noise, a perfect match between both set of features is rarely achieved. Thus, a similarity threshold must be established in order to have a trustworthy evidence of sameness between the compared features. However, if this threshold is naively established, it would be possible for an attacker to circumvent the protocol security by replacing a legit ECG signal with another one randomly generated. In the H2H scheme, the authors propose an statistical characterization for ECG authentication that allows to discern if the signal provided by a programmer device has been retrieved by means of physical contact or else if an attacker is trying to replace it with a fraudulent one. To do so, the authors base their approach on the statistical distribution of the error rates found in a legit comparison (both signals are retrieved synchronously by means of physical contact) and the error rate found in a fraudulent signal, which is assumed to be 0.5 (as the attacker is assumed to be unable to doing better than random guessing). In detail, the authors assume that an IPI feature set β can be accepted as a legit sample if and only if the likelihood ratio between the probability distributions of the error rates for a fraudulent read ($P(u)$) and a legit read ($Q(u)$) is bigger than a computed threshold τ. This threshold comes associated with a false positive ratio (FP) that indicates

Table 6. Results of False Positive rates values achieved for different N and FN_{req}.

N-IPI values	$FN_{req} = 1 \times 10^{-3}$	$FN_{req} = 1 \times 10^{-4}$
5	3.591×10^{-1}	5.440×10^{-1}
10	7.37×10^{-2}	1.555×10^{-1}
15	1.11×10^{-2}	3.28×10^{-2}
20	1.4×10^{-3}	5.6×10^{-3}
25	1.687×10^{-4}	8.1912×10^{-4}

the probability of accepting a fraudulent β set of IPI features as a legit one. Mathematically:

$$\log\left(\frac{P(u)}{Q(u)}\right) > \tau \tag{1}$$

Rostami et al. modeled $Q(u)$ as a binomial distribution $B(N, p)$, where N represents the number of IPIs in the feature set and p represents the mean error rate for the four LSBs of the IPI, obtained from a comparison between two legitimate signals. On the other hand, the $P(u)$ distribution is also modeled as a binomial distribution with the same N parameter and $p = 0.5$.

It is important to note that, as shown in Table 4, the dynamic quantization algorithm employed in H2H returns results that are not much better than 50% for the LSBs—only better results are obtained for the MSBs. Nevertheless, as depicted in Table 5, we are able to obtain substantially better results that blind guessing (having a hit ratio of 76.9% for the four LSBs) when using the scalar quantizer. Having results better than blind guessing makes necessary to calculate new false positive rates. To do so, we used the algorithm provided by the authors in the original paper (see Algorithm 1 in [8]). The inputs to this algorithm are P, the vector of the error rates in the four LSBs, N the number of IPIs to be compared, and FN_{req} the false negative ratio yielded by a legit programmer (i.e., meaning that a legit programmer will fail once in 10000 attempts).

In Table 6 we show our results after calculating the false positive rate for different FN_{req} and N values. As it can be seen, the false positive rates are much bigger when the adversary error rates decrease from 50% to 23%. A consequence of this difference is that, in order to achieve the same false positive rate, it is needed to retrieve more IPIs, extending the duration of the IPI retrieval process. This result can be more clearly observed in the following graphs. In Figure 4, it is possible to observe how the false positive rate decreases as the number of retrieved IPIs grows. This represents the variation for the H2H case, in which the error rate of the attacker is estimated to be 0.5. However, if a lower error rate is considered (i.e., the attacker is more accurate than random guessing), it is needed to retrieve a larger number of IPIs to achieve the same false positive rates. This can be observed in Figure 5, where the attacker error rate is set to 0.23, i.e., one minus the hit probability 0.77 shown in Table 5 for the scalar quantizer.

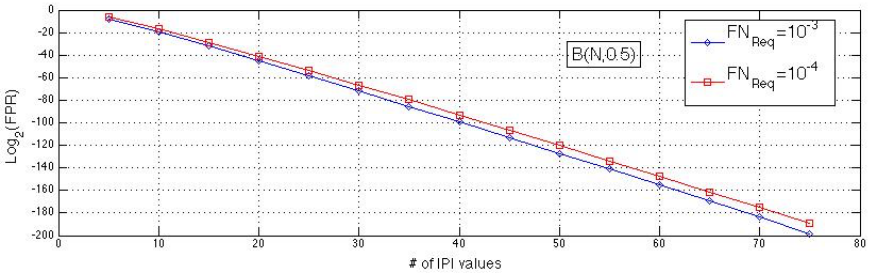


Fig. 4. Error rate equal to 0.50 (dynamic or uniform quantizer)

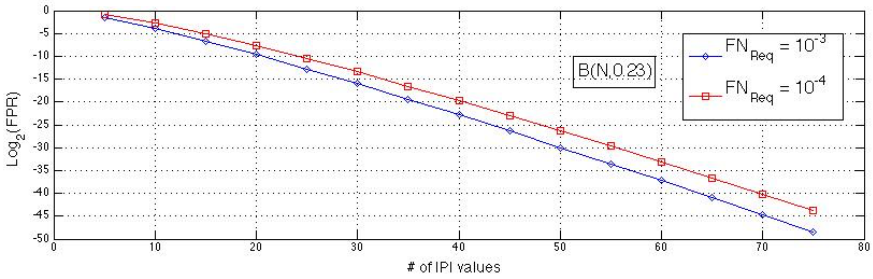


Fig. 5. Error rate equal to 0.23 (scalar quantizer)

Fig. 6. Variation of the FP rate with the number of retrieved IPIs for attacker's error rates equal to 0.50 and 0.23.

6 Concluding Remarks and Future Work

We have presented a study on the security of IPI-based security protocols when the attacker can obtain heart signals by means of a contactless method, in particular through video recording via webcam. We have analyzed the information extracted from both signals and presented a comparative study of the achieved similarity. The study has been done with different quantization algorithms, and the use of one to another will greatly affect the similarity of both signals and, therefore, the success probability of an attack. Finally, we have used the approach followed by Rostami et. al in H2H scheme to validate our hypothesis [8].

We have shown how using freely available commodity hardware it is possible to remotely gather useful information of cardiac signals. Through an analysis of the retrieved data, we have shown that even when the data obtained using contact-based techniques is highly entropic, the data obtained through a contactless technique represent up to the 70% of that information, which is clearly better than randomly guessing. Particularly, two main conclusion should be extracted from our study. First, quantization is a critical step for IPI-based schemes, so protocol designers should put more emphasis on selecting an appropriate scheme.

Second, entropy should not be the only criterion used for determining the most appropriate bits for generating cryptographic material such as keys; other criteria should include, for instance, bits that are more resistant to leakages via a webcam, as shown in this paper.

Our dataset is composed of 13 pair of signals retrieved from different volunteers, which is certainly a reduced sample for extracting strong conclusions. One immediate future work is to further validate our results with an extended dataset. It is also interesting to study how physiological parameters of the volunteers could affect the final results. For example, since all the volunteers share roughly the same skin tone, the performance of our proposal when considering volunteers with other skin tones remain unknown. We also found out that the quality of the data retrieved with the webcam strongly depends on environmental conditions such illumination or the distance between the camera and the subject. Because of our limited experimental setup, it is unclear if the use of better equipment (e.g., a camcorder with much higher resolution) will translate into a performance increase. Experimentation in open environments with a natural source of light and arbitrary distance between the subject and the camera will be also necessary.

Acknowledgements

This work was supported by the MINECO grant TIN2013- 46469-R (SPINY: Security and Privacy in the Internet of You) and the CAM grant S2013/ICE-3095 (CIBERDINE: Cybersecurity, Data, and Risks).

References

1. Halperin, D., Kohno, T., Heydt-Benjamin, T.S., Fu, K., Maisel, W.H.: Security and privacy for implantable medical devices. Pervasive Computing, IEEE **7** (2008) 30–39
2. Li, C., Raghunathan, A., Jha, N.K.: Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on, IEEE (2011) 150–156
3. Radcliffe, J.: Hacking medical devices for fun and insulin: Breaking the human scada system. In: Black Hat Conference presentation slides. Volume 2011. (2011)
4. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H.: Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: Security and Privacy, 2008. SP 2008. IEEE Symposium on, IEEE (2008) 129–142
5. Poon, C.C., Zhang, Y.T., Bao, S.D.: A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. Communications Magazine, IEEE **44** (2006) 73–81
6. Bao, S.D., Poon, C.C., Zhang, Y.T., Shen, L.F.: Using the timing information of heartbeats as an entity identifier to secure body sensor network. Information Technology in Biomedicine, IEEE Transactions on **12** (2008) 772–779

7. Bao, S.D., Zhang, Y.T., Shen, L.F.: Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In: Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the, IEEE (2005) 2455–2458
8. Rostami, M., Juels, A., Koushanfar, F.: Heart-to-heart (h2h): authentication for implanted medical devices. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM (2013) 1099–1112
9. Poh, M.Z., McDuff, D.J., Picard, R.W.: Non-contact, automated cardiac pulse measurements using video imaging and blind source separation. Optics Express **18** (2010) 10762–10774
10. Wu, H.Y., Rubinstein, M., Shih, E., Guttag, J.V., Durand, F., Freeman, W.T.: Eulerian video magnification for revealing subtle changes in the world. ACM Trans. Graph. **31** (2012) 65
11. Jain, A.K., Dass, S.C., Nandakumar, K.: Soft biometric traits for personal recognition systems. In: Biometric Authentication. Springer (2004) 731–738
12. Zhu, Y., Tan, T., Wang, Y.: Biometric personal identification based on iris patterns. In: Pattern Recognition, International Conference on. Volume 2., IEEE Computer Society (2000) 2801–2801
13. Kumar, A., Wong, D., Shen, H., Jain, A.: Personal verification using palmprint and hand geometry biometric. In Kittler, J., Nixon, M., eds.: Audio- and Video-Based Biometric Person Authentication. Volume 2688 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2003) 668–678
14. Guennoun, M., Abbad, N., Talom, J., Rahman, M., El-Khatib, K.: Continuous authentication by electrocardiogram data. In: Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto international conference, IEEE (2009) 40–42
15. Xu, F., Qin, Z., Tan, C.C., Wang, B., Li, Q.: Imdguard: Securing implantable medical devices with the external wearable guardian. In: INFOCOM, 2011 Proceedings IEEE, IEEE (2011) 1862–1870