applied sciences

MDPI

Article

Physical Layer Authentication and Identification of Wireless Devices Using the Synchrosqueezing Transform

Gianmarco Baldini *, Raimondo Giuliani and Gary Steri

European Commission, Joint Research Centre, 21027 Ispra, Italy; raimondo.giuliani@ec.europa.eu (R.G.); gary.steri@ec.europa.eu (G.S.)

* Correspondence: gianmarco.baldini@ec.europa.eu; Tel.: +39-0332-78-6618

Received: 9 October 2018; Accepted: 2 November 2018; Published: 6 November 2018

Abstract: This paper addresses the problem of authentication and identification of wireless devices using their physical properties derived from their Radio Frequency (RF) emissions. This technique is based on the concept that small differences in the physical implementation of wireless devices are significant enough and they are carried over to the RF emissions to distinguish wireless devices with high accuracy. The technique can be used both to authenticate the claimed identity of a wireless device or to identify one wireless device among others. In the literature, this technique has been implemented by feature extraction in the 1D time domain, 1D frequency domain or also in the 2D time frequency domain. This paper describes the novel application of the synchrosqueezing transform to the problem of physical layer authentication. The idea is to exploit the capability of the synchrosqueezing transform to enhance the identification and authentication accuracy of RF devices from their actual wireless emissions. An experimental dataset of 12 cellular communication devices is used to validate the approach and to perform a comparison of the different techniques. The results described in this paper show that the accuracy obtained using 2D Synchrosqueezing Transform (SST) is superior to conventional techniques from the literature based in the 1D time domain, 1D frequency domain or 2D time frequency domain.

Keywords: authentication; identification; security; wireless communication; machine learning

1. Introduction

The authentication of wireless devices can be implemented using various approaches. Historically, authentication has been implemented using information known by the device (cryptographic information) or owned by the device (a SIM card). Another form of authentication is based on what a device is (i.e., the physical properties). A well-known example is biometric authentication such as scanning of the human eye iris used to prove the authenticity of a person. This approach has disadvantages and advantages, which are well known in literature [1]. A known advantage is that the intrinsic information of a device is difficult to clone, to steal or remove from a device. The disadvantages are that the extraction of the information can be more difficult to achieve or it can provide a statistical-only confirmation of authenticity (e.g., biometrics matching to a certain level of accuracy), rather than a precise confirmation as it is obtained with cryptographic means (e.g., the signing of a message with a key). In this paper, we investigate the identification and authentication of wireless devices using the physical properties (physical layer authentication) in their transmission components, which generate specific analogical artifacts in their RF emissions. This paper is an extended version of our paper published in the 2018 41st International Conference on Telecommunications and Signal Processing (TSP) [2].

Physical layer authentication is relevant when the authentication based on cryptographic means is difficult to achieve, either due to the limitations of IoT devices or because the context does not support an efficient distribution of cryptographic materials (e.g., keys and certificates). In the case of the Internet of Things, the authors in [3] highlighted that, although the design of authentication mechanisms based on cryptography is always desirable, it may not be applicable to several IoT scenarios because it may imply high computational cost and/or always connected trusted entities. We propose an authentication mechanism for wireless devices, which can be an alternative to cryptography or can complement and strengthen it (i.e., multi-factor authentication).

The effectiveness of this identification and authentication technique has been demonstrated in the literature in various settings and propagation conditions, and it has different names: Radiometric Identification (RAI) [4], Special Emitter Identification (SEI) [5] or Radio Frequency DNA (RF-DNA) [6], because RF fingerprints resemble the DNA of human beings. It is due to small differences in the material and the composition of the electronic circuits used for wireless transmission, which are represented in the RF signal over the air. These differences are usually not relevant to hamper the correct functioning of wireless services, but they are significant enough to identify the model or the electronic device itself uniquely [7]. The differences in the wireless transmission components, which become embedded in the RF signal, are usually stable during the transmission time (even if environment and aging effects have been reported), and they are not strongly related to the transmitted content. In many cases, RF fingerprinting in ideal wireless propagation conditions (i.e., high signal to noise radio or low fading effects) can provide a very high authentication accuracy of wireless devices. This technique requires the selection of features and classification algorithms, which are both accurate and time effective. This is often a design trade-off, because the application of sophisticated features and algorithms may require a longer processing time than the application of simple features and algorithms, even if the former provide a better identification accuracy. RAI has been applied to a large variety of electronic devices and wireless standards including WiFi [8], ZigBee [9], WiMAX [6] and Global System for Mobile Communications (GSM) in [10]. An analysis of existing literature in this area is reported in Section 2.

In the rest of this paper, the terms identification and verification are used in a manner consistent with the sources in literature: Authentication is the process of confirming the claimed identity of a wireless device. In this case, the RF fingerprints of a wireless device, which claims to be the device A, are compared to the previously recorded (e.g., after the product phase and before marked deployment) fingerprints of the device A using the techniques described in this paper. Authentication (also called verification in other sources) is based on a binary classification. Identification is the process where the recognition system determines a wireless device's identity by comparing the device fingerprints with reference fingerprint templates for all known devices in the test set. Identification requires a one-to-many comparison and multi-classification algorithms.

A potential application scenario is where a wirelessly-connected central node can accept data only from authenticated wireless devices, but the computing capabilities of the wireless devices are not sufficient to support cryptographic-based authentication or the cryptographic material (e.g., private keys) in the wireless device cannot be adequately protected for cost reasons [3]. In this scenario, before the deployment of the wireless device, its wireless signals are analyzed and recorded by the central node in order to compute the RF fingerprints [7,8]. In a subsequent phase, the authentication is performed using the approach described in this paper. In this scenario, the authentication accuracy must be maximized to reduce the number of false alarms, and the processing time must be minimized. Another scenario is the fight against the distribution of counterfeit electronic products, where the RF fingerprints can be used to distinguish between counterfeit and proper products because the fingerprints will be different in counterfeit products of the same model [11].

A significant challenge for researchers both for identification and authentication is the definition of features or signal representations, which can be used to detect the differences and authenticate the wireless devices. A common strategy is to extract statistical features from the RF signal and then use

a machine learning algorithm to classify the obtained set of features and correlate them to the identity of the wireless device. There is an extensive literature on the selection of different statistical features for RAI including variance, entropy, skewness, kurtosis and others [8,12].

Our contribution: Following the recent trend of using 2D time frequency domain representations of the signal emitted by a wireless devices for the purpose of RAI, in this paper, we apply the SST algorithm to the problem of physical layer authentication and identification. In particular, we use a Wavelet Synchrosqueezed Transform (WSST) based on the Continuous Wavelet Transform (CWT). In the rest of this paper, such a transform will be called Wavelet Synchrosqueezed Transform (WSST). The WSST algorithm has been applied as a time frequency analysis tool for different kinds of nonlinear signals, such as the vibration signal in [13], for the detection of frequency shifting of earthquake damaged structures in [14] and to Time Frequency Domain (ECG) signal analysis in [15], but it has not been applied to the problem of physical layer authentication to the knowledge of the authors. In a similar way to the approach adopted by the other authors, this paper makes a comparison of the performance of WSST to methods based on the 1D time domain, 1D frequency domain and 2D Short Time Fourier Transform (STFT). The performance is evaluated on an experimental dataset of RF emissions transmitted by 12 wireless devices (i.e., GSM mobile phones) collected by the authors in a test bed environment.

As mentioned before, this paper is an extended version of our paper published in the 2018 41st International Conference on Telecommunications and Signal Processing (TSP) [2]. The following improvements and extensions have been made:

- A more extensive review of the related work in the literature for the problem of physical layer authentication (e.g., RAI, SEI or RF-DNA) and on the application of WSST.
- In the initial paper, only the identification problem was analyzed. In this paper, we also evaluate the verification/authentication problem.
- In the initial paper, only the K nearest neighbor with K = 1 was used to compare the performance of WSST with the other representations. In this paper, the authors have compared the results from different machine learning algorithms.
- A more extensive analysis and optimization of the hyperparameters of WSST and machine learning algorithms is performed in this paper.

Structure of this paper: The structure of the paper is the following: Section 2 provides a review of the related work on physical layer authentication. Section 3 provides a definition of the WSST. Section 4 provides a description of the methodology used to collect the RF signals and the test bed. Section 5 provides the experimental results and the related analysis where a comparison of different statistical features and machine learning algorithms is performed. In the first part, the results for the identification of wireless devices are provided. The second part presents the results for the verification or authentication of a wireless device. Finally, Section 6 concludes this paper.

2. Related Work

The concept of RAI is not new, as it was first proposed in the military domain to detect and identify hostile sources of RF emissions like radar systems, and it can be considered part of SIGnals INTelligence (SIGINT) or Measurement and Signature Intelligence (MASINT) [16].

More recently, the progress in electronic equipment for RF signal collection and analysis allowed the use of RAI in non-military contexts.

In some initial works [8,12], physical layer authentication was performed by analyzing the RF signal in space in the time domain or the frequency domain and by extracting statistical features or other signal characteristics. The RF devices used in the test were consumer mass market devices based on WiFi standards. The classification was performed both for the amplitude and phase components in the time domain by exploiting the non-content parts of the bursts defined in the wireless standard and transmitted by the device. The parts of the burst not related to the content must be used because the

content (e.g., data, voice) can introduce a bias. In other words, the classification could be performed on the content rather than the physical properties of the device itself. Two outcomes already appeared from these studies and other similar studies [17]. The first is that bursts are usually composed of a transient element and a steady element (e.g., the preamble). Then, a design choice appears in the design of the physical layer authentication process. As described in [17,18], a transient signal can be described as a short signal (typically lasting a few microseconds) that occurs during transmitter power-on. It is noted in [17,18] that the capture and digitization of the transient signal requires very high oversampling rates and sophisticated and expensive receiver architectures. In contrast to the transient signal, the steady-state signal can be much longer than the transient part of the burst, thus providing more information for classification purposes. The choice on which element should be used for classification depends on the wireless standard and the test bed equipment. This aspect appears in this paper, as well, where an empirical analysis has been performed on the entire burst (i.e., the non-content portion) to identify the more suitable element. In this paper, the transient is proven to provide the best performance.

Recent papers have shown that other representations of the signal can be more effective for physical layer authentication than the specific time domain or frequency domain. 2D time frequency representations have been recently used for radiometric identification in [6], where a joint time frequency Gabor Transform (GT) and Gabor–Wigner Transform (GWT) features have been used for WiMAX wireless devices. The assessments in [6] show that Gabor-based RF-DNA fingerprinting is much more effective than either 1D time domain or frequency domain methods.

As described before, WSST has not been applied (until this paper) to the problem of physical layer authentication or identification, but it has been used in other contexts. We also note that the concept of the physical layer authentication of electronic devices is not only limited to RF devices, but it can also be applied to other components like MEMS [19].

The authors have used the synchrosqueezing transform method in [20] to detect gearbox fault signals in wind turbines. The paper presents an improved diagnosis method for wind turbines via the combination of the synchrosqueezing transform and local mean decomposition. In the area of geophysics, the authors in [21] have compared different time frequency techniques, and they have highlighted the advantages for interpretations for seismic signals in the areas of speech signals and volcanic tremors. The authors in [14] have applied synchrosqueezing to interpretations of seismic signals. The results of the paper shows that synchrosqueezing outperforms other time frequency transforms like the Gabor–Wigner transform, Wigner–Ville distribution and S-transform. Both [14,21] used synchrosqueezing based on CWT (i.e., WSST). In particular [14] showed that synchrosqueezing outperforms its CWT basis. These results support the choice by the authors of this paper to use a synchrosqueezing based on CWT. To summarize: WSST provides better frequency localization and good time support in comparison with the 2D Time Frequency Domain (TFD) such as Wigner–Ville distribution (WVD) and GWT used in [6]. In relation to Empirical Mode Decomposition (EMD) used in [22] as part of Hilbert–Huang Transform (HHT), EMD lacks solid mathematical foundations, though it is attractive due to its simplicity and effectiveness, as discussed in [23]. Extensions of the synchrosqueezing algorithm in combination with other time frequency representations apart from CWT are also possible. In [24], the authors developed the Synchrosqueezing Generalized S-Transform (SSGST) for the analysis of field seismic data. Similar approaches can be used for future extensions of this paper.

As described before, WSST has not been applied until this paper to physical layer authentication or identification, which is the novelty of this paper.

3. Definition of the Wavelet Synchrosqueezing Transform

The SST is a time frequency analysis method. It is a special case of the reallocation method whose aim is to "sharpen" a time frequency representation by allocating its value to a different point in the time frequency plane [25]. This reassignment compensates for the spreading effects caused by

the mother wavelet, and it is performed only in the frequency direction, thus preserving the time resolution of the signal.

The starting point in the application of the synchrosqueezing algorithm in this paper is the continuous wavelet transform of the input signal from which instantaneous frequencies are extracted. After the extraction, an instantaneous frequency value is reassigned to a single value at the centroid of the CWT time frequency region. This final part corresponds to the squeezing of the CWT, which results in a sharpened output.

Therefore, following the description above, the synchrosqueezing algorithm can be summarized as three main steps. The first one is the application of the CWT to the original signal s, which is given by:

$$W_s(a,b) = \int s(t) a^{-\frac{1}{2}} \bar{\psi}\left(\frac{t-b}{a}\right) dt, \tag{1}$$

where $\psi(t)$ is the mother wavelet function and the bar denotes the complex conjugate, a is the scale factor and b the translation.

The extraction of the instantaneous frequencies from W_s, the second step, is done using a phase transform proportional to the first derivative of the CWT. Therefore, given a phase transform ω_s, the instantaneous frequencies can be expressed by [25]:

$$\omega_s(a,b) = -i(W_s(a,b)^{-1}) \frac{\partial W_s(a,b)}{\partial b} \tag{2}$$

Finally, the resulting wavelet coefficients containing the same instantaneous frequencies can be combined. This corresponds to the application of the SST that for a given set of wavelet coefficients $W_s(a,b)$ is expressed as follows:

$$SST(\omega_1, b) = \sum W_s(a_k, b) a^{-3/2} (\Delta a)_k, \tag{3}$$

where $(\Delta a)_k = a_k - a_{k-1}$ and ω_1 are the frequency bins. Since the SST inherits the invertibility property of the CWT, the signal can be reconstructed. In this paper, the focus is not on the signal reconstruction.

The WSST is applied to each of the bursts collected from the wireless devices as described in Section 4.2.

4. Materials and Methods

4.1. Materials

The material used in the experiment are the following:

- Twelve wireless devices (i.e., GSM mobile phones) of 4 different brands (Sony Experia, HTC One, Samsung S5 and Apple iPhone): three phones were used for each of the four models.
- An OpenBTS software was used to activate the GSM communication from each of 12 wireless Devices Under Test (DUT) and to generate the signal in space.
- A Universal Software Radio Peripheral (USRP) type N200 receiver (RX) configured with a sampling rate of 1 MHz is used to collect the signal in space from each of the 12 transmitting wireless devices. The wireless devices were linked with a GSM base station implemented using OpenBTS running on a USRP N200. The base station and digitizer were fully disciplined and synchronized using a Global Positioning System (GPS) receiver with a Global Positioning System Disciplined Oscillator (GPSDO). To support repeatability and stability, the same USRP digitizer, as well as the same base station were used for all tests. All tests were performed after a minimum half hour lock after the Global Navigation Satellite System (GNSS) receiver was properly synchronized

on at least four satellites. In the Software-Defined Radio (SDR), the signal is received and down-converted using a WBX, flexible frequency front-end compatible with the USRP with a passing bandwidth of 40 MHz and tuning capabilities from 20 MHz to 2 GHZ. Then, the signal is digitally down-converted by the built-in Digital Down Converter (DDC) employing half band and Cascaded Integrator Comb (CIC) decimators from 100 MHz to 1 MHz.

A summary of the parameters and settings used for the collection of the signal in space is provided in Table 1.

Table 1. Parameters for signal collection.

Sampling frequency	1 MS/s IQ
Sample recording time	60 s
Downlink frequency	935.2 MHz
Uplink frequency	890.2 MHz
Synchronization	GPS only, using GPSDO (min 4 satellites, min 30 min lock)
Distance between DUT and RX	0.84 m
USRP gain	5
GSM arfcn	1
OpenBTS version	3.1.3

4.2. Methodology

The overall methodology for the classification of the wireless devices using the WSST is shown in Figure 1.

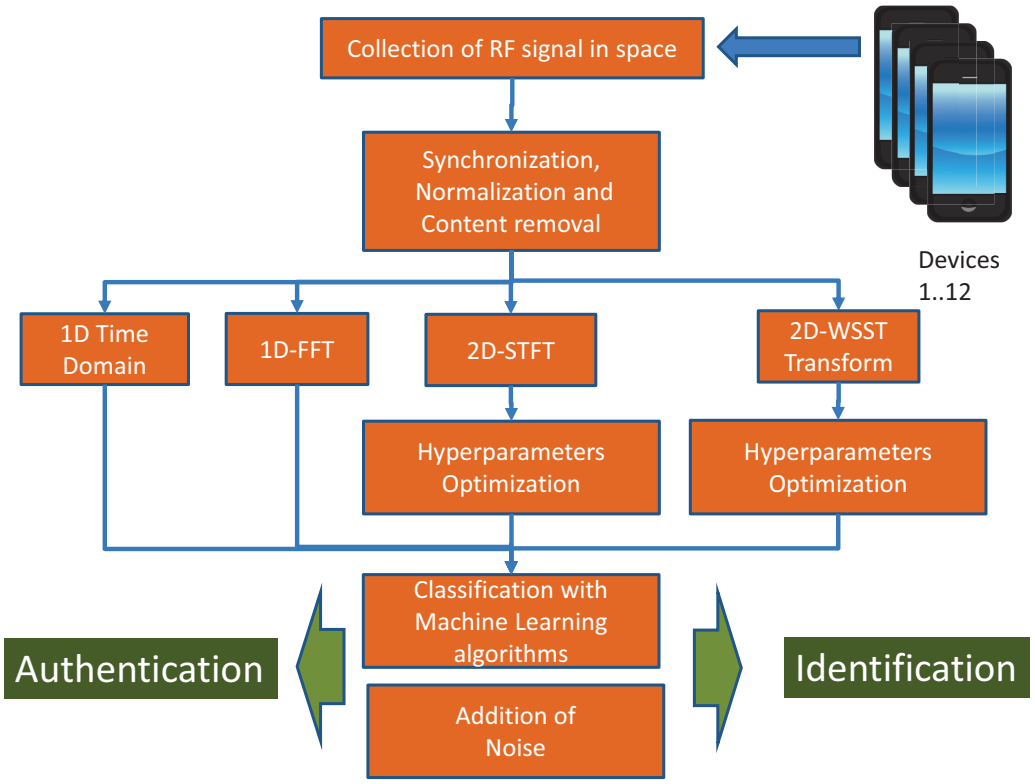

Figure 1. Overall methodology used in this paper for the identification and authentication of the wireless devices.

The methodology to generate the fingerprints from the RF signals consisted of the following steps:

1. Each of the 12 wireless devices (i.e., GSM mobile phones) were activated, and they started to transmit in a controlled environment where a specific transmission channel is used.
2. The signal in space from the wireless devices was collected using the SDR USRP type N200 receiver with the configuration described in the previous section.
3. The real-valued signal samples were sampled directly in In-phase and Quadrature components (IQ) format and then synchronized and normalized offline to extract the burst of traffic associated with each payload. For each wireless device, a set of 800 bursts was processed for a total of $800 \times 12 = 9600$ bursts.
4. From each burst, the content (payload data associated with the voice communication) was removed. In this way, each burst has only the transients and the preamble, which is the same for all the bursts and all the devices. After the removal, each burst is around 130 samples in length. An image of the normalized magnitude of the GSM bursts after synchronization, normalization and content removal is presented in Figure 2, where the differences among wireless devices can be seen especially near the transients. We note that the granularity of the digitized signal (i.e., number of samples for each burst) used for identification is quite inferior to the granularity of the datasets used by other authors [6,12,18], where a very high identification accuracy is obtained. This is intentional because the objective of this paper is to show that the application of WSST provides a better performance than conventional techniques from the literature in difficult datasets like the one used in this paper.
5. WSST was applied to each of the bursts recorded in the test bed. A representation of the burst is shown in Figure 3 for the Morlet mother wavelet, the scale factor $a = 10$ and the entire GSM burst.
6. Different machine learning algorithms are used for classification to implement identification and authentication: Support Vector Machine (SVM), K Nearest Neighbor (KNN) and decision trees. A 10-fold method was used for all the machine learning algorithms. Each collection of statistical fingerprints is divided into ten blocks. Nine blocks from each device are used for training, and one block is held out for classification. The training and classification process is repeated ten times until each of the ten blocks has been held out and classified. Thus, each block of statistical fingerprints is used once for classification and nine times for training. Final cross-validation performance statistics are calculated by averaging the results of all folds.
7. Optimization of the hyperparameters: In the application of WSST, the scale factor a from Equation (1) is used as a hyperparameter. The window size both for WSST and STFT is set to 10 because this is roughly the size of the transient of the burst. Each of the machine learning algorithms can be optimized on the basis of specific parameters (e.g., K index for the KNN algorithm). The optimization of these parameters is described in detail in Section 5.
8. Metrics definition: For identification, the overall identification accuracy is used as a metric to evaluate the performance of the identification. The accuracy is defined as the sum of the True Positives (TP)s and True Negatives (TN)s divided by the number of all samples. To show the relevance of False Positives (FP) and False Negatives (FN) in the final results, a confusion matrix is also provided. For verification and authentication, the adopted metrics are the Receiver Operative Characteristics (ROC) and the Equal Error Rate (EER), which is the point on the ROC where false positive and false negative rates are equal. The value of the X axis is used to determine the EER in this paper.
9. Impact of noise. Additive White Gaussian Noise (AWGN) is added to the original data sample to simulate the presence of noise in the environment. This is a common practice in the literature [26,27] to evaluate the performance of the classification algorithm in terms of identification accuracy for different values of Signal Noise Ratio (SNR).

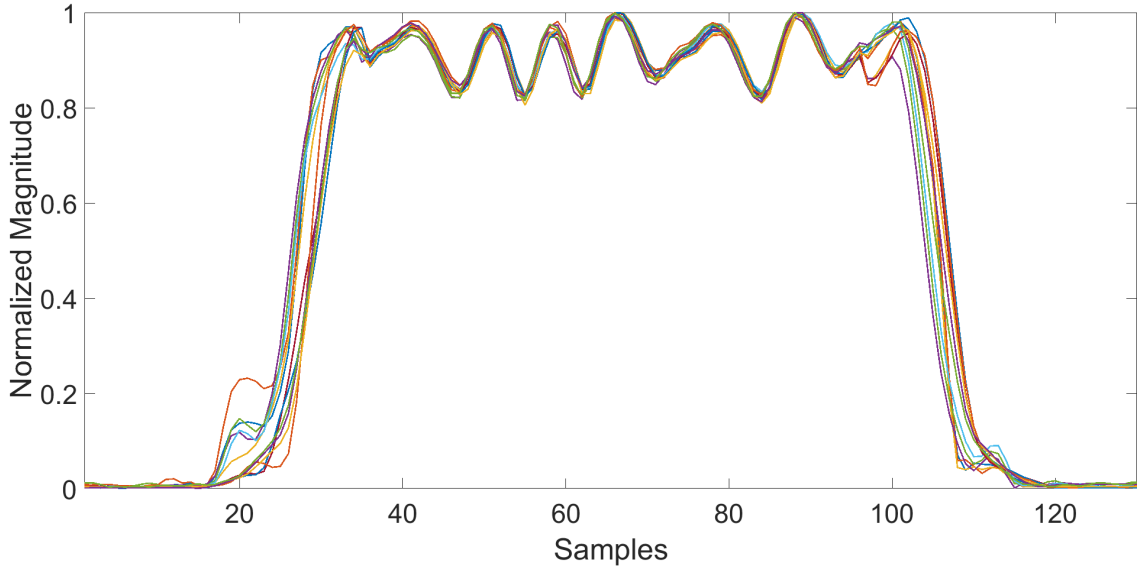

Figure 2. Normalized magnitude of 12 bursts (one for each wireless device).

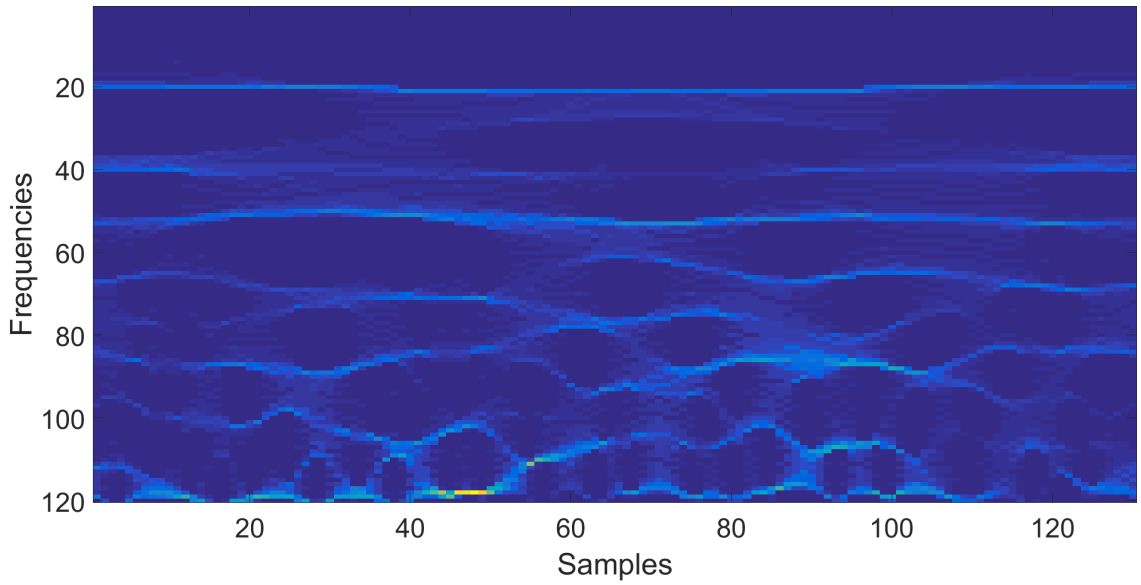

Figure 3. Spectrogram of the synchrosqueezing transform of the digitized signal from the wireless devices.

5. Discussion of the Results

5.1. Identification

In this section, the identification problem is evaluated. The first sub-section is focused on the optimization of the hyperparameters. The second section evaluates the performance in the presence of AWGN.

5.1.1. Optimization of the Hyperparameters

The WSST has different parameters (e.g., degrees of freedom), which can be optimized for the specific problem to be addressed. In this paper, we choose the two following parameters for our analysis: (a) the number of octaves and (b) the mother wavelet: Morlet or bump. Another parameter is the identification of a specific segment of the digital representation of the signal, which can be more

appropriate for classification. Signals captured from the wireless devices are usually represented as bursts, which are repeated in time, and they are usually composed by a transient portion and a steady portion. The digital representation of the GSM burst signal used in this work is provided in Figure 2. As described in the related work, some papers focus only on the transient phase of the digital signal, while other papers focus on the steady part. In this paper, the optimal segment is determined in an empirical way. In addition, the WSST can be applied to the entire complex digital output from RF emissions or only the magnitude (see Figure 2) and phase components in the time domain. Then, we have four degrees of freedom, which must be evaluated to determine the optimal values. Because the analysis of all four degrees of freedom (1 magnitude or phase, 2 segment, 3 scale factor, 4 base wavelet) will be too complex to pursue (the optimization should be conducted in a four-dimensional space), a piecewise approach is adopted. In the first step, the segment and the scale factor a from Equation (1) are optimized. A simple KNN neighbor algorithm with K = 1 is used to avoid the process of the optimization of the hyperparameters of the machine learning algorithm.

The next step is to optimize the scale value a and the segment of the burst at the same time. In comparison to the preliminary paper [2], where the optimization was performed with a specific scale factor value ($a = 10$), in this paper, we conduct a more extensive analysis on the bidimensional space of the WSST scale factor and the segment index.

In this paper, the WSST representation is divided into 10 segments along the X axis (e.g., the samples of the burst). The reason for this choice is based on two reasons: (1) the visual analysis of Figure 2, which shows that the strongest deviations from the ideal shape of the GSM burst are in the transient region, and (2) the results of [28], which showed an improved accuracy using transients rather than the steady portion of the GSM burst.

The result is shown in Figure 4, where it can be seen that the optimal segment is three, which is consistent with the original paper [2], while the optimal scale factor is 20, which provides a slighter improvement to the values of 10 adopted in the original paper. We note that the choice of the segment is the most relevant element to contribute to the performance.

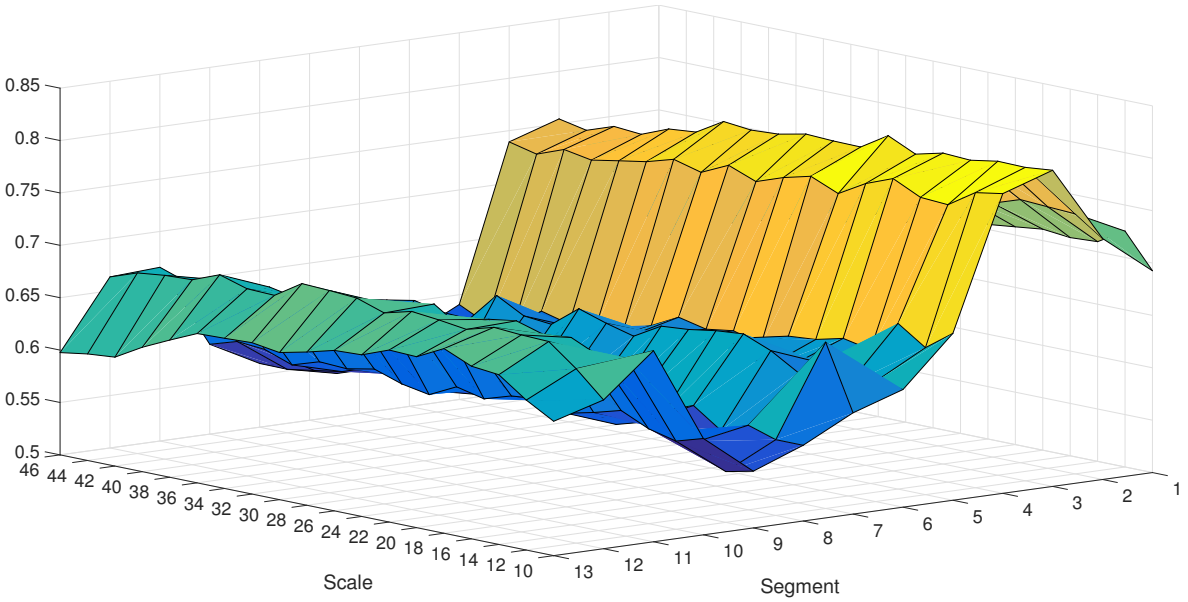

Figure 4. Accuracy for different values of segment Id and the scale factor value.

Then, a comparison of the Morlet and bump wavelets was performed, and the results are shown in the bar graph of Figure 5. The evaluation was performed using the KNN machine learning algorithm for different values of K (from one to 10). The result showed that the accuracy obtained using the Morlet wavelet in WSST was significantly better than the bump wavelet for all the considered values of K. The results are consistent with the initial findings of [2].

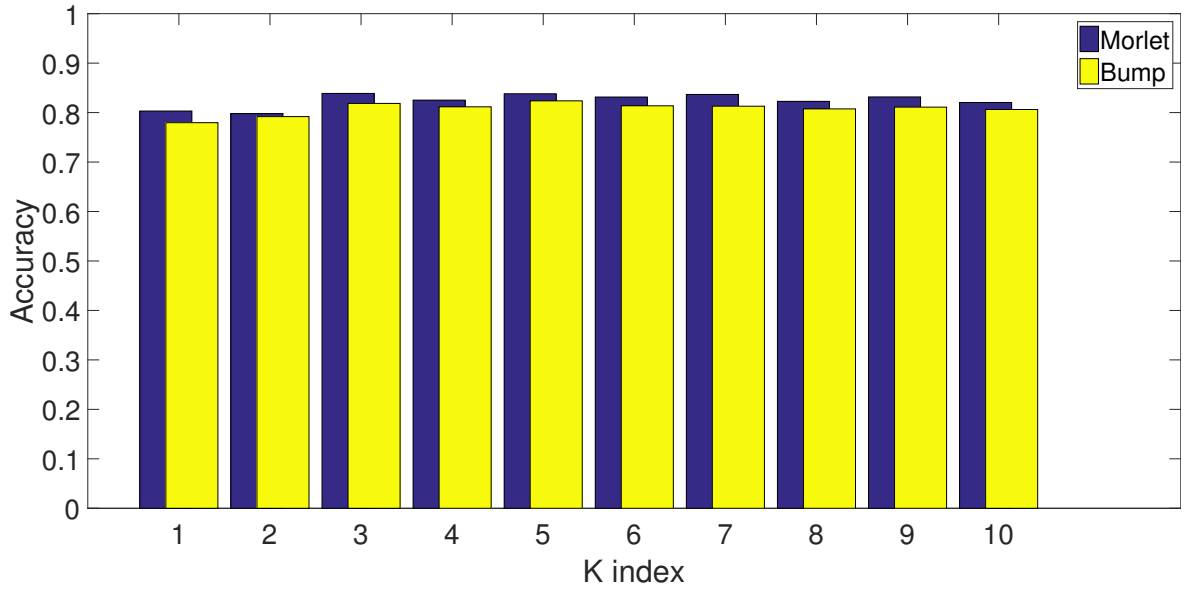

Figure 5. Comparison of the performance accuracy with KNN using Morlet and bump wavelets for different values of K.

A comparison of the amplitude and phase components of the digitized signal was performed, and the results are shown in the bar graph of Figure 6. The evaluation was performed using the KNN machine learning algorithm for different values of K. The results show that the best accuracy was obtained using the magnitude component in the time domain. The results are consistent for all the considered values of K, and they also confirm the initial findings of [2].

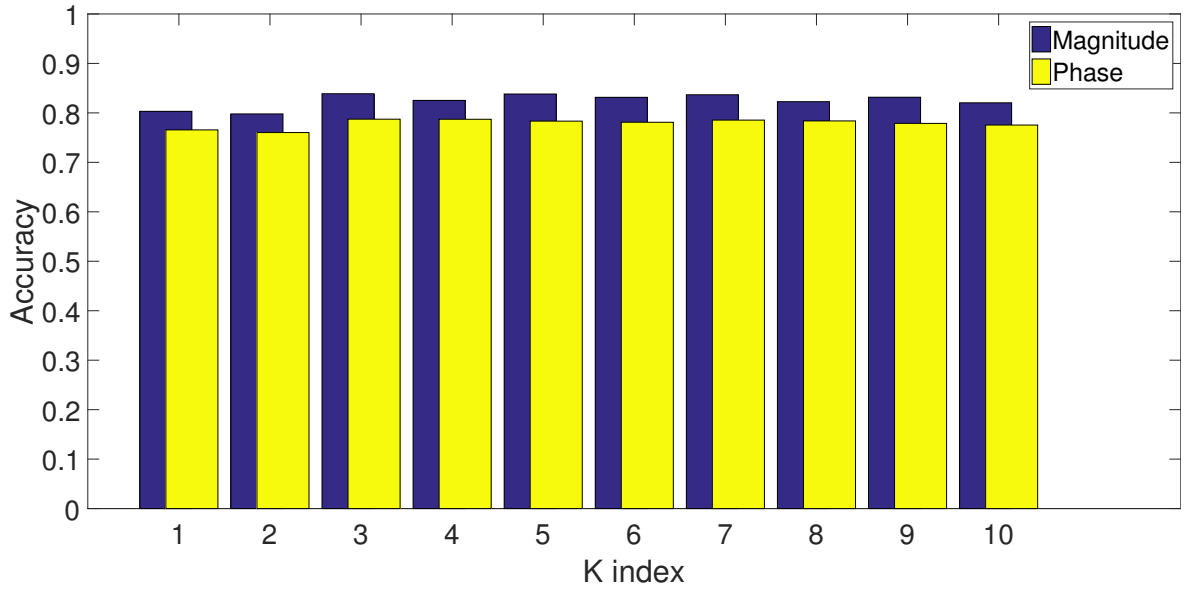

Figure 6. Comparison of the performance accuracy with KNN for the magnitude and phase components of the signal in the time domain for different values of K.

Finally, the optimization of the hyperparameters of the machine learning algorithms was performed. In this paper, we compared the results of three different machine learning algorithms: SVM (using a Radial Basis Function (RBF) kernel), KNN and decision trees.

The optimization of the SVM was performed for two hyperparameters: the scaling factor of the RBF kernel and the penalty factor C [29]. A grid approach was adopted to calculate the hyperparameters in the range of 2^1 to 2^{12} for both hyperparameters. The optimization process was

applied to each of the 10 folds, and the results were averaged. The results of the optimization analysis are shown in Figure 7 for a specific fold (where the specific fold result was the same of the average value), where the optimal value is highlighted with a black circle.

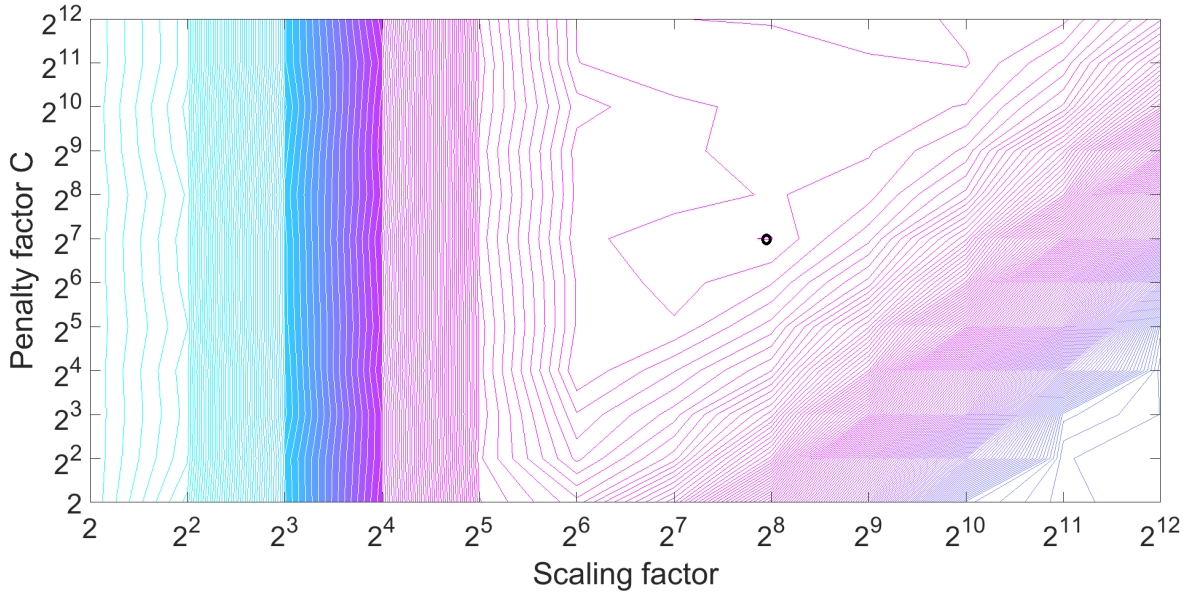

Figure 7. Optimization of the scaling factor and the penalty factor for SVM.

For WSST and KNN, the optimization results can also be seen from the previous Figures 5 and 6 where K (K = 3) for the KNN algorithm is the optimal value. In the application of the decision tree algorithm, the hyperparameter to optimize is the maximum number of splits for each branch. The optimal value is 12 for WSST.

The optimization process was repeated for the other representations of the digital signal (time domain, frequency domain and STFT) by averaging the results from each fold. The summary of the optimal values is shown in Table 2 for all the representations and for all the machine learning algorithms. The optimal values and machine learning algorithms were used in the subsequent sections of this paper.

Table 2 shows that the technique based on WSST significantly outperformed the other representations of the digital signal (time domain, frequency domain and STFT) for all the used machine learning algorithms. In other words, the superior performance of WSST was proven in a consistent way regardless of the machine learning algorithm.

Table 2 also provides the computation time requested by each machine learning algorithm and for each representation. The times were also based on averaging the results as written above. The computation time was expressed as the ratio with the smallest computation time (i.e., decision tree with time domain representation). The computation time is another metric (together with the identification accuracy) that a user can evaluate to decide the best technique in the practical deployment of the physical layer authentication approach described in this paper. It can be seen that the WSST required a larger computation time than the other techniques, while the most efficient technique was the time domain representation. The results from Table 2 were obtained on the experimental dataset where the RF signal was collected by the SDR in Line Of Sight (LOS) conditions and for high values of SNR. In the next subsection, we evaluate the performance of the WSST-based technique in the presence of AWGN for different values of SNR.

Table 2. Optimal values for the hyperparameters of the machine learning algorithms with the related identification accuracy and computing time ratio.

Machine Learning Algorithm	Optimal Values	Identification Accuracy	Computing Time Ratio
WSST	===	===	===
SVM	$C = 2^7, \gamma = 2^8$	**0.9236**	10
KNN	K = 3	0.8388	8.57
Decision Tree	$N_s = 12$	0.8225	7.28
STFT	===	===	===
SVM	$C = 2^7, \gamma = 2^9$	**0.8503**	4.64
KNN	K = 17	0.706	4.285
Decision Tree	$N_s = 18$	0.753	4
1D Frequency domain (magnitude component)	===	===	===
SVM	$C = 2^{12}, \gamma = 2^8$	0.753	4.35
KNN	K = 3	**0.7558**	1.785
Decision Tree	$N_s = 18$	0.7352	1.428
1D Time domain (magnitude component)	===	===	===
SVM	$C = 2^{12}, \gamma = 2^8$	0.7558	3.64
KNN	K = 9	**0.7910**	1.1
Decision Tree	$N_s = 17$	0.7265	1

5.1.2. Comparison of the WSST-Based Approach with Other Signal Representations in the Presence of AWGN

In the preliminary paper [2], an initial comparison was performed for different values of SNR using KNN as a machine learning algorithm with K = 1. The result has shown that the WSST-based techniques outperformed the other techniques for medium and higher values of SNR. The robustness of the identification algorithm in the presence of noise is an analysis commonly performed in the literature [26,27], to evaluate the impact of attenuation due to the propagation loss or the presence of obstacles (e.g., walls).

In this paper, we present an updated version of the comparison of the performance for the different representations, using the optimized hyperparameters from Table 2. The result is shown in Figure 8, where it can be seen that WSST still outperformed the other techniques for high values of SNR, while STFT had a better performance for lower values of SNR. The black line identifies the results from the preliminary paper [2] using the WSST technique. We note that the optimization of the parameters provided a significant improvement for all the values of SNR.

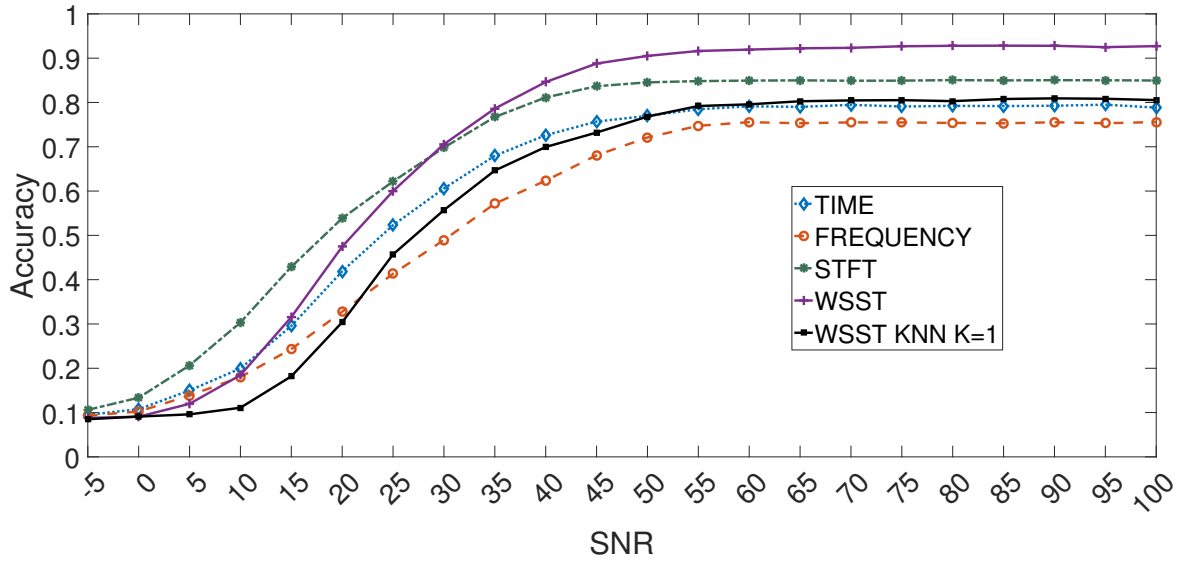

Figure 8. Accuracy for different values of SNR (expressed in dB) for 1D TD, 1D FD, 2D STFT and 2D WSST using the optimal selection of hyperparameters defined in Table 2. The black line is inserted to show the comparison with the application of the WSST technique with KNN (K = 1).

Finally, the confusion matrices were calculated. Two figures are presented: The original confusion matrix from [2] is presented in Figure 9, where KNN with K = 1 was used. A new confusion matrix is provided in Figure 10, which is based on the optimal values reported in Table 2: SVM with $C = 2^7$, $\gamma = 2^8$. Both confusion matrices have been calculated at SNR = 50. The lower accuracy for the last three phones (10 to 12) was due to the strong similarity of the RF emissions of the Apple (i.e., iPhone) models.

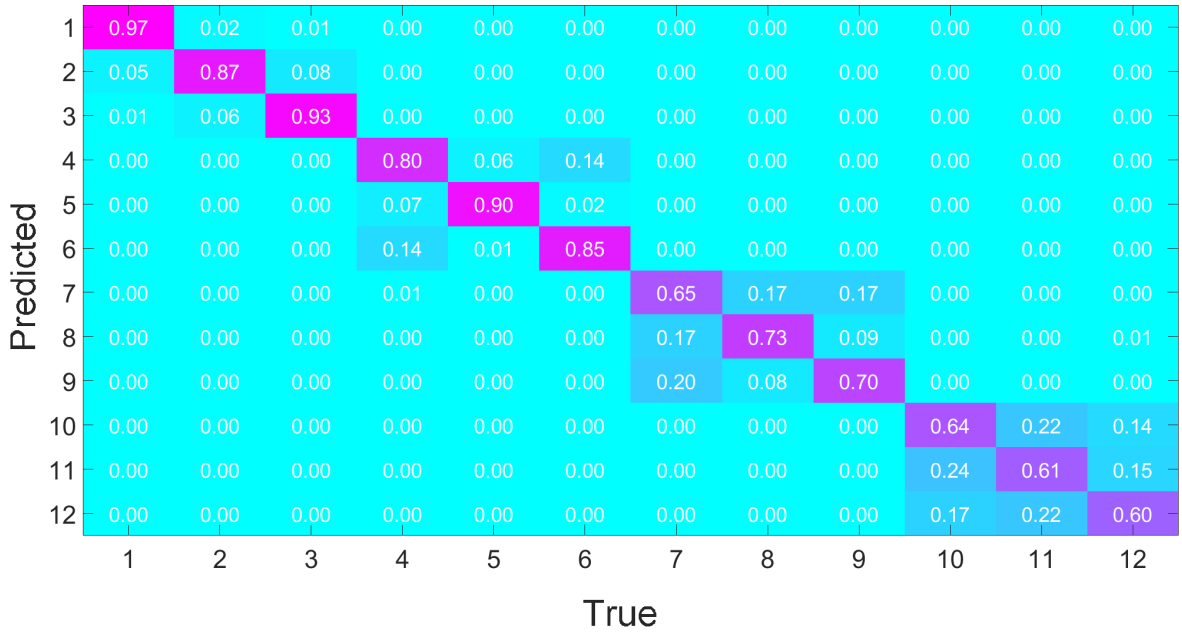

Figure 9. Confusion matrix for WSST calculated with the KNN machine learning algorithm with K = 1 at SNR = 50 dB.

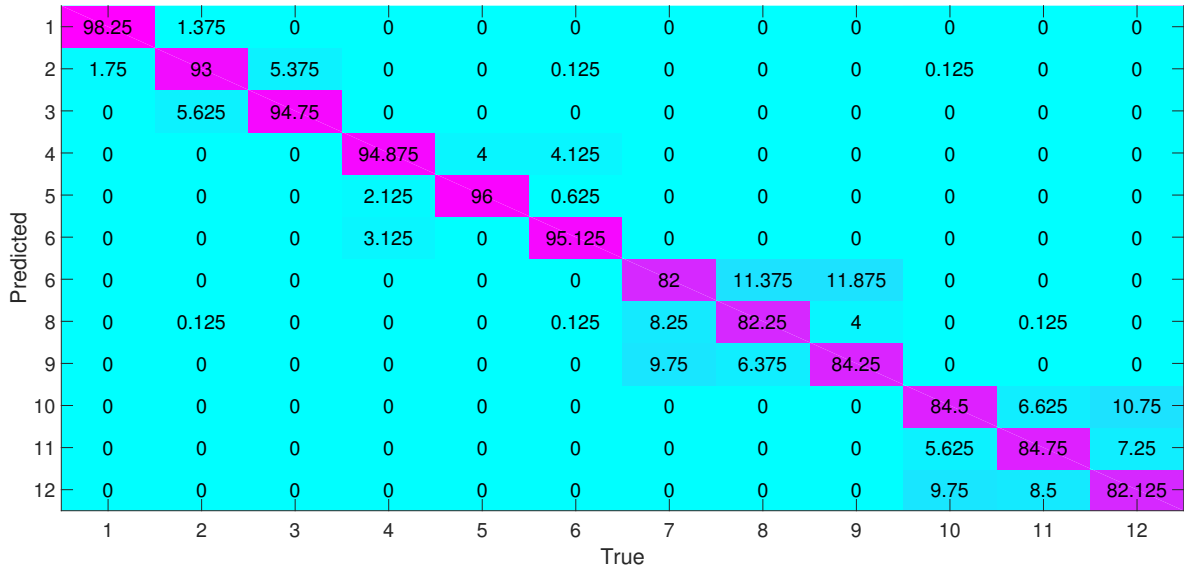

Figure 10. Confusion matrix for WSST calculated with the optimized values of Table 2 and SNR = 50 dB.

5.2. Authentication

In this section, we investigate the performance of WSST in comparison to the other techniques for the problem of authentication. The confusion matrix provided in Figure 9 shows that the final three mobile phones were the most difficult to distinguish. Then, in this section, we focus on the authentication of two of these phones (Phone 10 and Phone 12).

As for the previous results, we used the optimal values of WSST from the previous section and the SVM machine learning algorithm identified in Table 2.

Figure 11 shows the results for the EER metric for the authentication of Phone 10 against Phone 12. The scenario is that Phone 12 claimed to be Phone 10 and the EER was used to measure how well the algorithm was able to authenticate Phone 10. Figure 11 shows the comparison of the performance of WSST against the other representations. The results are consistent with the analysis on the identification accuracy: the WSST-based approach provided a higher authentication accuracy (lower EER for medium/high values of SNR) in comparison to the other representations. For lower values of SNR, the other techniques performed better than WSST, which was consistent with the findings of the previous section where STFT performed better than WSST at lower SNR. On the other side, a low accuracy limits the practical use of this technique. Then, for low values of SNR, all the techniques would have a limited use (as also reported in the literature), and filtering techniques should be used to remove the presence of noise [7].

Figure 12 shows the ROCs for the WSST-based approach with SVM for different values of SNR. The results are consistent with the previous Figure 11 because higher values of SNR generated ROC curves that showed a better authentication.

5.3. Authentication of Unknown Devices

In the previous section, we provided the results with a closed set of devices used both in training and testing where a 10-fold cross-validation was applied. This section deals with the identification of unknown devices, which were not in the training set: What if unknown devices, which are not used in training, tried to identify or authenticate themselves? To address this question, we have analyzed two cases: (a) when the unknown device is of the same model of some of the devices in the training set; in this case, the algorithm should predict that it is of a specific model, but not of the other models; (b) when the unknown device is of a different model from the models already present in the training set. In this case, the algorithm should determine that it is completely unknown. To implement the first case (a), we have first decreased the initial training set to 11 devices. Device 12 (i.e., an Apple

iPhone) has been removed from the training set and then tested against the training model built with the other 11 devices, where nine devices belonged to three different models (i.e., three Sony Experia devices, three HTC One devices and three Samsung S5 devices) and two devices belonged to the same iPhone model. The expected result was that the classification algorithm should predict that the unknown phone did not belong to the three models Sony Experia, HTC One and Samsung S5. It should predict that it was an iPhone model. On the other side, the classification algorithm should also predict that the unknown device was not one of the two specific iPhones (called iPhone 1 and iPhone 2 in the rest of this section). In an ideal case, the classification results should indicate a random choice (50% probability) that the unknown device was one of the two iPhones.

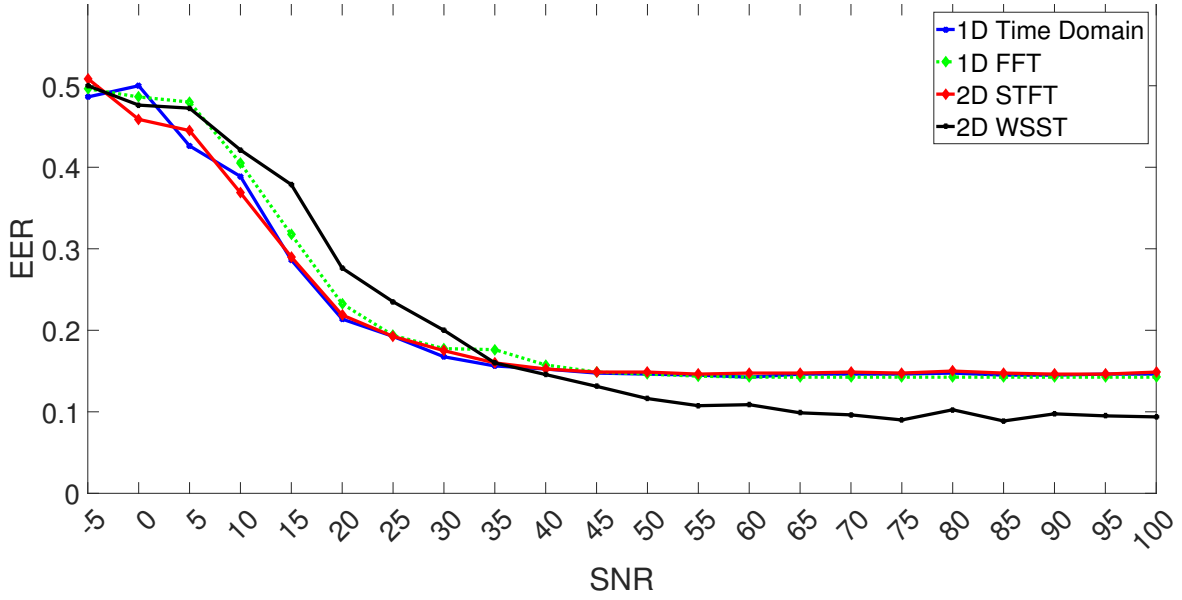

Figure 11. Evaluation of the authentication performance in the presence of noise between Device 10 and Device 12 using EER for the different techniques. SNR is expressed in dB.

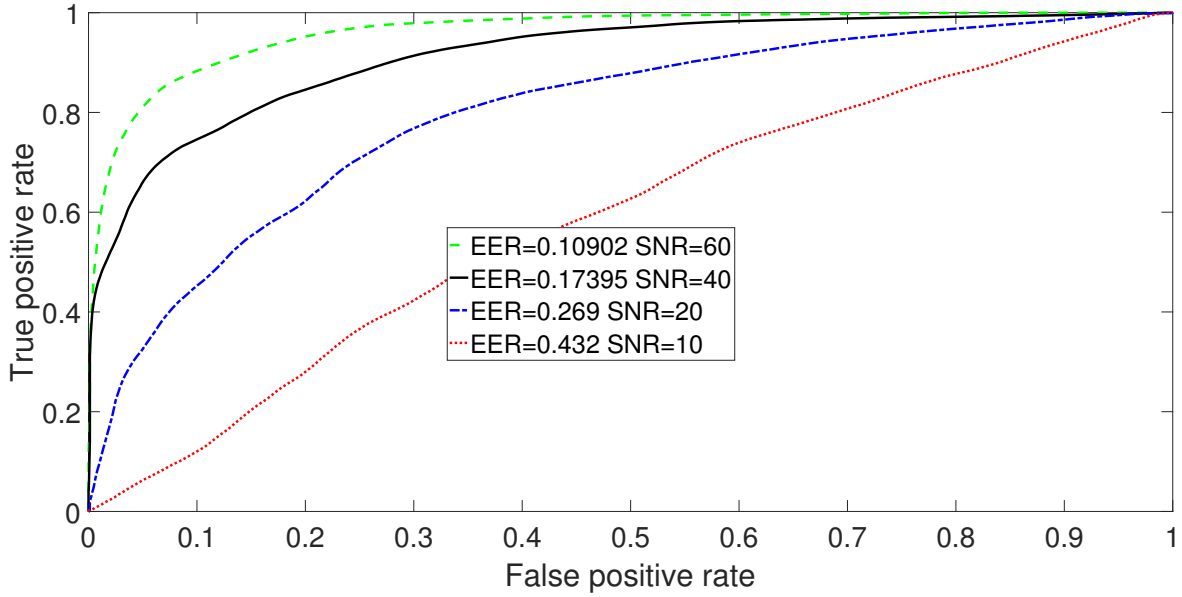

Figure 12. ROCs for the authentication performance between Device 10 and Device 12 for specific values of SNR. SNR is expressed in dB.

The results for Case (a) are shown in Table 3 for all the different representations. The SVM algorithm has been used in this case. For completeness, the classification has been repeated for

different values of SNR. The predicted percentage in the first column shows the predictions against the devices of the three models (Sony Experia, HTC One and Samsung S5), and the second and third columns show the predicted percentage against the iPhone 1 and iPhone 2.

Table 3. Predicted percentage with an unknown device.

Technique	Predicted Percentage for the Three Models	Predicted Percentage for iPhone 1	Predicted Percentage for iPhone 2
SNR = 100	===	===	===
WSST	0	0.51	0.49
STFT	0	0.72	0.28
FFT	0	0.57	0.43
TIME	0	0.77	0.23
SNR = 10	===	===	===
WSST	0.45	0.18	0.37
STFT	0.3	0.21	0.49
FFT	0.44	0.18	0.38
TIME	0.26	0.26	0.48
SNR = 0	===	===	===
WSST	0.8	0.09	0.11
STFT	0.71	0.1	0.19
FFT	0.77	0.1	0.13
TIME	0.69	0.15	0.16

The results confirm the initial assumptions: for high values of SNR, the algorithm successfully predicted that the unknown device was not one of the three models (i.e., Sony Experia, HTC One and Samsung S5) as the predictions were zeros for all the techniques (first column in Table 3). The predicted percentage was not zero for the iPhone 1 and iPhone 2 as the algorithm predicted that the unknown device was of type iPhone. We note that the WSST-based technique provided the best predictions, because the predicted percentage was almost equally divided between iPhone 1 and iPhone 2. In other words, the algorithm did not associate the unknown device to a specific known device of the same model. The other techniques (STFT and TIME) predicted that the unknown device was more similar to iPhone 1, which was an inaccurate prediction. The FFT-based technique provided similar results (but slightly worse) to the WSST-based technique. In the presence of noise (low SNR values), the prediction degraded significantly, as expected from the results in Section 5.1.2. For SNR = 0, the algorithm was not able to provide accurate predictions for all techniques. In Case (b), the training set was composed only of the nine devices of the three models (i.e., Sony Experia, HTC One and Samsung S5), and the algorithm was tested against each of the iPhone devices. We obtained a predicted percentage of 0.112 for iPhone 1, 0.131 for iPhone 2 and 0.1 for iPhone 3, which shows that the algorithm recognized them as unknown devices in comparison to the training set.

6. Conclusions

This paper has presented the novel application of WSST to the physical layer authentication and identification of wireless devices for an experimental dataset based on the collection of RF emissions of 12 wireless devices (e.g., GSM mobile phones). The dataset is particularly challenging because the RF emissions has been collected with a low sample rate (1 MHz). This paper has performed an analysis on the application of WSST both for the problem of identification and authentication. The analysis includes the evaluation of the performance in the presence of AWGN. In both cases, the application of WSST

outperforms STFT and the time domain and the frequency domain representation for medium and high SNR values. The results are consistent for different machine learning algorithms. An extensive analysis of the hyperparameters for the application of WSST has been implemented.

Author Contributions: Conceptualization, G.B., R.G. and G.S. Methodology, G.B. Software, G.B., G.S. Validation, G.S. Resources, R.G. Data curation, R.G. Writing, original draft preparation, G.B. Writing, review and editing, G.B., R.G. and G.S. Project administration, G.B. Funding acquisition, G.B.

Funding: This research has been supported by the EC H2020-IOT-2016-2017 (H2020-IOT-2017) Program under Grant Agreement 780139 for the SEcuRe and safe Internet Of Things (SerIoT) Research and Innovation Action.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses or interpretation of the data; in the writing of the manuscript; nor in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AWGN	Additive White Gaussian Noise
CMOS	Complementary Metal Oxide Semiconductor
CWT	Continuous Wavelet Transform
DDC	Digital Down Converter
ECG	Electro-CardioGram
EER	Equal Error Rate
EMD	Empirical Mode Decomposition
FAR	False Accept Rate
FN	False Negatives
FP	False Positives
FRR	False Reject Rate
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile Communications
GT	Gabor Transform
GWT	Gabor–Wigner Transform
HHT	Hilbert–Huang Transform
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
KNN	K Nearest Neighbor
PNU	Pixel Non-Uniformity
PRNU	Photo-Response Non-Uniformity noise
PUF	Physical Unclonable Functions
RAI	Radiometric Identification
RF	Radio Frequency
RF-DNA	Radio Frequency DNA
ROC	Receiver Operative Characteristics
SDR	Software-Defined Radio
SNR	Signal to Noise Ratio
SST	Synchrosqueezing Transform
STFT	Short Time Fourier Transform
SVM	Support Vector Machine
TAR	True Accept Rate
TD	Time Domain
TFD	Time Frequency Domain
TN	True Negatives
TP	True Positives
UMTS	Universal Mobile Telecommunications System

USRP Universal Software Radio Platform
WSST Wavelet Synchrosqueezed Transform
WVD Wigner–Ville distribution

References

1. Sandhu, R.; Samarati, P. Authentication, access control, and audit. *ACM Comput. Surv.* **1996**, *28*, 241–243. [CrossRef]
2. Baldini, G.; Steri, G.; Giuliani, R. Synchrosqueezing Transform Based Methodology for Radiometric Identification. In Proceedings of the 2018 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 4–6 July 2018; pp. 1–5.
3. Restuccia, F.; D'Oro, S.; Melodia, T. Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking. *IEEE Internet Things J.* **2018**. [CrossRef]
4. Brik, V.; Banerjee, S.; Gruteser, M.; Oh, S. Wireless device identification with radiometric signatures. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, San Francisco, CA, USA, 14–19 September 2008; pp. 116–127.
5. Huang, G.; Yuan, Y.; Wang, X.; Huang, Z. Specific Emitter Identification Based on Nonlinear Dynamical Characteristics. *Can. J. Electr. Comput. Eng.* **2016**, *39*, 34–41. [CrossRef]
6. Reising, D.R.; Temple, M.A.; Oxley, M.E. Gabor-based RF-DNA fingerprinting for classifying 802.16 e WiMAX mobile subscribers. In Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 30 January–2 February 2012; pp. 7–13.
7. Xu, Q.; Zheng, R.; Saad, W.; Han, Z. Device Fingerprinting in Wireless Networks: Challenges and Opportunities. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 94–104. [CrossRef]
8. Suski, W.C., II; Temple, M.A.; Mendenhall, M.J.; Mills, R.F. Using spectral fingerprints to improve wireless network security. In Proceedings of the IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, New Orleans, LO, USA, 30 November–4 December 2008; pp. 1–5.
9. Bihl, T.J.; Bauer, K.W.; Temple, M.A.; Ramsey, B. Dimensional reduction analysis for Physical Layer device fingerprints with application to ZigBee and Z-Wave devices. In Proceedings of the Military Communications Conference, MILCOM 2015, Tampa, FL, USA, 26–28 October 2015; pp. 360–365. [CrossRef]
10. Reising, D.R.; Temple, M.A.; Mendenhall, M.J. Improved wireless security for GMSK-based devices using RF fingerprinting. *Int. J. Electron. Secur. Digit. Forensics* **2010**, *3*, 41–59. [CrossRef]
11. Lakafosis, V.; Traille, A.; Lee, H.; Gebara, E.; Tentzeris, M.M.; DeJean, G.R.; Kirovski, D. RF Fingerprinting Physical Objects for Anticounterfeiting Applications. *IEEE Trans. Microw. Theory Tech.* **2011**, *59*, 504–514. [CrossRef]
12. Klein, R.; Temple, M.A.; Mendenhall, M.J.; Reising, D.R. Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–5. [CrossRef]
13. Li, C.; Liang, M. Time–frequency signal analysis for gearbox fault diagnosis using a generalized synchrosqueezing transform. *Mech. Syst. Signal Process.* **2012**, *26*, 205–217. [CrossRef]
14. Kumar, R.; Sumathi, P.; Kumar, A. Synchrosqueezing Transform-Based Frequency Shifting Detection for Earthquake-Damaged Structures. *IEEE Geosci. Remote Sens. Lett.* **2017**, *14*, 1393–1397. [CrossRef]
15. Wu, H.T.; Chan, Y.H.; Lin, Y.T.; Yeh, Y.H. Using synchrosqueezing transform to discover breathing dynamics from ECG signals. *Appl. Computat. Harmonic Anal.* **2014**, *36*, 354–359. [CrossRef]
16. Dudczyk, J.; Matuszewski, J.; Wnuk, M. Applying the radiated emission to the specific emitter identification. In Proceedings of the 15th International Conference on Microwaves, Radar and Wireless Communications, 2004, MIKON-2004, Warsaw, Poland, 17–19 May 2004; Volume 2, pp. 431–434.
17. Rehman, S.U.; Sowerby, K.W.; Coghill, C. Analysis of impersonation attacks on systems using {RF} fingerprinting and low-end receivers. *J. Comput. Syst. Sci.* **2014**, *80*, 591–601. [CrossRef]
18. Scanlon, P.; Kennedy, I.O.; Liu, Y. Feature extraction approaches to RF fingerprinting for device identification in femtocells. *Bell Labs Tech. J.* **2010**, *15*, 141–151. [CrossRef]
19. Baldini, G.; Steri, G.; Dimc, F.; Giuliani, R.; Kamnik, R. Experimental Identification of Smartphones Using Fingerprints of Built-In Micro-Electro Mechanical Systems (MEMS). *Sensors* **2016**, *16*, 818. [CrossRef] [PubMed]

20. Guo, Y.; Chen, X.; Wang, S.; Sun, R.; Zhao, Z. Wind Turbine Diagnosis under Variable Speed Conditions Using a Single Sensor Based on the Synchrosqueezing Transform Method. *Sensors* **2017**, *17*, 1149. [CrossRef]
21. Tary, J.B.; Herrera, R.H.; Han, J.; Baan, M. Spectral estimation—What is new? What is next? *Rev. Geophys.* **2014**, *52*, 723–749. [CrossRef]
22. Huang, N.E.; Shen, Z.; Long, S.R.; Wu, M.C.; Shih, H.H.; Zheng, Q.; Yen, N.C.; Tung, C.C.; Liu, H.H. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. Royal Society of London A: Mathematical, Physical and Engineering Sciences. *R. Soc.* **1998**, *454*, 903–995. [CrossRef]
23. Auger, F.; Flandrin, P.; Lin, Y.T.; McLaughlin, S.; Meignen, S.; Oberlin, T.; Wu, H.T. Time-frequency reassignment and synchrosqueezing: An overview. *IEEE Signal Process. Mag.* **2013**, *30*, 32–41. [CrossRef]
24. Chen, H.; Lu, L.; Xu, D.; Kang, J.; Chen, X. The Synchrosqueezing Algorithm Based on Generalized S-transform for High-Precision Time-Frequency Analysis. *Appl. Sci.* **2017**, *7*, 769. [CrossRef]
25. Daubechies, I.; Lu, J.; Wu, H.T. Synchrosqueezed wavelet transforms: An empirical mode decomposition-like tool. *Appl. Comput. Harmonic Anal.* **2011**, *30*, 243–261. [CrossRef]
26. Baldini, G.; Steri, G.; Giuliani, R.; Gentile, C. Imaging time series for internet of things radio frequency fingerprinting. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–6.
27. Reising, D.R.; Temple, M.A.; Jackson, J.A. Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1180–1192. [CrossRef]
28. Reising, D.R.; Temple, M.A.; Mendenhall, M.J. Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints. In Proceedings of the 2010 IEEE Wireless Communication and Networking Conference, Sydney, NSW, Australia, 18–21 April 2010; pp. 1–6. [CrossRef]
29. Cristianini, N.; Scholkopf, B. Support vector machines and kernel methods: the new generation of learning machines. *Ai Mag.* **2002**, *23*, 31.