Imaging Time Series for Internet of Things radio frequency fingerprinting

Gianmarco Baldini*†, Gary Steri*, Raimondo Giuliani*, Claudio Gentile†
* European Commission Joint Research Centre (JRC)
Via Enrico Fermi 2749, 21027 Ispra, Italy
† Università degli Studi dell'Insubria
Via Ravasi 2, 21100 Varese, Italy

***Abstract*—The concept of Radio Frequency (RF) fingerprinting is that electronic devices can be identified and authenticated through their radio frequency emissions, which contain intrinsic features of the device itself. RF fingerprinting can be used to enhance the security of wireless networks because the fingerprints provide a form of authentication. In previous research papers, the RF fingerprints have typically been obtained by extracting statistical features from the time series generated by the analog-to-digital conversion of the RF emissions. In this paper, we investigate a novel approach to the RF fingerprinting of Internet of Things (IOT) devices, where the time series are converted into images, out of which image processing features are extracted. The performance of this approach is experimentally evaluated by applying different machine learning algorithms on different types of conversions of time series to images. Our analysis shows that the proposed approach provides a better identification accuracy as compared to the accuracy achieved by conventional sets of statistical features used in the literature. Even if relatively small (around 1%), this accuracy improvement is statistically significant when classification is repeated over different folds of the training and test data. Yet, this enhanced accuracy is obtained at the cost of the longer time taken to process the images.**

I. Introduction

RF fingerprinting or Special Emitter Identification (SEI) concepts relate to the ability to identify and authenticate an electronic device through its RF emissions. The basic idea is that the small differences in the electronic circuits (e.g., due to different manufacturing plants or production chains) used for wireless transmission, generate small differences in the RF signal over the air. Even if these differences are not relevant enough to hamper the correct functioning of wireless services, they are significant enough to uniquely identify the model or the electronic device itself — see, e.g., the recent survey [1]. These differences can be typically identified for each device through the extraction of suitable statistical features of the time series. For example, the variance of the time series generated from the RF emissions can vary from one device to another, even after time series normalization. A common strategy for RF fingerprinting [2], [3] is thus to extract suitable statistical features from the RF signal, and then use appropriate machine learning algorithms to classify the obtained set of features so as to correlate them to the identity of the electronic device. For identification purposes, a supervised machine learning approach can be used, where a trained model is built from a known set of electronic devices and test samples are validated against the trained model to distinguish a specific electronic device from the others. The key challenge here is both the selection of predictive statistical features and the implementation and choice of parameters for the machine learning algorithms. There is an extensive literature on the problem of selecting statistical features, including variance, entropy, skewness, kurtosis, and others (e.g., [2], [3]). RF fingerprinting can be used to authenticate the electronic device, because the fingerprints are based on the physical properties of the RF circuits of the electronic device itself, which are not easy to be duplicated. To support authentication, it is important to have at one's disposal a classification algorithm which is able to distinguish between wireless devices of the same model and different serial numbers. Multi-factor authentication requires *intra-model* classification abilities, which is more difficult to achieve than *inter-model* classification, where wireless devices of different models are compared. Inter-model authentication is easier than intra-model authentication since different models have different designs and materials.

In this paper, we focus on the authentication of IoT wireless communication devices of the same model: nine nRF24LU1+ devices [4] used to implement IoT sensor networks. We are therefore addressing a more challenging intra-model classification task.

Our contribution. This paper adopts a novel approach to RF fingerprinting. Rather than applying the statistical features directly to the time series, as conventionally done in the literature on this subject (e.g., [3], [5]), the time series are first converted to images. The images are generated by calculating, in an iterative way, the distance between two points of the time series, starting from the beginning of the burst, for different number of samples. Three distances over complex numbers were adopted: Minkowski distance of order 2 (i.e., euclidean distance), Minkowski distance of order 3, and the Chebyshev distance. Then, standard image processing features like Histogram of Oriented Gradients (HOG), Binary Robust Invariant Scalable Keypoints (BRISK), Speeded-Up Robust Features (SURF), and Local Binary Pattern (LBP) are extracted from the resulting images. Different metrics are computed from the image processing features, as described in Section II. This approach is similar to the one followed in [6] for generic time series but, to the best of our knowledge, it has not

978-1-5386-1585-0/17/$31.00

been applied to RF fingerprinting, yet. In addition, in [6] the authors have applied various categories of image processing features, which is also not reported in the literature on RF fingerprinting. Here we show that this approach can indeed provide better classification accuracy as compared to more standard approaches relying on statistical features employed in the RF fingerprinting literature computed directly from the time series.

The structure of this paper is the following: Section II describes the test bed and how the RF signals from the IoT devices have been collected and processed. In the same section, it is presented the method we adopted to generate the time series, the way we transformed the time series to images, and also the way we computed image processing features on the images (e.g, HOG, BRISK and others). Section III reports our experimental evidence on the application of different supervised classification methods by comparing the overall accuracy obtained through standard statistical features applied to the time series to the accuracy achieved by image processing features applied to the images. Concluding remarks are contained in Section IV.

II. Methodology

A. Test Bed

In this section, we describe the IoT devices used in our experiment, and the methodology we followed to extract and process the RF signals, which are used as fingerprints of the wireless devices. We had at our disposal a set of 9 nRF24LU1+ devices used to implement wireless sensor networks for IoT applications. The number of devices used in the test bed is comparable with the number of devices (of the *same* model) used in literature: 9 ZigBee devices in [7], 8 Noise radars in [8] and 10 Zigbee devices in [9]. As described in [4], this wireless device is an Ultra Low Power (ULP) device transmitting for the 2.4GHz acISM band. The device includes a 2.4GHz RF transceiver core, 8-bit CPU, full-speed USB 2.0 device controller, and embedded Flash memory. These wireless devices have been programmed to build a MySensors network. MySensors is a free and open source DIY (do-it yourself) software framework for wireless Internet of Things (IoT) devices allowing devices to communicate through radio transmitters. A description of a wireless networks built with MySensors is provided in [10]. The RF signals transmitted by the wireless devices are collected using a low cost Universal Software Radio Peripheral (USRP) Software Defined Radio (SDR) receiver of type N210, equipped with a XCVR2450 front-end locked to the Global Positioning Systems (GPS) disciplined to 10 MHZ reference to ensure repeatability in the collection of RF observables [11]. The SDR receiver was equipped with a ublox NEO6Q GPS receiver. The RF signals were sampled by the SDR with a sampling rate of 5 msamples/sec.

B. Generation of the time series and related images

Our overall methodology, illustrated in Figure 1, consists of the following steps:

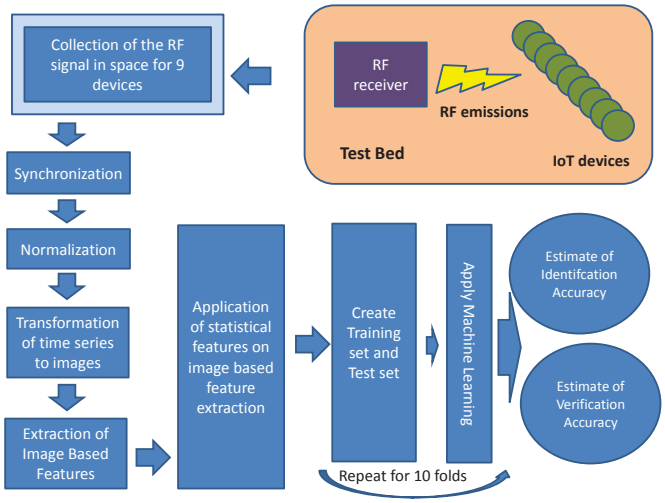
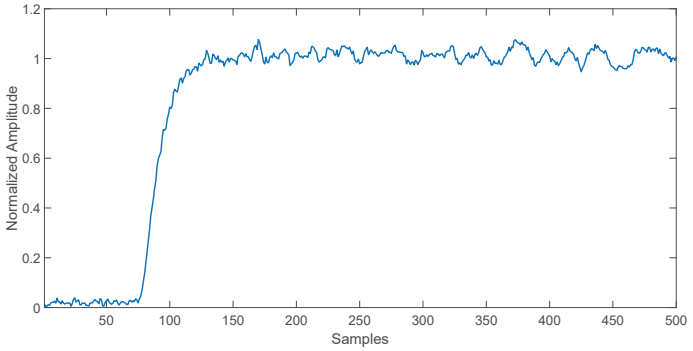


Fig. 1: Overall methodology.

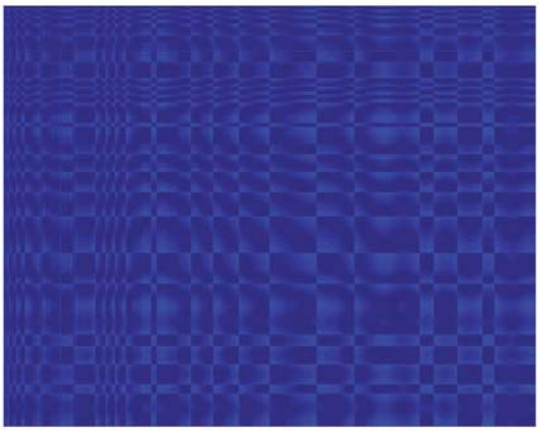
1) The 9 wireless devices were configured to transmit a fixed payload based on MySensors specifications with a data rate of 250 Kbit/sec.
2) The real-valued signal samples were sampled directly in In-phase and Quadrature components (IQ) format, and then synchronized and normalized offline to extract the burst of traffic associated with each payload. For each wireless device, a set of 900 packets were processed.
3) Rather than applying the statistical features directly to the time series as conventionally reported in the literature (e.g., [3], [5]), the time series are converted to images. The images are generated by calculating, in an iterative way, the distance between two points of the time series, starting from the beginning of the burst, and for different number of samples. Three different distances over complex numbers have been computed: Minkowski distance of order 2 (i.e., euclidean distance), Minkowski distance of order 3, and Chebyschev distance. An example of our time series-to-image transformation is shown in Figure 2, where we give the image created by the first 500 samples of the first burst of the first device after applying a Minkowski distance of order 3.
   This approach is somewhat similar to [6], though a different transformation is used here which turns out to be more effective for RF fingerprinting. The reason of the difference is that the time series used in this paper is actually the digital representation of a modulated RF signal, where both the modulus and the phase of the signal carry specific digital information.
4) The transformation from time series to image can be a time consuming process (as described in Section III). In this specific case, the time series for each burst is quite long (7112 samples) and it would not be practical to transform the entire time series to images. Only specific portions of the time series are used for imaging; for instance, the ramp section of a RF burst is typically more

useful for RF fingerprinting [5]. The specific portions we considered here include at least the first ramp or both ramps (ramp up and ramp down). More specifically, the sections of the bursts that we used for fingerprinting are the following: a) The first 100 samples with the ramp up burst, b) the first 200 samples with the ramp up burst, c) the first 500 samples with the ramp up burst, d) the first 800 samples with the ramp up burst, and e) a time series made up of the ramp up and the ramp down. As shown in Section III, as we increase the length of the burst section we achieve a higher classification accuracy, at the cost of a higher computational burden.

5) Unlike [6], where a deep learning approach is used, in this paper we adopt an image-based approach, where different image processing features are applied to the images, including HOG, BRISK, SURF and LBP. These features are themselves the result of a selection process from a wider set of image-based features, where the set of features used in this paper provided the best identification accuracy. For example, other features based on Maximally Stable Extremal Regions (MSER) and Features from Accelerated Segment Test (FAST) were also taken in consideration in a preliminary stage of our experiments, but soon discarded, for their cross-validated accuracy performance turned out to be relatively poor. In this paper we present only the results for the image-based features exhibiting the best classification accuracy. The feature extraction is performed in two steps: in the first step, the image-based features are extracted from the image. Rather than single numeric values (e.g., number of corners of the image), most of the image-based features provide histograms or arrays of numeric values for each of the cell values to which the statistical feature is applied. For example, The HOG feature is based on a cell size of 120*120 pixels. A potential extension of this paper may include the HOG cell size as an additional degree of freedom of our experimental analysis. In the second step, new statistical features are calculated on the histograms and arrays generated from the image-based features. A set of 32 statistical features was created as defined in Table I for 900 payloads and 9 devices amounting to a total of 8100 samples.
6) On the final set of 32 features, Principal Component Analysis (PCA) was applied so as to further reduce feature dimensionality and/or improve accuracy. Comparative results on using different sets of features are presented in Section III.
7) Different machine learning algorithms were applied to the statistical features, specifically: Support Vector Machines (SVM) with Gaussian kernels, K-Nearest Neighbor (KNN) with Euclidean distance, and Decision Trees. In order to evaluate the resulting accuracy, a 10-fold cross-validation method was adopted. The optimal parameter values for the SVM algorithm have been computed separately with a grid search scheme, and turned out to be as follows: scaling factor = 2^7, box constraint = 2^{14}. Different values have also been considered for K in the KNN algorithm (see Section III). For the Decision Trees, the optimization parameter is the Maximum number of decision splits or branch nodes per tree.
8) Evaluation Metrics. A set of tools was used to quantify classification accuracy: confusion matrix, Receiver Operative Characteristics (ROC), and Equal Error Rate (EER). In the confusion matrix, each column represents the instances in the predicted class while each row represents the instances in the actual class. The sum of the diagonal entries divided by the sum of all entries of the matrix provides the overall accuracy of the classification method at hand. The ROC is generated here by plotting the true positive rate against the false positive rate as the verification threshold changes. The point where the two rates have the same value is the EER (the EER on the X-axis is used). In general, a lower EER indicates a higher verification accuracy.



(a) Original Time Series with 500 samples



(b) Transformed image using Minkowski distance of order 3 and 500 samples

Fig. 2: Transformation of the initial section of the time series (a) to an image (b).

Feature Id	Description of the feature
1	Root Mean Square (RMS) of the HOG features.
2	Variance of the HOG features .
3	Shannon Entropy of the HOG features.
4	Log Entropy of the HOG features.
5	RMS of the LBP features.
6	Variance of the LBP features.
7	Shannon Entropy of the LBP features.
8	Log Entropy of the LBP features.
9	RMS of the BRISK features. Strength at which the BRISK feature is detected.
10	Variance of the BRISK features. Strength at which the BRISK feature is detected.
11	Shannon Entropy of the BRISK features. Strength at which the BRISK feature is detected.
12	Log Entropy of the BRISK features. Strength at which the BRISK feature is detected.
13	RMS of the BRISK features. Scale at which the BRISK feature is detected.
14	Variance of the BRISK features. Scale at which the BRISK feature is detected.
15	Shannon Entropy of the BRISK features. Scale at which the BRISK feature is detected.
16	Log Entropy of the BRISK features. Scale at which the BRISK feature is detected.
17	RMS of the SURF features. Strength at which the SURF feature is detected.
18	Variance of the SURF features. Strength at which the SURF feature is detected.
19	Shannon Entropy of the SURF features. Strength at which the SURF feature is detected.
20	Log Entropy of the SURF features. Strength at which the SURF feature is detected.
21	RMS of the SURF features. Scale at which the SURF feature is detected.
22	Variance of the SURF features. Scale at which the SURF feature is detected.
23	Shannon Entropy of the SURF features. Scale at which the SURF feature is detected.
24	Log Entropy of the SURF features. Scale at which the SURF feature is detected.
25	Maximum value of the histogram of the HOG features.
26	Variance of the histogram of the HOG features.
27	Maximum value of the histogram of the LBP features.
28	Variance of the histogram of the LBP features.
29	Maximum value of the histogram of the BRISK features.
30	Variance of the histogram of the BRISK features.
31	Maximum value of the histogram of the SURF features.
32	Variance of the histogram of the SURF features.

TABLE I: Statistical features used for identification and verification purposes.

III. Results

In this section, we provide the results of classification for different machine learning algorithms over training samples of different size.

A. Identification results

In this subsection we report the results obtained by applying the SVM machine learning algorithm. Because SVM is traditionally designed as a binary classifier, a one-vs-one approach was used to adapt it to the multiclass classification problem over the 9 IoT devices of our experiment.

The first two parameters we considered to optimize identification accuracy are the number of samples and the distance used to generate images. Figure 3 contains the bar chart of the overall 10-fold cross-validation accuracy against the number of samples for the three distance functions considered here, after using PCA on the 32 features of Table I. PCA is applied to the training set before the application of the machine learning algorithm. From this plot, it is clear that the highest accuracy is obtained on images generated by the first 500 samples of the time series, with a slightly higher accuracy achieved when using Minkowsky distance of order 3. See also table V with the reported values for some of the combinations.

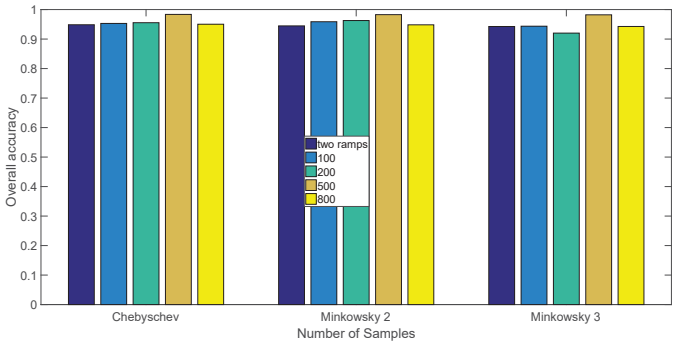


Fig. 3: Graphical comparison of results of the overall accuracy when using different sets of distances and different number of samples.

The selection of features is itself part of the optimization process. To give an idea, Table II compares the overall identification accuracy obtained by PCA to the one achieved by selected sets of features on the images generated by 500 samples through the Minkowsky distance of order 3.

Features	Overall Accuracy
PCA (all features)	0.9836
HOG based features	0.8009
LBP based features	0.6879
BRISK based features	0.7979
SURF based features	0.69

TABLE II: Overall accuracy results for PCA and selected sets of features on images generated by 500 samples via Minkowsky distance of order 3.

From Table II, we can see that the HOG and BRISK sets of features provide a good accuracy but, in fact, it is only the contribution from all sets of features that provides the very high identification accuracy (98.36 %) which makes our method suitable for multi-factor authentication in security related applications.

On the basis of the previous results, we report in Table III the confusion matrix for the images obtained by Minkowski distance of order 3 over the first 500 samples with PCA.

B. Verification results

In this section, we present the results for the verification accuracy of an IoT device against another. Only the features derived from PCA have been used here. Verification accuracy is an important aspect in multi-factor authentication, where

	IOT1	IOT2	IOT3	IOT4	IOT5	IOT6	IOT7	IOT8	IOT9
IOT1	900	0	0	0	0	0	0	0	0
IOT2	0	897	3	0	0	0	0	0	0
IOT3	0	10	890	0	0	0	0	0	0
IOT4	0	3	11	880	6	0	0	0	0
IOT5	0	0	0	5	868	2	0	0	25
IOT6	0	0	0	0	0	879	8	0	13
IOT7	0	0	0	0	0	7	888	0	5
IOT8	0	0	0	0	0	0	0	900	1
IOT9	0	0	0	0	14	15	6	0	865

TABLE III: Confusion Matrix obtained by SVM on the images based on 500 samples and Minkowski distance of order 3. PCA was applied before feeding the SVM. Here, IOTX denotes the X-th IoT device (e.g., IOT3 is the third device out of 9).

RF fingerprinting can be used to verify that IoT device A is indeed device A and not a rogue IoT device, which is impersonating device A. In this case, this takes the form of a binary classification problem and the verification accuracy can be evaluated using EER. Table IV shows the EER averaged across all possible combinations of the IoT devices against each other for different sizes and different distance criteria. In fact, these results confirm the previous results on identification accuracy (Section III-A), where the combination of size 500 and Minkowsky distance of order 3 yielded the best results (lowest EER). We also observe that these results are related to the specific type of RF equipment (the mySensor devices) used in this test-setup.

Type of distance	Size	**Average EER**
Minkowski order 2	(size 800)	0.0263
Minkowski order 3	(size 500)	0.0081
Minkowski order 3	(size 100)	0.0246
Chebyschev	(size 100)	0.0201

TABLE IV: Verification accuracy results measured by the average EER metric applied to different types of distances and different number of samples.

C. Comparison with different machine learning algorithms

The identification accuracy was evaluated by means of different machine learning algorithms: SVM (already reported in Section III-A), KNN, and Decision Trees across different sizes of the burst portion and types of distances. For each machine learning algorithm, the identification accuracy is given only for the optimal value of their parameters (in braces). The results are contained in Table V, where we can see that SVM's performance is superior to the one of the other two algorithms considered here. Again, only the features derived from PCA have been used for this comparison.

The values in parenthesis are the optimal values for the KNN and decision tree.

D. Comparison with conventional statistical features applied to the time series

Finally, we have compared the results of the proposed image approach to conventional statistical features used for RF fingerprinting, which are shown in Table VI. These features are derived from the literature (e.g [5], [12], [13]. The permutation entropy is computed with a parameter called Embedding dimensions (D). In this paper, we have used the embedding dimensions values equal to 4 and 5, which were used by the authors in [13]. The first 500 samples of the IoT bursts were chosen, because this provided the best overall accuracy not only for the image based approach but also for the approach based on the statistical features.

Algorithm	**Machine Learning Algorithm**	**Overall Accuracy**
Minkowski order 3 (size 500)	SVM	0.9836
Minkowski order 3 (size 500)	KNN(6)	0.9343
Minkowski order 3 (size 500)	Decision Tree(20)	0.8658
Minkowski order 2 (size 800)	SVM	0.9483
Minkowski order 2 (size 800)	KNN(6)	0.8899
Minkowski order 2 (size 800)	Decision Tree(20)	0.8240
Chebyschev (size 200)	SVM	0.9202
Chebyschev (size 200)	KNN(6)	0.9088
Chebyschev (size 200)	Decision Tree(20)	0.8148

TABLE V: Overall accuracy results achieved by different machine learning algorithms, types of distance and samples numbers.

Feature Id	Feature (amplitude in time)	Feature Id	Feature (phase in time)
T1	Variance (amplitude)	T8	Variance (phase)
T2	Skewness (amplitude)	T9	Skewness (phase)
T3	Kurtosis (amplitude)	T10	Kurtosis (phase)
T4	Shannon Entropy (amplitude)	T11	Shannon Entropy (phase)
T5	Log energy entropy (amplitude)	T12	Log energy entropy (phase)
T6	Permutation entropy with D=4 (amplitude)	T13	Permutation entropy with D=4 (phase)
T7	Permutation entropy with D=5 (amplitude)	T14	Permutation entropy with D=5 (phase)

TABLE VI: Statistical features used for RF fingerprinting from the literature.

Figure 4 compares the overall accuracy calculated with the image processing approach (green line) to the one obtained by the conventional features (red line). In both cases, we used a parameter-optimized SVM on top of PCA. The optimized SVM parameters (i.e., scaling factor and box constraint) for the images have been provided before. For the conventional features, the optimized SVM parameters were scaling factor equal to 2^4 and box constraint equal to 2^{16}. The accuracy was computed over different 50 random folds to ensure statistical significance of the comparison of the two approaches. From figure 4, we can see that the image processing approach outperforms the conventional one in the large majority of the folds, as well as on average over the folds (dashed lines). A more fine-grained comparison delivered by a Wilcoxon signed rank test [14] reveals that the null hypothesis that the 50

accuracy difference values come from a distribution having zero median has p-value less than 0.001, thereby supporting the claim that the image features are indeed superior to the conventional features, the difference being statistically significant.

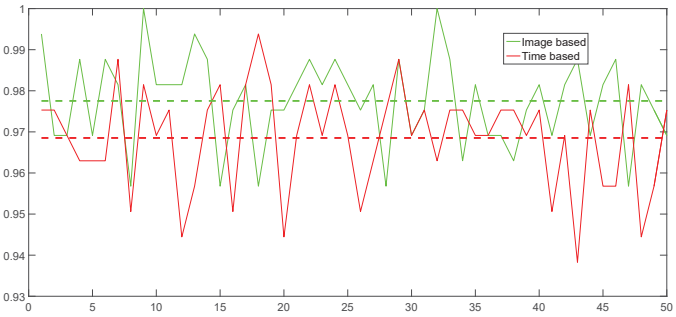


Fig. 4: Comparison between the image based approach and the conventional feature approach on 50 folds. Dashed lines give the average overall accuracy of the two approaches over the 50 folds.

The price we pay for this improved accuracy is the longer time needed to convert the time series into images and then extracting the image-based features. The slowdown of the image-based approach compared to the conventional one is around a factor of 30. While this difference is indeed significant, it is worth saying that the overall time for converting a time series to an image and extracting the associated features is still in the order of a 1-2 seconds.

IV. Conclusions

In this paper, we have investigated a novel approach to RF fingerprinting where the collected time series are converted to images out of which suitable image-based features are extracted. The extracted features are then used to perform the identification and the verification tasks. A number of free parameters are available in this approach: the size of the time series to be turned to images, the type of transformation from time series to images, the type of image-based statistical features, and so on. This paper has presented a first experimental analysis for some of these parameters, for both identification and verification purposes. The overall identification accuracy we reported with this approach is quite high (98.36 %), which supports the application of RF fingerprinting to multi-factor authentication in security-based applications. In particular, the overall accuracy obtained through the image-based features turned out to be higher than the one achieved by more conventional features taken from the existing literature. The price we pay is the longer time required to perform the conversion of time series to images.

Future developments of this line of research will investigate the application of deep learning techniques to the images generated from the time series, and the evaluation of identification accuracy in the presence of noise and fading effects.

Acknowledgment

This work was done in the context of the ARMOUR project Grant id 688237 of the Horizon 2020 Call ICT-12-2015 Integrating experiments and facilities in FIRE+. The authors would like to thank David Shaw from the European Commission Joint Research Centre for the technical support.

References

[1] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 94–104, Firstquarter 2016.

[2] R. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity analysis of burst detection and RF fingerprinting classification performance," in *2009 IEEE International Conference on Communications*, June 2009, pp. 1–5.

[3] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[4] N. Semiconductors, "nrf24lu1+," http://www.nordicsemi.com, 2016, [Online accessed 22-December-2016].

[5] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK-based devices using rf fingerprinting," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 1, pp. 41–59, 2010.

[6] Z. Wang and T. Oates, "Imaging time-series to improve classification and imputation," in *Proceedings of the 24th International Conference on Artificial Intelligence*, ser. IJCAI'15. AAAI Press, 2015, pp. 3939–3945. [Online]. Available: http://dl.acm.org/citation.cfm?id=2832747.2832798

[7] C. K. Dubendorfer, B. W. Ramsey, and M. A. Temple, "An RF-DNA verification process for Zigbee networks," in *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*. IEEE, 2012, pp. 1–6.

[8] M. Lukacs, P. Collins, and M. Temple, "Device identification using active noise interrogation and RF-DNA "fingerprinting" for non-destructive amplifier acceptance testing," in *2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, April 2016, pp. 1–6.

[9] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1862–1874, Aug 2016.

[10] A. D. Nisio, T. D. Noia, C. G. C. Carducci, and M. Spadavecchia, "Design of a low cost multipurpose wireless sensor network," in *2015 IEEE International Workshop on Measurements Networking (M N)*, Oct 2015, pp. 1–6.

[11] Ettus Research, "USRP N200 N210 Networked series specifications," 2016, [Online accessed 22-December-2016]. [Online]. Available: https://www.ettus.com/

[12] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced rf-dna fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180–1192, June 2015.

[13] G. Huang, Y. Yuan, X. Wang, and Z. Huang, "Specific emitter identification based on nonlinear dynamical characteristics," *Canadian Journal of Electrical and Computer Engineering*, vol. 39, no. 1, pp. 34–41, winter 2016.

[14] J. D. Gibbons and S. Chakraborti, *Nonparametric statistical inference*. Springer, 2011.