Characterization of a Connected Object by Its Acoustic Signature

François Bouchaud, Thomas Vantroys, A. Boé

Characterization of a Connected Object by Its Acoustic Signature

François Bouchaud[1], Thomas Vantroys[2,4], and Alexandre Boe[3,4]

[1] C3N - National cyber-crime unit
Gendarmerie Nationale
francois.bouchaud@gendarmerie.interieur.gouv.fr
[2] Univ. Lille, CNRS, Centrale Lille, UMR 9189 - CRIStAL F-59000 Lille, France
thomas.vantroys@univ-lille.fr
[3] Univ. Lille, CNRS, Centrale Lille, Univ. Polytechnique Hauts-de-France, UMR 8520 - IEMN F-59000 Lille, France
alexandre.boe@univ-lille.fr
[4] Univ. Lille, CNRS, USR 3380 - IRCICA, F-59000 Lille, France

Abstract. With the proliferation of connected objects, the fine identification and the technical characterization of digital devices are one challenge for the monitoring and security of information systems. Connected objects are of different types, and each has different characteristics, whether it is the embedded operating system, their sensors or their firmware version. Connected objets are difficult to identify by non-expert. The activity of a microcontroller generates a set of physical phenomena that can be quantified, observed and exploited. The acoustic emissions resulting from this activity are quantifiable and have been proven to be a formidable means of discrimination and qualification of electronic equipments. In this paper, we present our prelimary work on generating "digital fingerprint" of connected objects by exploiting the emitted acoustic emissions to automatically categorize the devices.

Keywords: Internet of Things · Identification · Acoustic fingerprinting · Signature · Side-channel attack

1 Introduction

With an estimated average annual growth rate of 11.3% between 2020 and 2024 by International Data Corporation (IDC) [1], the Internet of Things (IoT) market is in full boom. This attractive sector is a significant vector of economic growth and innovation. The IoT opens up new perspectives on the interconnection of people and goods with intelligence: home automation and access control, wearable, connected health, industrial applications and network management, transportation, environmental and energy monitoring, etc. The structuring of information systems is based on connected objects, which can communicate with the outside world via gateways, but also directly with each other. The access points are generally local: at the scale of a house or a factory. This partially decentralized network is mobile and flexible, depending on the services provided.

This transformation is amplified by the phenomena *makers kit* and *Do-It-Yourself*. The physical world is becoming connected through the use of communication devices. For example, STMicroelectronics has recently released an evaluation board to integrate voice interaction into connected objects using the Alexa voice service developed by Amazon. This hardware is more flexible and versatile in terms of use and configuration.

As soon as we start to depict some scenarios for studying connected objects, we realize that, given the diversity of objects and protocols used, there is no universal approach to accessing to data. It is therefore imperative to know what a connected object is and how it works in order to be able to harvest information from it and, if necessary, to decide on a strategy to capture and access this internal data. Given the diversity of devices on the market, it is impossible to know in advance how all connected objects will work. Visual recognition of devices suffers from limitations due to the absence of distinguishing features or similarity in shape. The phenomenon is amplified by the wide variety of objects, spread across various application areas, the lack of information about protocols, proprietary designs, and the misuse of innate solutions or features. As an example the energy optimization solution that, depending on the services chosen, is able to integrate an acoustic sensor to characterize a sound level and therefore a presence. The time, financial and human dimensions of the study of connected objects are added to these difficulties. To overcome this problem, it is necessary to develop fine identification techniques dedicated to connected equipments, based on known characteristics, common to these objects, and/or derivable from one object to another. These tools must be robust, reliable and economic.

This article presents a preliminary work on the identification of a connected object by studying its acoustic emissions. This solution is all the more relevant as it does not involve any interaction and/or modification of the connected objects. The measurement is carried out at the periphery of the material, without prior knowledge of the environment to be studied.

Section 2 of this article summarizes previous works in the field of acoustic emissions of an electronic device; Section 3 describes the acquisition chain of sound emissions; Section 4 presents various acoustic measurements of electronic devices; Section 5 proposes the automation of the study of the signature and identification of connected objects; Section 6 presents the application domains of the solution and discusses the uses. Finally Section 7 provides the conclusion of the paper and the next step in the research.

2 Related Works

Emissions from electronic equipment have long been a concern for the security and privacy science community [2]. Acoustic emissions are side-channels. They betray information about the electronic system. They are also used to steal secret data or to interact with the system during offensive actions. There are many sound sources that can be exploited in a computer environment, such as listening

to keyboards or printers [3–5], the mechanical noise of fans, or the read/write head of a hard drive. For example, researchers have shown that acoustic emanations from dot-matrix printers contain important information about the printed text. Research has also focused on the emission of sounds from production units such as 3D printers [6], or more globally from connected factories [7, 8]. This approach assumes that the sounds carry information about the process that can be exploited in the reverse engineering of the system, without needing to access to the original design.

There are also scientific contributions on computer noise coming from the passage of electric current in electronic components [9]. This emanation takes the form of perceptible vibrations in the form of a low-pitched sound or a hissing noise commonly called "coil whine", although often generated by capacitors. These acoustic emanations, usually caused by voltage regulation circuits, are correlated to the system activity, since the modern processors radically modify their power consumption according to the type of operations performed [10, 11]. However, the bandwidth of these signals is very low: limited to 20 kHz for audible signals measurable by conventional microphones, and up to 200 kHz with ultrasound microphones. Beyond these frequencies, the attenuation in the air and the reduced sensitivity of the microphones make the signals undetectable. The study of the signals should allow us to discriminate a device, to recognize its activity rate and to characterize it. The operations of the processors being of the order of the kHz are not observable in the state. This information is drowned in the noise of 300 kHz. The study of acoustic emissions also has industrial applications in the context of the performance of existing solutions, the quality approach and the verification of equipment.

The fingerprinting of connected objects can also be realized based on the radiofrequency communication [12–14]

Our goal is to generate "digital fingerprint" of connected objects in order to simplify the work of forensics investigator. We investigate the use of accoustic signature because it can be easily realized on the field. As we want to test this method during legal forensic investigation, we also need to have a method who doesn't need radio communication. We have to ensured that no interaction is done between the connected objects and the Internet.

3 Experimental Configuration

The measurement environment consists in a robust data acquisition and processing chain deployed in a controlled environment. This chain is based on economic and easily transportable solutions.

3.1 Measuring Chain

The specifications of the sound measurement acquisition chain are conditioned by the needs of robustness, adaptability to the environment and low cost. For the experiments, we capture the acoustic noise of various communicating devices

using a microphone *BEHRINGER ECM8000* (effective up to about 98 kHz, well beyond its nominal range of 20 kHz). This equipment has a very linear frequency response. For the power supply and amplification, it is connected to a *STEINBERG UR12*. The amplified signal of this acquisition chain is digitized at a sampling frequency of 192 kHz (Fig. 1).

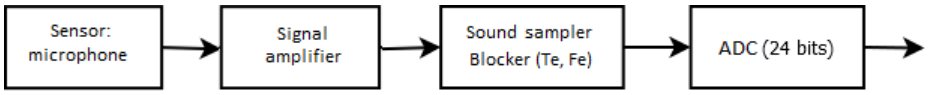

Fig. 1. Acquisition chain for sound measurement

The audio signal processing is done with a Rasberry Pi. The acquisition of the measurements is based on the Library *PyAudio* of Python. The spectrograms of these signals are drawn using the *spectrogram* function of the *SciPy* library and by custom scripts. These developments offer a modification of the resolution of the results such as the time allocated to each fast Fourier transform (FFT) with their interleaving rate, the frequency ranges to analyze or the values to return.

3.2 Noise attenuation

In order to limit the external noises and to absorb the sound waves to avoid any reflection, an acoustic anechoic chamber has been designed (Fig. 2). This solution reproduces quasi free field conditions and absorbs the echo that can disturb the measurements. With a dimension of 560x560x310 mm, this box is covered with dihedral polymer foam. This acquisition environment is also isolated from external vibrations by an appropriate support.

The attenuation of the box has been characterized by the measurement of an external frequency variable sound source(Fig. 3). The graph represents the noise attenuation (dB) as a function of frequency (Hz). The results are consistent with the properties of the polymer used to attenuate the noise. A script is used to provide a correction to the further measurements.

The acoustic anechoic chamber embbeds only the measurement microphones. The other elements of the acquisition chain are outside in order to limit the disturbance to the measurements. A second microphone has been added to record the ambient noise. The data are subtracted from the main measurement during processing in order to cancel the punctual noise coming from outside. The Fig. 4 show the noise cancellation. The top graphs are made for a sound measurement of a charger and the bottom ones for a sound measurement of a board of *STM32F769I-DISCO* from *STMicroelectronics*. This operation makes it possible to remove a parasitic frequency around 64 kHz. We also observe an improvement of the low and medium frequencies.

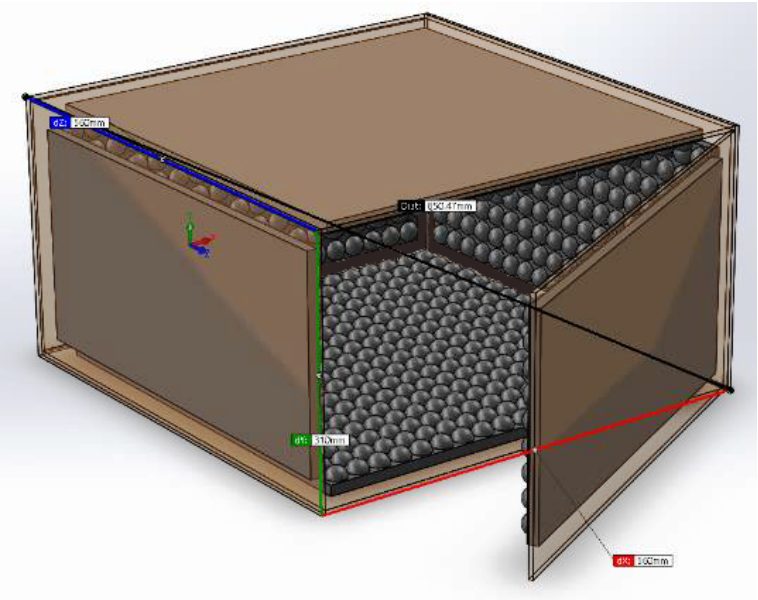

Fig. 2. Modeling of acoustic anechoic chamber

4 Measurement of the acoustic emissions of an electronic device

The series of measurements allows us to check the acoustic properties of an electronic equipment. We try to verify several hypotheses on the differentiation of materials and their behavior.

4.1 Experiments on different connected equipments

Different measurements have been done on cell phone chargers including a Motorola Moto G5 Plus (phone number 1), a Samsung Galaxy S4 mini (phone number 2), and a commercial microcontroller board *STM32F769I-DISCO*. This work should allow us to validate our measurement environment and to demonstrate the possibility to classify the objects by the sound emitted during the electrical charge. For this experiment, a single cell phone charger has been used to power the three devices. The cell phones have been configured as follow: standby mode, airplane mode enabled. Airplane mode is a setting that cuts off all network connections. However, this action leaves free access to softwares, and functions that do not need to be connected. We note that the sound emitted by the charger allows to differentiate between different objects (Fig. 5). We also observe that the noise from a vacuum charger is not distinctly reflected in the noise from a phone charging device or a disco card. The Disco Card noise recording contains a continuous signal around the same frequency, unlike the non-linear

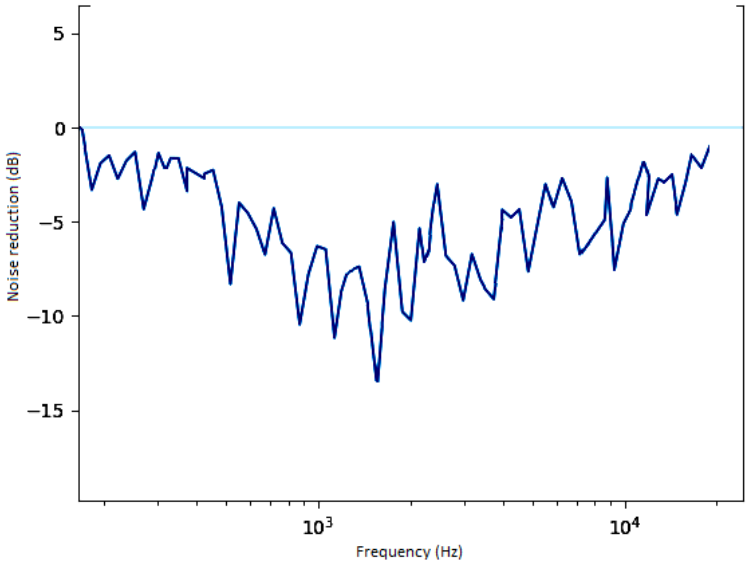

Fig. 3. Frequency characterization of the acoustic insulation of the box

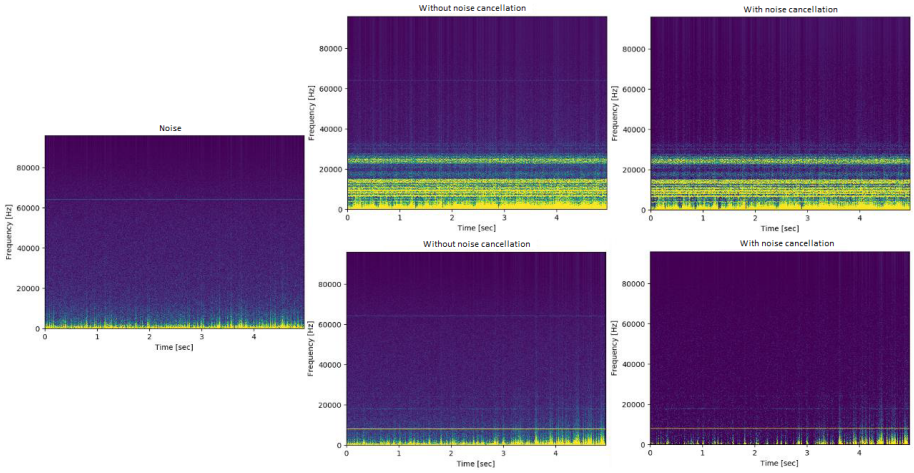

Fig. 4. Spectrograms of noise (left graphic), raw measurements on a cell phone charger (middle top) and on a microcontroller board (middle bottom), on right the same measurements after noise cancellation

recordings associated with phones 1 and 2. This observation can be explained by the type of power supply of the studied equipment. The Disco Card has an equal consumption on the regulator. The cell phones have in addition to a regulator, a charging circuit with a battery. We also observe the presence of an activity dur-

ing the measurement of the different equipment, without being able to qualify it.

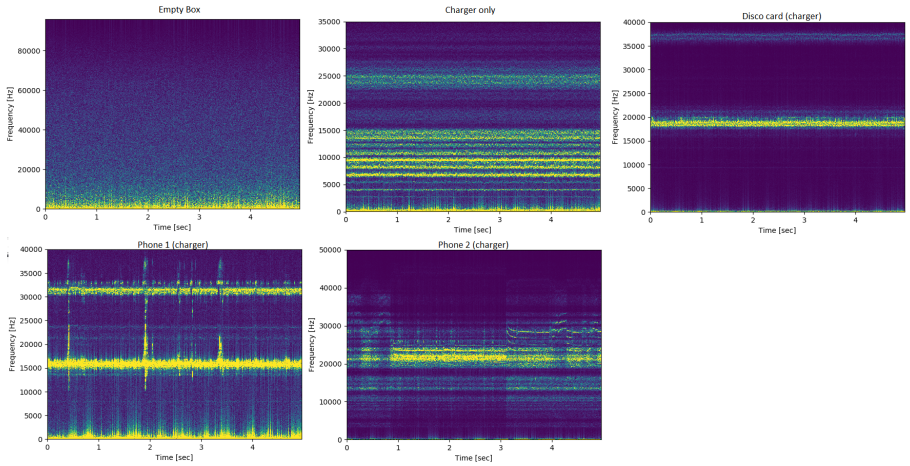

Fig. 5. Spectrograms (from top left to bottom right) of the empty chamber, the cell phone charger alone (not plugged in), microcontroller board, cell phone 1, and cell phone 2

4.2 Classification by activity of the device

The second experiments consist in demonstrating that the activity of device can be detected by measuring the acoustic emanations (Fig. 6). The measurements were carried out on the Motorola Moto G5 Plus (phone number 1). The cell phone were subjected to differents conditions using home made Android applications: 100 000 000 incrementations of a variable, and the calculation of the first 5000 prime numbers. These operations are triggered by pressing a button in our mobile application. We perform successive measurements with the airplane mode on, and with the airplane mode off. The launch of the computational operations is measured and symbolized by a frequency peak on the graphs. We notice a clear difference between the phases of activity during the calculations and the rest. Depending on the calculation performed, we can distinguish different periods of activity within the same block. In the case of the incrementation of a variable, we observe a rather regular signal. This instruction calls for a single type of operation. Conversely, the calculation of a prime number requires several types of operations and therefore the activation of several microprocessor circuits. This operation is carried out on a block of 1 second 80 with different phases of calculation. Disabling airplane mode reveals many frequency spikes related to network connections. This synchronization generates significant power consumption spikes. It is difficult to characterize precisely and visually a typical

pattern related to a calculation operation. The multi-core processor of our phone is capable of performing several tasks in parallel, which may affect the result of our measurement.

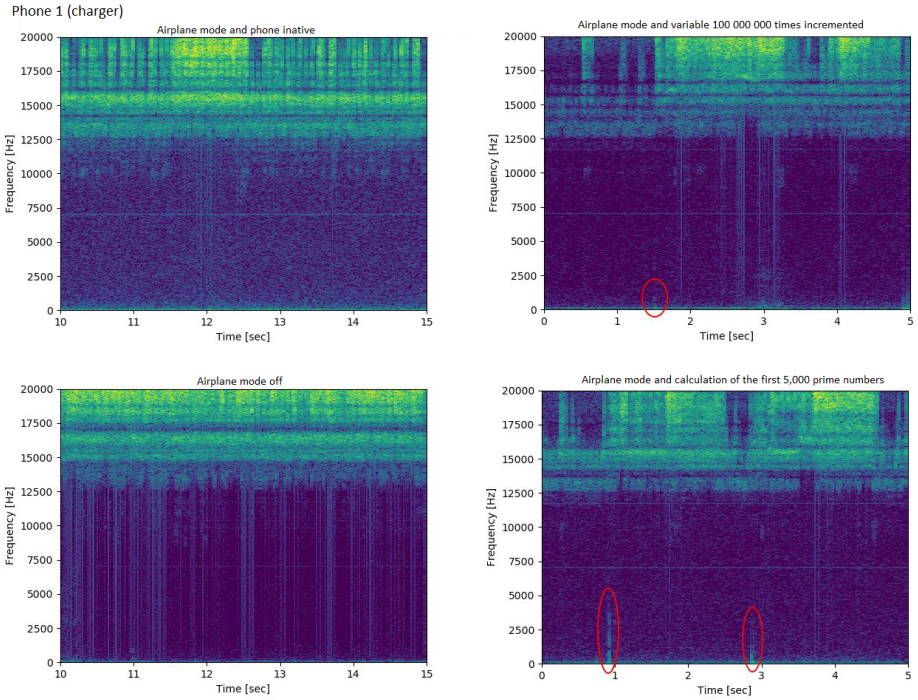

Fig. 6. Spectrograms (from top left to bottom right) of the phone 1 in quiet conditions and airplane mode enabled; variable incrementation and airplane mode enabled; quiet conditions and airplane mode disabled; calculation of prime numbers and airplane mode enabled

A third set of measurements was conducted to determine and qualify the activity of a device by measuring the sound emanations at the board level, and not at the cell phone charger level. Our measurements were carried out on the board *STM32F769I-DISCO* from *STMicroelectronics*. This board embeds a microcontroller *STM32F769NIH6* based on the 32-bits ARM Cortex-M7 core and a LCD screen. Several screen configurations are evaluated: the home mode, the demonstration mode without animation, and the demonstration mode with animations integrating real time calculations. The results returned by our acquisition chain do not allow us to detect a particular state of the object or a characteristic pattern linked to an activity (Fig. 7). However, we notice that the recorded signals are not identical. This reading difficulty can be explained by the technical limitations of the acquisition chain equipment, mainly the limited sensitivity. For the same reasons, we were not able to further qualify the differentiation of two

equipment with identical configurations (brand, models and operating system). Moreover, the electronic board emits only a weak audible and visible sound, unlike its control circuit. The laboratory equipment proposed by Genkin et al. [15] or a solution based on a Laser Doppler Vibrometer could provide the beginning of an answer to this question. The visual approach can also be coupled with a mathematical study for the detection of repetitive characteristic elements and the identification of significant patterns invisible to the human eye.

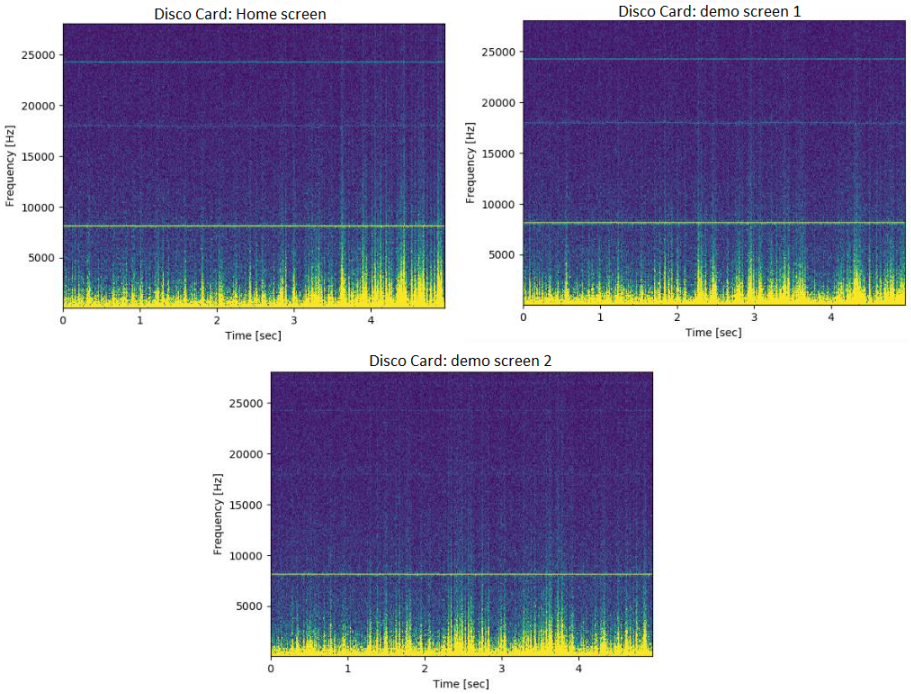

Fig. 7. Spectrogram of the sound emission of a Disco board with LCD screen displaying the home screen (top left), demo screen 1 (top right), and demo screen 2 with real time effects (bottom)

5 Automatic classification and identification

The acoustic measurements of the same cell phone charger connected to several equipments show different signal traces, allowing to discriminate them (measure 1). On the other hand, we are not able to visually characterize the activities on an electronic device (measures 2 and 3). In this section, an automatic classification of devices, based on their sound signature, is described. The classification is done in two steps: first a principal component analysis (PCA) reduction is applied, and

secondly a support vector machine (SVM) classification allows to differentiate the devices.

5.1 Principal Component Analysis

Principal Component Analysis (PCA) is a descriptive method used to explore multivariate data.This mathematical approach provides a graphical representation of the information contained in a table of quantitative data. A table with n dimensions gives n principal components. These new variables correspond to a linear combination of the original variables. The objective of this method is to identify the principal components around which the variation of the data is maximal.

The mathematical approach can be modeled according to the following process (Fig. 8).

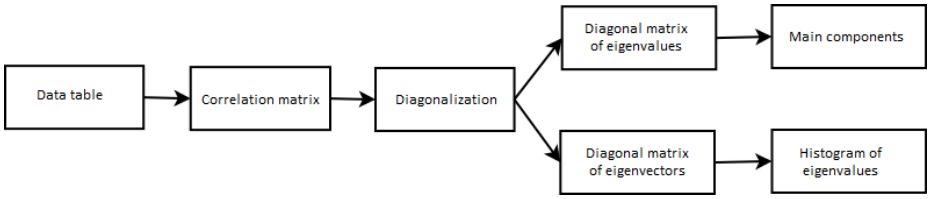

Fig. 8. Principal Component Analysis

5.2 Support Vector Machine

Support vector machines or wide margin separators are a class of learning algorithms, applicable to the classification of linear data. They determine the boundary between categories from the training data. After the learning phase, they make a prediction of the category to which the encountered input belongs. This process is automatically performed. The classification of the measurements is done in Python, using the libraries *numpy*, *sklearn*, *matplotlib*, and *customSpectrogram*.

5.3 Automatic classification of measurements

To train the SVM, we perform a series of acoustic measurements on a *Motorola Moto G5 Plus* (Android 9 and *ROM* : AOSPExtended Pie) and a *Samsung Galaxy S4 Mini* (Android 6.0.1 and *ROM* : CyanogenMod 13). We develop an Android application that performs mathematical operations over a long period of time: increments on a variable, multiplications, and logical test (if condition). To avoid the Android system considers the loop as infinite and kills the process, some periodic pause periods were included. The learning phase involved 87 audio

files and led to the creation of 8 categories. Each measurement is indicated by a colored dot

The Fig. 9 shows the PCA without SVM and with SVM as a function of several kernels: linear, radial and polynomial. The measurements taken allow us to identify each piece of equipment separately. For each equipment, we are also able to differentiate a mathematical operation. This result allows us to confirm the hypothesis of a discrimination of equipment and its operating state.

We find that no algorithm can categorize the mathematical operations of multiplication and the logical test (if condition) for the Motorola Moto G5 Plus. The measurements are grouped under one set. However, we are able to separate them visually. This may be due to the small volume of representative measurements or a software error. The linear method contains 6 measurement errors out of 87 measurements made, for an error rate of 6.9%. The radial and polynomial methods contain 4 measurement errors out of 87 measurements made, or an error rate of 4.6%.

The boundary between the categories can be refined by increasing the amount of training data. The linear method, which is less resource and computationally intensive, can be preferred.

6 Discussion

This sound measurement and characterization process can be used to quickly determine if a connected object complies with design recommendations. Sound measurement can be performed by a manufacturer or service provider throughout the product lifecycle: as part of a production quality audit, during a compliance test or during troubleshooting. The measurement allows to ensure that there are no modifications on the object, the correct version of firmware is embedded, or the object remains in nominal operation, in particular for maintenance and follow-up phase. This practice is all the more relevant with the intervention of many actors, in the case of outsourcing of services to benefit from a common reference of control, to proceed to random checks in any place and at any time.

The sound identification process is also relevant in the context of digital forensics. For example, connected objects encountered by forensic investigators are not always immediately recognizable, due to the lack of standardized identifiers or means to determine possible connectivity. These objects are black boxes for investigators. The identification of connected objects by an acoustic approach appears all the more interesting as this approach does not alter the object studied, due to the absence of interaction with the subject. By analyzing the different acoustic emissions of the different connected IoT devices, forensic investigators can potentially become aware of the different electronic evidence that is in the IoT devices if this electronic evidence is not directly accessible to forensic investigators. Identifying the connected object can also helps the forensic technician to extract and to exploit the evidence data.

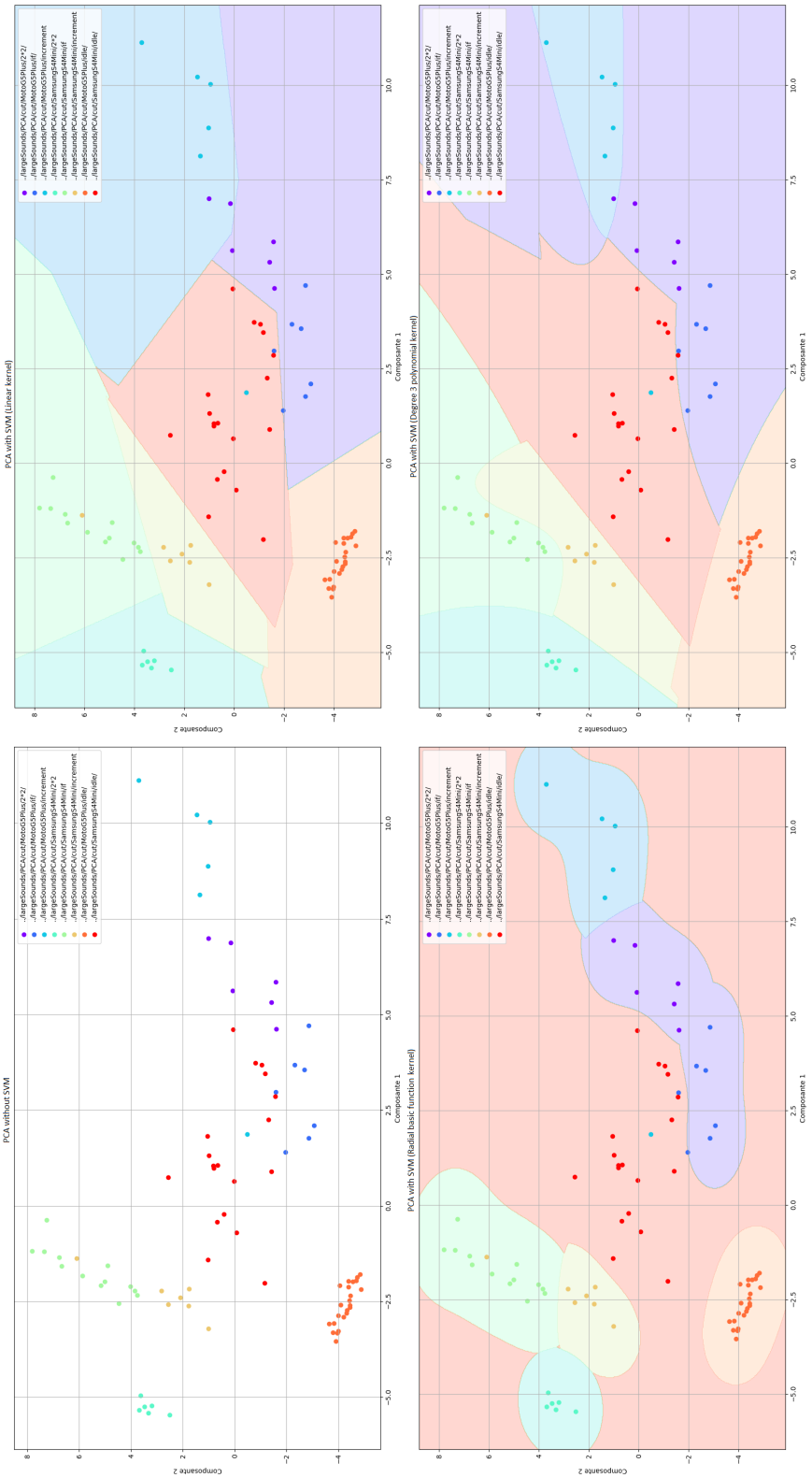

Fig. 9. Categorization by PCA and SVM

This measurement of acoustic waves can also be applied to the fight against cybercrime, and to the secure the IT infrastructure: fight against counterfeiting, attacks on data processing systems, corruption of electronic equipment, misuse of electronic material, etc. An IT department can also rely on this sound study process to validate the integration of a new connected object in the company environment.

7 Conclusion and future works

The field of connected objects is evolving very quickly. Research on the digital fingerprint of objects is still under development. Most existing approaches try to identify an object based on a small set of object characteristics. Often, they are only interested in hardware or software aspects, without ever confronting simultaneously these two attributes, which are inseparable in the context of the Internet of Things.

The acoustic study of electronic device gives promising results for equipment identification. With a machine learning approach, we obtain the beginning of an automatic classification of devices. The behavior of commercial cell phones can be discriminated just by listening to the acoustic noise emitted by the cell phone charger. Two different cell phones are quite easy to distinguish by looking at the spectrogram of the sound. More interesting, the distinction is made between similar behaviors, such as the incrementation of a variable or the calculation of prime numbers.

This first step is very promising, and is easy to implement since it only uses off-the-self components. The characterization operation is all the more relevant, as the measurement is based on inexpensive tools and can be performed over a short period of time.

To go further, improvements need to be made to the measurement apparatus, including hardware, acquisition software, and processing chain. The sensitivity of the measurement will be enhanced by using more than one microphone to capture the sound data. With more data, the signal processing is more complex, but the noise can be limited more easily. To avoid the issues of machine learning on limited-size sets with a high specialization on non-interesting charateristics, the machine learning will be directed by some physical characteristics, manually selected. The selection process of physical based metrics is not obvious and should be explored more into the detail. Indeed, a small change in the metrics will lead to major changes in the classification process. Using some “optimized” metrics will help to define a digital fingerprint based on sound emanations. The fingerprints can be stored in databases. The use of such metrics could be also used to refine digital traces in order to fit to the uses. For example in forensic studies, the metrics could be selected in order to extract specific features from the measurements, such as trying to find counterfeit devices or discriminating between objects with a high processing activity from others with a limited activity.

References

1. IDC: Worldwide internet of things forecast, 2020–2024. https://www.idc.com/getdoc.jsp?containerId=US45861420 (2020)
2. Briol, R.: Emanation: How to keep your data confidential. In: Proceedings of Symposium on Electromagnetic Security For Information Protection. pp. 225–234 (1991)
3. Asonov, D., Agrawal, R.: Keyboard acoustic emanations. In: IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004. pp. 3–11. IEEE (2004)
4. Zhuang, L., Zhou, F., Tygar, J.D.: Keyboard acoustic emanations revisited. ACM Transactions on Information and System Security (TISSEC) 13(1), 1–26 (2009)
5. Backes, M., Dürmuth, M., Gerling, S., Pinkal, M., Sporleder, C.: Acoustic side-channel attacks on printers. In: USENIX Security symposium. pp. 307–322 (2010)
6. Al Faruque, M.A., Chhetri, S.R., Canedo, A., Wan, J.: Acoustic side-channel attacks on additive manufacturing systems. In: 2016 ACM/IEEE 7th international conference on Cyber-Physical Systems (ICCPS). pp. 1–10. IEEE (2016)
7. Association, N.D.I., et al.: Cybersecurity for advanced manufacturing. Retrieved May 28 (2014)
8. Reznick, C.: Manufacturing: A persistent and prime cyber attack target (2015)
9. Genkin, D., Shamir, A., Tromer, E.: Acoustic cryptanalysis. Journal of Cryptology 30(2), 392–443 (2017)
10. Shamir, A., Tromer, E.: Acoustic cryptanalysis: On nosy people and noisy machines. eurocrypt 2004 rump session, 2004
11. LeMay, M., Tan, J.: Acoustic surveillance of physically unmodified pcs. In: Security and Management. pp. 328–334 (2006)
12. Polak, A.C., Goeckel, D.L.: Identification of wireless devices of users who actively fake their rf fingerprints with artificial data distortion. IEEE Transactions on Wireless Communications 14(11), 5889–5899 (2015)
13. Klein, R.W., Temple, M.A., Mendenhall, M.J.: Application of wavelet-based rf fingerprinting to enhance wireless network security. Journal of Communications and Networks 11(6), 544–555 (2009)
14. Xu, Q., Zheng, R., Saad, W., Han, Z.: Device fingerprinting in wireless networks: Challenges and opportunities. IEEE Communications Surveys & Tutorials 18(1), 94–104 (2015)
15. Genkin, D., Pattani, M., Schuster, R., Tromer, E.: Synesthesia: Detecting screen content via remote acoustic side channels. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 853–869. IEEE (2019)