symmetry

MDPI

Article

Detection of the Compromising Audio Signal by Analyzing Its AM Demodulated Spectrum

Alexandru Madalin Vizitiu [1,2,*], Lidia Dobrescu [1], Bogdan Catalin Trip [1,2], Vlad Florian Butnariu [1,2], Cristian Molder [3] and Simona Viorica Halunga [1]

[1] Faculty of Electronics, Telecommunications and Information Technology, National University of Sciences and Technologies Politehnica Bucharest, 060042 Bucharest, Romania; lidia.dobrescu@upb.ro (L.D.); bogdan.trip@stsnet.ro (B.C.T.); vlad.butnariu@stsnet.ro (V.F.B.); simona.halunga@upb.ro (S.V.H.)
[2] The Special Telecommunications Service, 060044 Bucharest, Romania
[3] Center of Excellence in Robotics and Autonomous Systems—CERAS, "Ferdinand I" Military Technical Academy, 050141 Bucharest, Romania; cristian.molder@mta.ro
* Correspondence: alexandru.vizitiu@stsnet.ro

Abstract: The information technology and communication (IT&C) market consists of computing and telecommunication technology systems, which also include a variety of audio devices. Preserving the confidentiality of transmitted information through these devices stands as a critical concern across various domains and businesses. Notably, spurious electromagnetic emanations emitted by audio devices can be captured and processed, potentially leading to eavesdropping incidents. The evaluation of electronic devices for potential security vulnerabilities often involves employing Transient Electromagnetic Pulse Emanation Standard (TEMPEST) technology. This paper introduces a novel approach to TEMPEST testing specifically tailored for audio devices. The outcomes of the proposed approach offer valuable insights into TEMPEST equipment testing, aiming to mitigate the potential risks posed by threats exploitable by eavesdroppers in everyday scenarios. The present work delves into the examination of two ubiquitous global electronic devices: a notebook and a pair of in-ear headphones. The symmetrical framework of this study arises from the intrinsic similarity that, despite belonging to distinct categories, both devices possess the capability to emit electromagnetic emissions that contain compromised audio signals. This assertion is substantiated by the measurement results presented herein. The proposed methodology involves the analysis of the audio amplitude modulation (AM) demodulated signal in the frequency domain. This innovative approach not only mitigates operator fatigue but also significantly reduces the testing time required for these devices and instrument running hours and leads to the development of new applications.

Keywords: cybersecurity; electromagnetic compatibility; audio eavesdropping; TEMPEST; signal processing; equipment testing

Citation: Vizitiu, A.M.; Dobrescu, L.; Trip, B.C.; Butnariu, V.F.; Molder, C.; Halunga, S.V. Detection of the Compromising Audio Signal by Analyzing Its AM Demodulated Spectrum. *Symmetry* **2024**, *16*, 209. https://doi.org/10.3390/sym16020209

Academic Editor: Iuon-Chang Lin

Received: 10 January 2024
Revised: 2 February 2024
Accepted: 7 February 2024
Published: 9 February 2024

1. Introduction

In our modern world, IT equipment's technological advances and their affordability are leading to ever-increasing numbers of IT users [1,2]. The quality of the circuits and electronic components that are contained in communications equipment is often lower, especially in a society governed by consumerism. Passing the conformity and electromagnetic compatibility requirements is not enough for a product if it is used to transmit users', companies', or institutions' sensitive information. The present paper aims to increase the awareness among users from fields of work that are sensitive to interception of information, and also among common users regarding the device's security, intimacy, and privacy issues, as well as their limitations [3,4]. In this way, they will acquire the ability to adapt the use of IT equipment according to the context.

Computing devices can process different types of information (video, audio, etc.) [5–9] in digital or analog format. According to the information sensitivity, it falls into two categories:

unclassified and classified. The communications security terminology has two suggestive names for these categories. Hence, the computing device lines that carry unclassified information are called BLACK lines, and those carrying classified information are called RED lines [10–13].

It is well known that the flow of charged particles through an electric conductor generates an electromagnetic field around it [14]. IT equipment is composed of numerous electrical lines passed through by various electric currents, used to process and transmit information in the form of electronic signals. As electrical lines transmit various signals, two adjoined conductors can generate electromagnetic interference and cross-talk. In this process, the modulating informational signal is represented by the signal carrying the information for transmission, so electronic devices generate radiated or conducted electromagnetic emissions. The information carried by those electromagnetic emissions is considered to be compromised if, following reception, acquisition, and processing, specific information is found to belong to red communication lines and components of signals transmitted on these lines are found within those emissions. TEMPEST stands for Transient Electromagnetic Pulse Emanation Standard and corresponds to the field that deals with the study of compromising electromagnetic emissions generated unintentionally by electronic devices. This is a component of signal intelligence (SIGINT), but with direct implications for civilian areas where classified information is transmitted and processed [15].

Testing equipment to identify security breaches due to the level of unintentionally generated compromising electromagnetic emissions plays a crucial role in establishing the confidentiality, processing, and transmission of information. The current method by which devices processing audio signals are tested is cumbersome due to the need for increased user attention during testing. The main factors leading to the hindrance of this activity are the prolonged exposure time of the user to a high level of concentration, the lengthy testing period due to the properties of the analyzed signal, and the increased operating time of the instruments used. The method proposed in this article aims to reduce the factors that hinder the testing process. This paper begins by examining related works in the field discussed, followed by an exploration of the conventional method employed for identifying compromised audio signals from electromagnetic leakage. Following the appropriate process of the new method proposed in this article leads to increased accuracy in detecting compromising audio signals and reduced testing times for computer equipment, thereby reducing the exposure times of testing operators and the wear and tear on the equipment used. In the final chapter, the contributions that this article makes to the field are highlighted and future directions are also depicted.

2. Related Works

Specialists and researchers in both civilian and military domains study and engage in the process of reconstructing information accidentally emitted by electronic devices through their electromagnetic emanations.

Within the domain-specific literature, the computing devices compromising electromagnetic emanations' study are addressed, at a general level, in several papers, such as [16–18]. In work [16], the authors present how electromagnetic emanation security breaches can be exploited using economically affordable instrumentation to eavesdrop on the interest's signals. In the same manner, paper [18] highlights the feasibility of information leakage, emphasizing the integrated circuits (IC), elements that depict the key of the current electronic devices [19].

The research results regarding signals that can be carried by IT&C equipment are conducted and published according to the nature of the information transmitted. Video signal eavesdropping risks in the case of flat-panel displays are studied and presented in [20]. Considering the earliest approaches in this domain, the authors of the paper [21] propose a countermeasure for video signal eavesdropping. The efficiency of the proposed asymmetric and symmetric TEMPEST fonts that can be used for classified document editing and visualization are highlighted by analyzing the video signal generated by three commercial off-the-shelf video projectors connected to a laptop using analog and digital

interfaces. The risk awareness among users regarding video compromising electromagnetic emanations (CE) was increased in paper [22]. In this work is presented a software-defined radio (SDR) tool developed to further emphasize the simplicity of eavesdropping video signals from display units that use HDMI and DVI-D interfaces.

According to Hugo Fastl and Eberhard Zwicker [23], hearing is triggered by physical stimuli only if the signal corresponds to the spectrum domain from 20 Hz to 20 kHz. At the same time, this range varies based on different factors, including gender, age, and individual differences in environmental and cultural factors. On the other hand, the main telephony band was historically established, to optimize bandwidth efficiency, from 300 Hz to 3.3 kHz. With the advent of digital technologies, the audio signal bandwidth for VoIP telephony has been widened from 50 Hz to 7 kHz [24]. As in this work, those aspects are addressed in the paper [25], which emphasizes the presence of audio CE. In this work, it is presented that an electronic device with proper functioning can lead to the audio signal being unintentionally modulated and emitted in the electromagnetic spectrum within the frequency range of 1 MHz to 1000 MHz. From the TEMPEST perspective, the study highlights security breaches using different test patterns. Similar to compromised video signal analysis in the related literature, this investigation consists of analyzing different spectrum captures that reflect the differences that allow the compromised frequency's identification. The signals' analysis from the TEMPEST perspective is based on the fact that for each transition that corresponds to a rising or falling edge from the communication line, an electromagnetic pulse is emitted unintentionally in the electromagnetic spectrum. The pulse sequence is, therefore, captured and processed in order to establish the risk of eavesdropping on the information processed by the targeted device. In consequence, a mathematical process of correlation cannot be computed among the waveform of the signal processed by the studied equipment and the received signal's waveform that corresponds to its unintended electromagnetic emanations. Hence, visual correlations are performed by human operators to detect the presence of the compromised signal in the received waveform. The visual correlation among the received signal and test patterns occurs in the time domain, a process that can take a long period when analyzing the entire spectrum of interest. To ascertain the percentage of leaked signal reconstruction, this paper presents various time-domain captures. The objective of this paper is to underscore that security breaches of audio IT&C devices are crucial when the integrity of transmission is needed.

Also, the existence of compromising electromagnetic emissions related to the video signal carried by laptops on the power line was highlighted for distances up to 50 m in work [26]. This paper explores the propagation of conducted electromagnetic emissions and the associated risks when utilizing computing devices. While the study primarily bases its findings on the analysis of video signal propagation mode and parameters, the implications of the results extend to other compromising signals, including audio. A key of this article focuses on outlining strategies to eliminate or, at the very least, mitigate the risk of compromised communication. In situations where traditional shielding methods present challenges for small audio devices like headphones due to their compact size, the utilization of suitable power filters and uninterruptible power supplies (UPS) emerges as an equally viable approach to safeguard audio signals.

In another manner, the phenomena presented in our previous work [27], in which the vulnerability of wireless headphones is presented, was further exploited in paper [28], focused on the reconstruction of sound information leakage. The authors present the importance of knowledge about this signal's propagation breaches. Following the mathematical exposure of the phenomenon, the paper presents a new approach to increasing the number of leakages. The approach considered in this paper is relevant for this domain with a contribution to offensive activities. From a defensive perspective, those results can lead to the development of new methods to overcome the presented phenomena and to increase the knowledge of this domain among researchers.

According to the state of research in this area, this paper will look into improving the process of detecting compromised audio signals. The goal is to make the detection method

more efficient, cutting down on the time and effort required in the correlation step and minimizing human involvement.

3. Actual Detection Process

The audio compromising electromagnetic emanation presence (also called in this paper audio compromising signal) in IT&C equipment transmissions is, therefore, well-known at the moment and an ongoing continuous concern among scientists who study these vulnerabilities [28,29]. In practice, and also in the specialty literature, the audio compromising signal detection procedure implies, firstly, the device's generated emissions radio frequency (RF) measurements. Subsequently, correlations are performed to identify the presence of test messages in the unintentional electromagnetic emissions of the equipment.

To further emphasize the results in this paper, measurements were performed in an anechoic room, the device under test (DUT) being placed on the test table. The RF receiving chain is illustrated in Figure 1. Using specified electromagnetic transducers, electromagnetic emissions generated by the studied devices were captured and transmitted via RF cables to the command room, where the reception system was installed. This system consists of a wideband receiver specially designed for TEMPEST testing, an oscilloscope connected to the intermediate frequency (IF) port of the receiver, and a computer used to control the previously mentioned equipment. The oscilloscope is used to perform the correlations among the received signal's waveform and the test pattern. While the DUT is processing signals corresponding to different test patterns, its unintended electromagnetic emissions are captured by the reception system. The results presented in this paper were obtained using the Rohde&Schwarz FSWT wideband receiver and RTO oscilloscope.

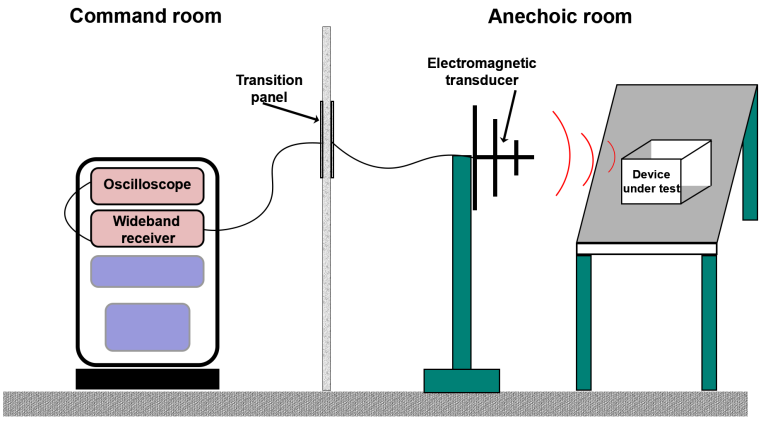


Figure 1. Reception chain.

The presence of the compromising signal in the received signal is first detected by overlapping two spectrum sweeps and comparing them. The first sweep corresponds to the situation in which the DUT processes the test pattern (represented in the following figures using red color), and the second one corresponds to the situation where the DUT does not process such information (represented in the following figures using green color). Whether the signal-to-noise ratio (SNR) allows the identification of the test pattern's particularities in the spectrum sweeps or not, the compromising signal identification in the DUT's unintended electromagnetic emanations is performed by correlating the test pattern with the received signals. This operation is performed with a predilection in frequency ranges where large differences in carrier amplitude are observed among measurements with and without processing the test message [30]. Correlations are performed by human operators by visualizing on an oscilloscope, in the time domain, the signal provided by the receiver's IF output. This process is highlighted in the workflow depicted in Figure 2.

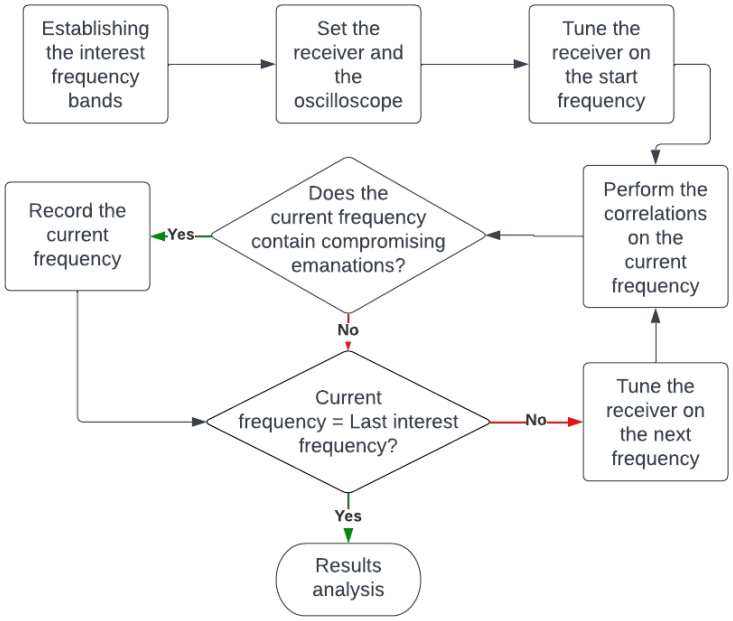


Figure 2. Audio compromising signal's correlation process workflow.

4. Detection and Analysis of Compromised Audio Signal: Traditional and Novel Approaches

4.1. Audio Signal Analysis via Oscilloscope Employing Receiver's IF Output

In order to test electronic devices and their susceptibility to TEMPEST attacks, specific test patterns are used. These patterns are transmitted to the device's hardware unit responsible for processing the test pattern. The test patterns are designed to help detect any compromising signal. For display unit TEMPEST testing, the test patterns consist of images that show either vertical or horizontal stripes [31,32]. This type of test pattern is used when notebooks, monitors, televisions (TV), or smartwatch devices are tested. When testing for compromising audio signals, the test pattern consists of an audio tone sequence. The duration and harmonics are created by the testing operator according to the standard requirements to achieve optimal correlation between the unintended electromagnetic emanations of the device being tested and the test pattern being used.

In the matter of this paper, one of the test messages from the previous article [27] is used, the one with a duration of 500 ms, composed of three harmonics (700 Hz, 1 kHz, 1.3 kHz), with the tones and silence durations illustrated in Figure 3.

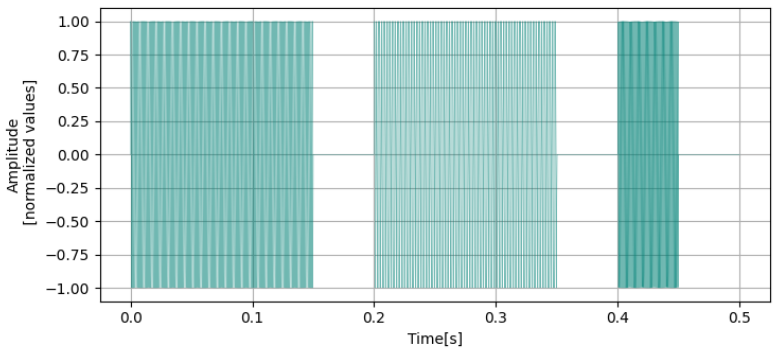


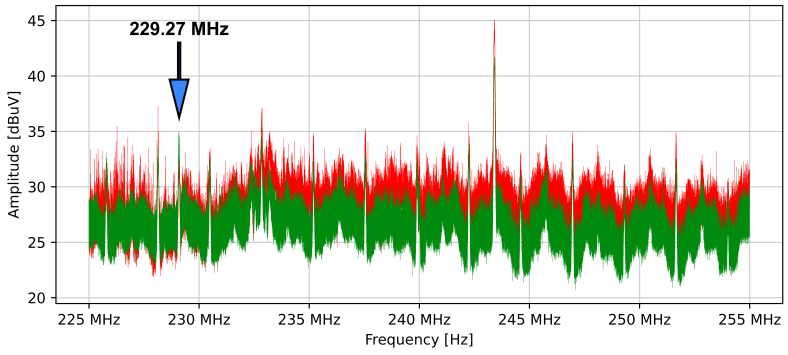
Figure 3. Test pattern with 500 ms duration composed of 3 tones (700 Hz, 1 kHz, 1.3 kHz).

Using the optimal reception and analysis parameters for audio compromising signal testing, to ensure the research symmetry, compromising electromagnetic emanation

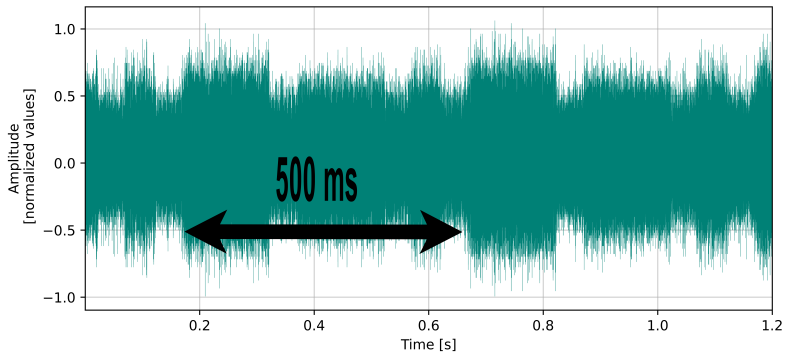
measurements were performed for two ubiquitous electronic devices (notebook and in-ear wired headphones). For each one, two measurements were performed in the cases of the studied devices while processing the test patterns or not.

The measurement results for the notebook are illustrated in Figure 4a. It can be noticed, comparing the two sweeps, that several carriers in this frequency range could contain compromising audio signals. It should be mentioned that a visible difference in a given carrier among the two measurements taken does not always lead to the identification of the carrier on which the test pattern is modulated. To highlight the presence of the audio compromised signal in the analyzed frequency ranges, all the frequencies analyzed in this paper have been chosen to illustrate clearly the described elements; therefore, it corresponds to a high SNR value. With the spectrum receiver tuned on those frequencies, it facilitates the identification of tones composing the test messages and the measurement of its duration. The presented figures are derived through the acquisition of instrument-generated data traces, subsequently processed and visualized utilizing Python scripts.

Following the process in the presented workflow diagram in Figure 2, by analyzing on the oscilloscope's display the signal provided from the IF port of the receiver, we find that at f = 229.27 MHz a compromising audio signal is found. In the oscilloscope's acquisition, Figure 4b, the test pattern's presence in the received signal's content is observed. The double-sided arrow marks the test pattern presented in Figure 3.



(**a**)

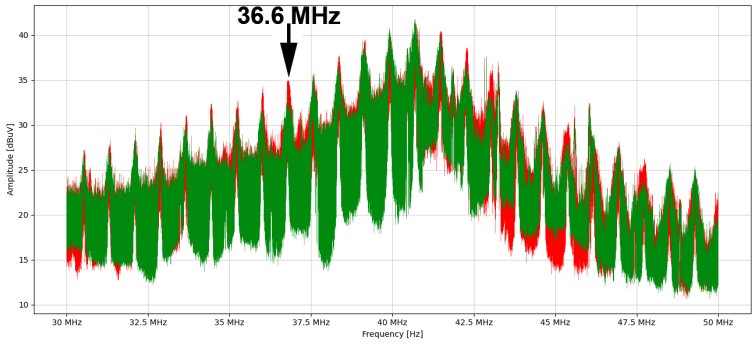


(**b**)

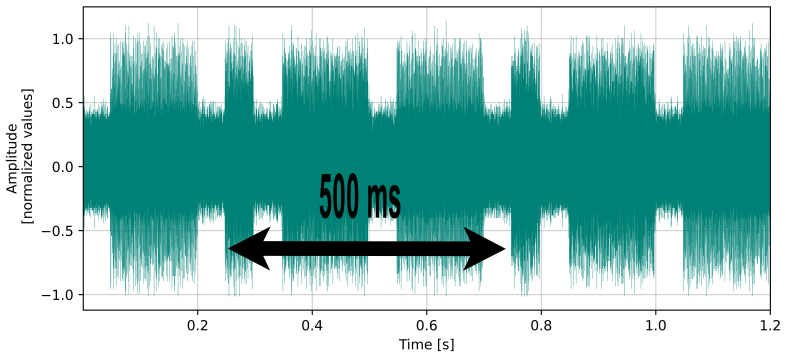
Figure 4. (**a**) Spectrum capture in 225–255 MHz frequency range (red trace—sweep while the device is running the test pattern, green trace—sweep with the device not running the test pattern) and (**b**) compromised signal highlighted, identified at 229.27 MHz frequency. Studied device: notebook.

For the second studied device, in-ear wired headphones, the analysis of Figure 5a concludes that a compromising audio signal could be present at the 36.6 MHz frequency. By correlating the received signal at this frequency with the test pattern used, we noticed that the compromised signal can be more easily identified in the case of this studied device than in the case of the studied notebook. The duration of the test pattern used, presented in

Figure 3, is highlighted with a double-sided arrow. More specifically, the duration of the tones and silences that make up the test pattern can be easily analyzed in the performed measurements presented in Figure 5b, realizing symmetry in the article with the previously presented results for the notebook analysis case.



(**a**)



(**b**)

Figure 5. (**a**) Spectrum capture in 30–50 MHz frequency range (red trace—sweep while the device is running the test pattern, green trace—sweep with the device not running the test pattern) and (**b**) compromised signal identified and highlighted at 36.6 MHz frequency. Studied device: in-ear headphones.

This process of identifying the presence of compromising emissions corresponding to the audio signal carried on the communication lines of the IT&C devices is expensive if we evaluate the receiving equipment's operating time, but also if we consider the long time required for the operator to make correlations. In addition, given the audio test pattern signal's narrow bandwidth (hundreds of Hz), for the human factor, it is extremely challenging to cover the entire spectrum of interest (from kHz to hundreds of MHz). This leads to an increased correlation operator fatigue, and hence, the operator may fail to identify in some cases the compromising emanations' presence while performing the correlations, especially in situations where the SNR does not facilitate the visualization and detection of the test message in the time domain.

4.2. The Novel Approach: Detection of Compromised Audio Signal through Spectrum Analysis of AM Demodulated Signal

There is hereby a strong need to develop new audio signal detection methods to support the operator in optimizing the compromising audio signal identification process. This paper proposes a new approach to how correlations can be performed for the audio signal. It consists in using the audio output (phones) port of the used receiver instead of using its IF port. The AM demodulated signal is transmitted from the receiver's phones

port to the oscilloscope using an audio cable, at the ends of which we find a 3.5 mm jack connector, which is inserted into the receiver's phones port, i.e, the oscilloscope's galvanic probe.

Modern oscilloscopes, due to their high signal processing capabilities, allow real-time computation of the applied input signal's spectrum. Thus, the proposed method consists of the AM demodulated signal's frequency domain analysis of the signals applied at the oscilloscope's input. The process flow diagram corresponds to the previously presented method and it is highlighted in Figure 2. In the proposed method, the operator must watch the oscilloscope's display for the harmonics that make up the message's presence, without the need to analyze the signal in the time domain (which is difficult in very noisy frequency bands) or listen to the demodulated signal played back in the receiver's loudspeaker. Experimentally, it has been determined that is enough for the oscilloscope's acquisition time to match with a single test message's duration. The spectral bandwidth of interest for the tones making up the test patterns is DC—10 kHz. Following this process, correlations are performed to identify the compromising audio signal at the frequencies shown above by the IF output port signal analysis in the time domain.

In Figure 6, the AM demodulated signal's spectrum is shown for the case where the DUT is represented by the laptop and the receiver is tuned to the 229.29 MHz center frequency. Harmonics in the spectrum corresponding to the frequencies 700 Hz, 1000 Hz, and 1300 Hz are observed, representing the tones that make up the test message. Visually comparing Figure 4b with Figure 6, it can be concluded that the compromising emanation's presence can be made easier in the case of AM demodulated signal's spectrum analysis than the IF corresponding signal's time-domain analysis.

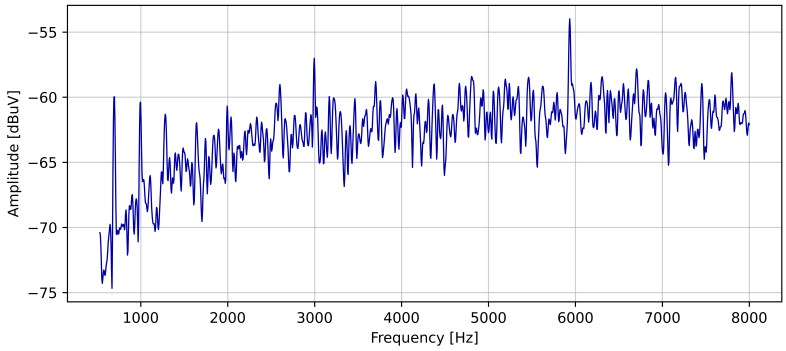


Figure 6. AM demodulated signal's spectrum when the test pattern with 500 ms length is processed by the notebook. Fundamental tones that comprise the test pattern can be observed. Capture from oscilloscope.

The processing and amplification stages, through which the audio signal is transmitted to the audio studied devices' speakers, and the electronic component's imperfections occasionally cause the test pattern's tones' harmonics to be present in the received compromised signal. In some cases, these harmonics' presence and the test pattern's three tones' absence are found. In this manner, the asymmetrical attribute of this subchapter is delineated by the variances observed in the results obtained from the examination of the two studied devices.

To enhance the readability of this paper, the harmonics of test tones that comprise the test patterns are presented in three tables. Table 1 corresponds to the 700 Hz tone, Table 2 corresponds to the 1 kHz frequency tone, and Table 3 corresponds to the third tone of the test pattern with 1.3 kHz frequency. In the presented tables, the Notation column contains the notations that will be used in the figures for each frequency to facilitate the identification of harmonics in the frequency spectrum captures.

Table 1. Harmonics of 700 Hz tone.

Harmonic's Order	Harmonic's Frequency	Notation
1	700 Hz	A1
2	1.4 kHz	A2
3	2.1 kHz	A3
4	2.8 kHz	A4
5	3.5 kHz	A5
6	4.2 kHz	A6
7	4.9 kHz	A7
8	5.6 kHz	A9
9	6.3 kHz	A9
10	7 kHz	A10

Table 2. Harmonics of 1 kHz tone.

Harmonic's Order	Harmonic's Frequency	Notation
1	1 kHz	B1
2	2 kHz	B2
3	3 kHz	B3
4	4 kHz	B4
5	5 kHz	B5
6	6 kHz	B6
7	7 kHz	B7
8	8 kHz	B8

Table 3. Harmonics of 1.3 kHz tone.

Harmonic's Order	Harmonic's Frequency	Notation
1	1.3 kHz	C1
2	2.6 kHz	C2
3	3.9 kHz	C3
4	5.2 kHz	C4
5	6.5 kHz	C5
6	7.8 kHz	C6

The harmonics' presence, in the laptop analysis case, is shown in Figure 7 and corresponds to the situation where the receiver is tuned to 235.08 MHz frequency. The 4.9 kHz and 6.3 kHz frequency carriers identified in the AM demodulated signal's spectrum correspond to the test pattern's first tone's (700 Hz) harmonics, and the 5.2 kHz frequency carrier corresponds to the 1300 Hz test pattern's tone.

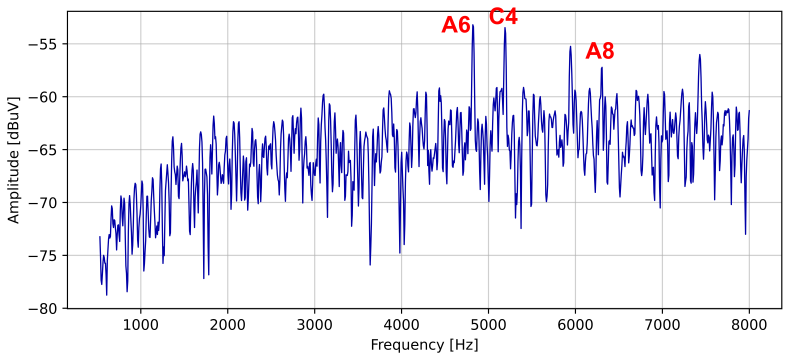


Figure 7. The spectrum of the AM demodulated signal shows that only the higher harmonics of the tones comprising the test pattern are emitted by the notebook at a frequency of 235.08 MHz.

In Figure 8, the demodulated AM signal's spectrum is shown for the situation where the test device is represented by the in-ear wired headphones and the receiver is tuned to the 36.6 MHz center frequency. In the spectrum capture from the oscilloscope, we observe the 700 Hz, 1000 Hz, and 1300 Hz frequency tones that comprise the test pattern, as well as the harmonics of these tones. The 2.1 kHz and 3.5 kHz harmonics correspond to the first tone of the test pattern; those of 3 kHz, 4 kHz, 5 kHz, and 7 kHz correspond to the second tone of the test pattern; and the 3.9 kHz harmonic corresponds to the test message's third tone. By visual analysis and comparison of Figure 5b with Figure 8, it can be concluded that the test pattern's presence in the studied device's unintended electromagnetic emanations is more easily seen when analyzing the AM demodulated signal's spectrum than the signal corresponding to the receiver's IF port.

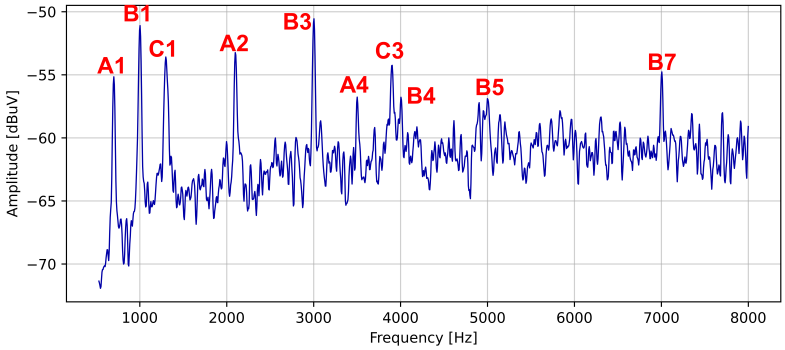


Figure 8. Regarding the in-ear headphones case, at a frequency of 36.6 MHz, both fundamental tones that constitute the test pattern and their associated higher harmonics unintentionally are emitted.

The tones comprising the test patterns' harmonics' presence are also observed in this studied device's case, having the receiver tuned to the 49.15 MHz frequency. Analyzing Figure 9, it can be noticed that 1.4 kHz, 2.1 kHz, 2.8 kHz, and 4.9 kHz frequency harmonics correspond to the 700 Hz test pattern's tone. Also, the 2 kHz, 3 kHz, and 4 kHz harmonics correspond to the test pattern's second tone. At 3.9 kHz frequency, in the presented figure, a harmonic can be noticed that corresponds to the third test pattern's tone. Also, in this case, looking at the AM demodulated signal's spectrum, the harmonics of the tones composing the test message can be observed.

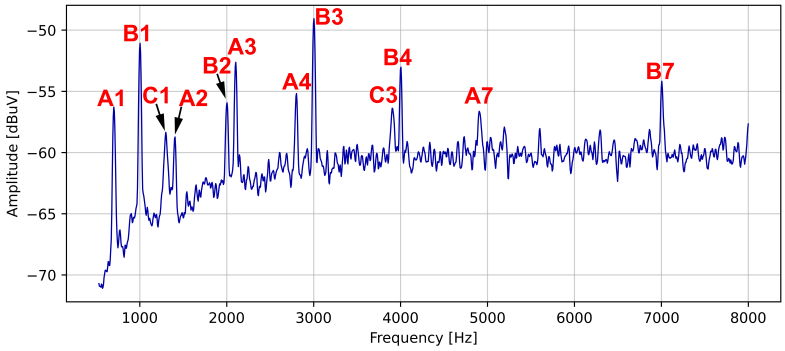


Figure 9. The evidence of fundamentals tones and their harmonics for the in-ear headphones case. Receiver tuned to 49.15 MHz frequency.

Sweeping the interest frequency range for audio signal-carrying devices, using the proposed method in this paper, it is revealed that the compromising signal can be easily detected even when the SNR is unfavorable to the received signal's time-domain visualization. The AM demodulated signal's carrier amplitudes of interest will be maximum in the situation where the SNR has the highest value.

In Figure 10, the efficiency of the proposed method in a noisy environment can be observed. Thereby, three harmonics can be noticed corresponding to the 700 Hz tone at 700 Hz, 2.8 kHz, and 5.6 kHz; the fundamental of the second used tone at the 1 kHz frequency; and a possible harmonic of the third used tone at 5.2 kHz frequency.

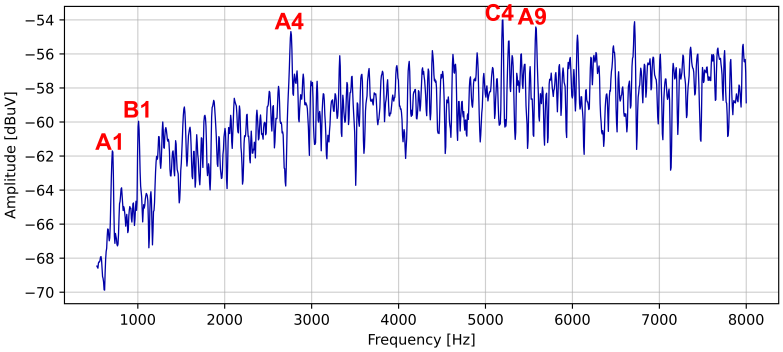


Figure 10. In a scenario with a lower SNR value, the presence of various harmonics of the tones comprising the test pattern are received at the 36.5 MHz frequency.

With the proposed method, we can conclude that the operator can achieve early detection of the test message's presence in the studied device's unintended electromagnetic emanations.

5. Reduction of Test Message Duration—Reduction of Correlation Time: New Approach Performance Evaluation

5.1. Improvement of the Test Patterns

The used test pattern's duration is 500 ms and the analyzed electromagnetic spectrum in the case of audio device testing is wide (hundreds of MHz). The oscilloscope's signal acquisition duration corresponds to the test pattern duration and, therefore, the electronic device's compromising electromagnetic emission analysis will take a long period (on the order of hours). In this situation, the human factor's fatigue increases considerably and affects the optimal and efficient performance of correlation activities. We consider it opportune to compose some test messages of which the duration is shorter than the test message used above. Therefore, respecting the tone order and the timing ratios, three new test patterns were created. In Figure 11 is presented the new test pattern with 250 ms length; in Figure 12 is presented the second new test pattern with 100 ms length; and in Figure 13 is represented the last new test pattern with 50 ms length.

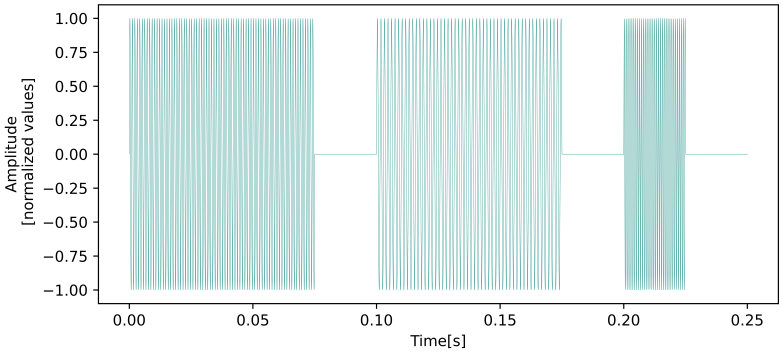


Figure 11. New test pattern with 250 ms length.

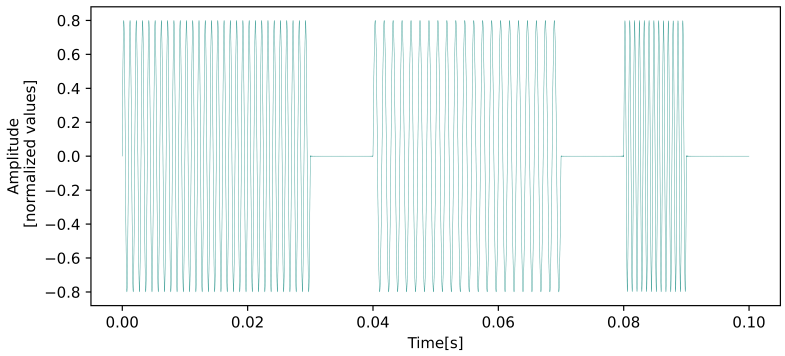


Figure 12. New test pattern with 100 ms length.

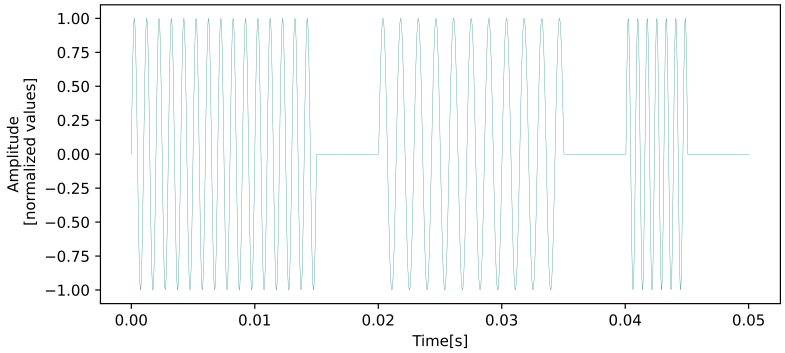


Figure 13. New test pattern with 50 ms length.

The audio signal's presence in the unintended electromagnetic emanations of electronic devices was studied for the three new test pattern messages. The analysis frequencies are the same as for the first test message.

Analyzing the results, it is found that, in the notebook's case, tone detection can be successfully achieved for two of the three test patterns. For the 250 ms length test pattern's case, as presented in Figure 14, it can be noticed that we can easily observe the presence of the first harmonic presence for each tone that comprises the test pattern. Reducing by five times the length of main the test pattern, observing the frequency spectrum presented in Figure 15, it can be concluded that this does not affect the tone detection. A significant difference is observed when applying the test message ten times shorter than the initial test message.

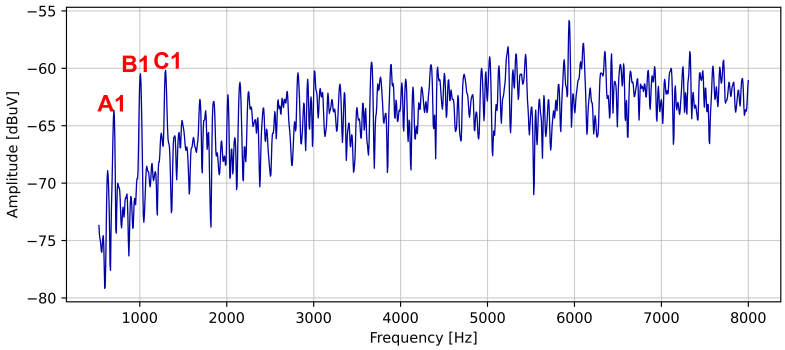


Figure 14. The implementation of a novel test pattern lasting 250 ms on the notebook results in the successful identification of CE.

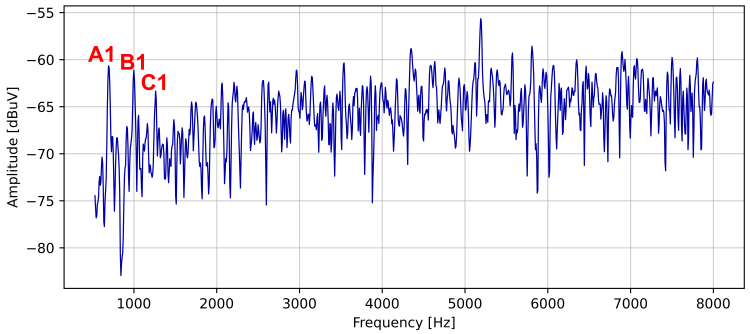


Figure 15. When the notebook functions as the device under test, successful detection of CE occurs during its processing of the new test pattern lasting 100 ms.

Using the third new test message with a duration of 50 ms, harmonics can rarely be detected, leading to compromising emissions identification failure. The spectrum plotted in Figure 16 can only be noticed in the presence of a 1 kHz tone, making the test pattern's presence very difficult to achieve. Therefore, in the notebook's case, reducing the test message length and hence, the oscilloscope acquisition time, can be successfully achieved for a duration of at least 100 ms.

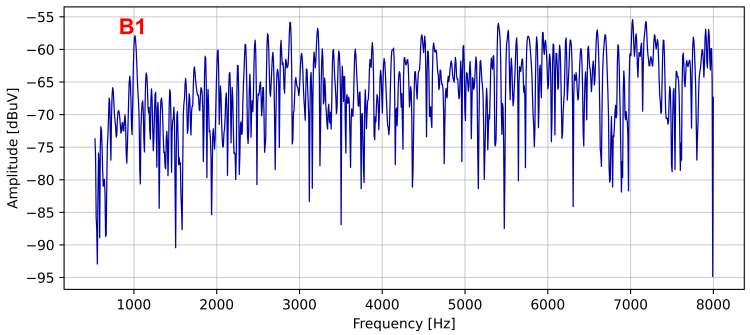


Figure 16. The test pattern's duration of 50 ms does not lead to the successful identification of the harmonics corresponding to the tones comprising the test pattern.

In the wired in-ear headphones' case, it should be noted that at a 36.6 MHz frequency, the SNR's value facilitates the compromising signal's detection, as shown above in the time-domain acquisition. Analyzing the AM demodulated signal's spectrum, it can be noticed that, compared to the results obtained for the notebook, in the wired in-ear headphone's case, the three new test patterns can be successfully applied in the compromising audio test pattern's detection. By applying the new test pattern with a duration of 250 ms, the first harmonic and also high-order harmonics of the tones that comprise the test pattern are detected, as presented in Figure 17.

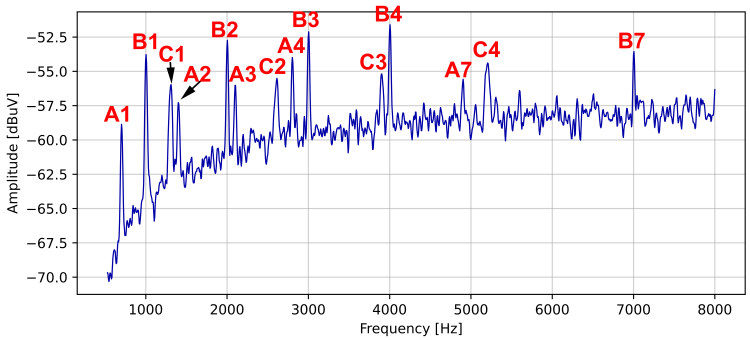


Figure 17. AM demodulated signal's spectrum corresponding to test pattern with 250 ms length. Studied device: in-ear headphones.

Also for this studied device, applying the second test message, with a length reduced by five times compared to the main test pattern's duration, the frequency spectrum of the AM demodulated signal is represented in Figure 18. In this plot, three fundamental tones con be noticed corresponding to 700 Hz, 1 kHz, and 1.3 kHz, and also a harmonic with 3 kHz, corresponding to the third harmonic of the 1 kHz frequency tone. Even if fewer harmonics than in the previous case are found, it can be concluded that the application of the test pattern with a 100 ms length leads to the compromising signal's successful identification at the 36.6 MHz frequency.

As can be seen in Figure 19, for the 50 ms duration message's case, the tones' harmonic amplitudes do not have comparable values with those obtained for the other test patterns (500 ms, 250 ms, and 100 ms).

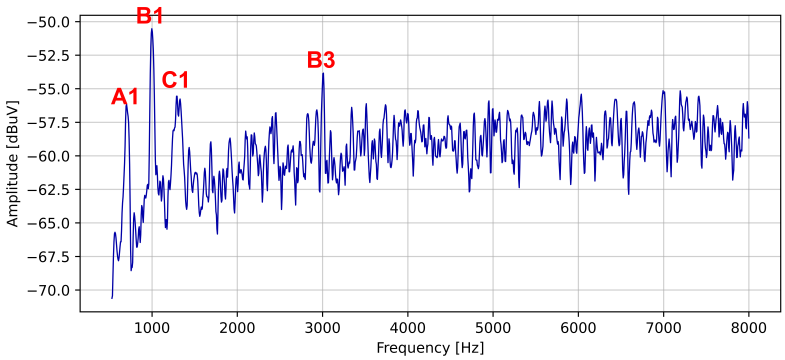


Figure 18. AM demodulated signal's spectrum corresponding to test pattern with 100 ms length. Studied device: in-ear headphones.

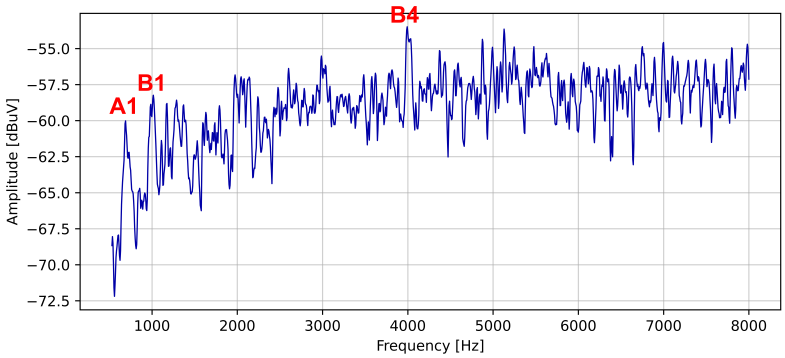


Figure 19. The 50 ms length of the new test pattern does not result in successful identification of the CE in the case of in-ear headphones due to the shorter periods of the lowest tones.

It can therefore be stated that test messages with a duration two or five times shorter than the original one (500 ms) can be used for the second device. By reducing the test pattern's duration, it is experimentally shown that the compromising audio signal's detection can be successfully achieved even when using a 100 ms duration test pattern and using for correlations the AM demodulated signal's spectrum. Using this test pattern and the proposed method for correlations in the case of an audio compromising signal, it is found that the time required for correlations decreases significantly. This leads to a reduction in human factor fatigue, receiving equipment's operating time, and DUT testing time.

5.2. Evaluation the Novel Approach Effectiveness: A Performance Analysis

In previous subsections, the new approach regarding compromising electromagnetic emissions that correspond to audio signals processed by electronic equipment was highlighted. It can be noticed that the proposed method consists of an early identification of frequency bands that contain the CE. Using the traditional method, the TEMPEST testers need to follow the oscilloscope's display of the waveform that corresponds to the received

signal and, in the meantime, identify similarities with the used test pattern. The novel approach helps the operator, who has to detect whether the harmonics of the tones composing the test message are found above the noise level.

The new proposed procedure was presented to a group of 15 TEMPEST testers to evaluate its performance by the target group. The participant selection for the experiment considered varying backgrounds and levels of experience in the task at hand. This approach ensured a comprehensive evaluation of the strengths and weaknesses of the proposed method.

During a multi-day period, each member of the established group was tasked with performing visual correlations to detect the compromised audio signal using both methodologies outlined in this article. After concluding the task, the operators analyzed their work processes and subsequently compared the two methods.

The selected metrics for evaluating the effectiveness of the proposed methodology included detection efficiency, time required for device testing, and the level of fatigue experienced during the activity. Specifically, the determination of detection efficiency involved a detailed analysis of situations where the classical method, hindered by low SNR values, struggled to identify the compromised signal within the received waveform, as opposed to the visual correlations facilitated by the approach proposed in this paper.

Given the metrics provided, the 15 operators were assigned the following questions to address:

- How do you assess the time consumption of the proposed method in comparison to the previously used one?
- How do you evaluate the exhaustion level generated by the proposed method compared to the previously used one?
- How do you assess the efficiency of detection in the proposed method compared to the previously used one?

Upon analyzing the findings presented in Figure 20, it is evident that, for the majority of operators, the methodology proposed in this paper effectively addresses the needs of the target group, thus streamlining the process of detecting compromised audio signals, as can be noticed in Figure 20.

While for three operators the appreciation of time consumption is similar for both used methods, only one operator observed that the detection of desired signals still requires a significant amount of time, but it is anticipated that this issue will be fixed with the future directions outlined in this paper.

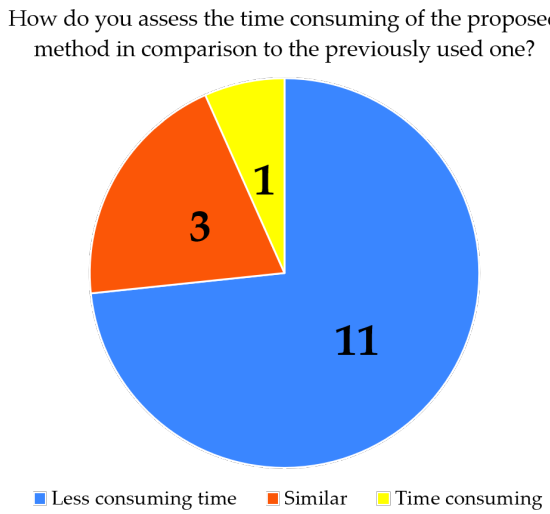


Figure 20. Operators' evaluation of time consumption of the novel approach compared to the classical method.

Additionally, based on the operators' feedback highlighted in Figures 21 and 22 regarding the exhaustion level and the efficiency of detection, respectively, another achievement of the proposed approach is the reduction in operator fatigue, while also enhancing effectiveness in scenarios where the low SNR value presents challenges for compromised signal detection using the traditional method.

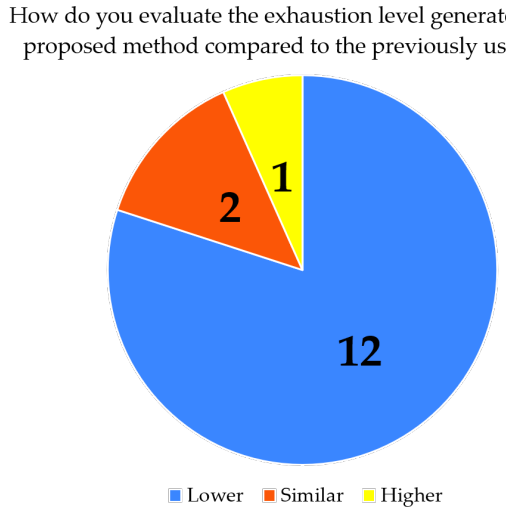


Figure 21. Operators' evaluation of exhaustion level of the novel approach compared to the classical method.

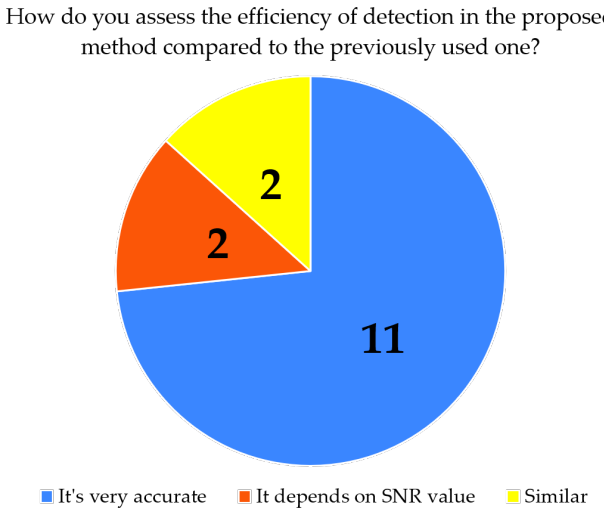


Figure 22. Operators' evaluation of detection efficiency of the novel approach compared to the classical method.

The selected group of 15 operators acknowledged that employing test messages up to five times shorter in duration than the original message resulted in a quicker sweep of the electromagnetic spectrum. This approach also mitigated the risk of overlooking the presence of the compromised signal during spectrum analysis of the AM demodulated received signal.

Upon assessing the effectiveness of the novel method for detecting compromised audio signals, it was discovered that its implementation results in an implicit increase in the quantity of equipment tested within the TEMPEST laboratory, enhances the precision of evaluating equipment processing audio signals, and promotes the well-being of operators' health.

6. Conclusions

The compromising audio signal is part of the signals tested in the TEMPEST domain. At the same time, it is of particular importance in military and civilian environments, where classified information is conveyed. This signal's importance, also presented in other publications [5,7,25] in different manners, leads to the development of new methods for IT equipment compromising electromagnetic emissions' detection.

To underscore the advancements introduced by the novel approach proposed in this article, the initial phase involved emphasizing notable works in the field. Subsequently, a specific methodology was followed to illustrate the process of audio compromising signal detection using existing procedures. Following an analysis of the compromising signal and the elucidation of the challenges associated with this method, this article introduced a novel approach.

The proposed method for targeted signal detection consists of using the AM demodulated signal supplied by the used RF receiver and its analysis in the frequency domain on a powerful oscilloscope. Further acquisition of the signal's spectrum traces has been exported to a notebook for a laborious analysis using Python scripts. Analyzing how the test message information is reflected in the captures and the required duration of analysis for human operators to be triggered, the benefits of the presented approach are real.

Relative to findings in other research papers employing test messages comprising test patterns lasting approximately 500 ms, the suggested method offers the capability to reduce the duration of the test message by a factor of up to five. Furthermore, with the high SNR value corresponding to the harmonics of the tones comprising the utilized test pattern, the adoption of the novel method, according to the interviewed group of TEMPEST testers, results in a reduction in the time required for correlations of compromised audio signals and minimizes the effort exerted by the human factor during these tasks, even in scenarios with low SNR values, as illustrated in Figure 10.

Upon analyzing the results obtained with shorter test patterns, it is noticed that the length of the test message cannot be significantly diminished. For certain devices, it is observed that their speaker remains inactive when a short test pattern is used, resulting in no discernible variations in the electromagnetic field surrounding the speaker. Nevertheless, achieving a reduction in the duration of the test message by up to fivefold is a noteworthy accomplishment.

Our future research endeavors involve enhancing detection efficiency. Utilizing machine learning (ML) algorithms could automate the detection of audio signals in TEMPEST testing equipment, thereby streamlining the workload of human operators. This approach could enable the detection of compromising audio emanations even when the signal-to-noise ratio (SNR) is subunitary, surpassing the limitations of human observation.

Author Contributions: Conceptualization, A.M.V., L.D., C.M. and V.F.B.; methodology A.M.V., C.M. and B.C.T.; software A.M.V. and C.M.; validation, A.M.V., L.D. and S.V.H.; formal analysis A.M.V., L.D., C.M. and B.C.T.; investigation, A.M.V., V.F.B. and B.C.T.; resources, A.M.V. and L.D.; data curation, A.M.V. and V.F.B.; writing—original draft preparation, A.M.V.; writing—review and editing, L.D., C.M. and S.V.H.; visualization, A.M.V.; supervision, L.D.; project administration, L.D.; funding acquisition, L.D. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the National University of Science and Technology POLITEHNICA Bucharest's PUBART project.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IT&C	Information technology and communications
CE	Compromised electromagnetic emanations
TEMPEST	Transient Electromagnetic Pulse Emanations Standard
UPS	Uninterruptible power supplies
SDR	Software-defined radio
DUT	Device under test
IC	Integrated circuit
RF	Radio frequency
SNR	Signal-to-noise ratio
f	Frequency
IF	Intermediate frequency
AM	Amplitude modulation
TV	Television
ML	Machine learning

References

1. Qualcomm Technologies. *The 2022 State of Sound Report: A Global Analysis of Audio Consumer Behaviors and Desires*; Technical Report; Qualcomm Technologies: San Diego, CA, USA, 2022.
2. BlueWave Consulting. *Wireless Headphones Market—Global Size, Share, Trend Analysis, Opportunity and Forecast Report, 2018–2028, Segmented by Product Type (In-Ear, Over-Ear Headphones, Others), Distribution Channel (Online, Offline), Application (Music & Entertainment, Gaming, Virtual Reality, Fitness, Others), Region (North America, Europe, Asia Pacific, Latin America, Middle East and Africa)*; Technical Report; BlueWave Consulting: Noida, India, 2022.
3. National Research Council. *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*; National Academies Press: Washington, DC, USA, 2010.
4. Sandescu, C.; Dinisor, A.; Vladescu, C.V.; Grigorescu, O.; Corlatescu, D.; Dascalu, M.; Rughinis, R. Extracting exploits and attack vectors from cybersecurity news using NLP. *UPB Sci. Bull. Ser. C Electr. Eng. Comput. Sci. Politech. Univ. Buchar.* **2022**, *84*, 63–78.
5. Birukawa, R.; Nagata, D.; Hayashi, Y.i.; Mizuki, T.; Sone, H. The Source Estimation of Electromagnetic Information Leakage from Information Devices. In Proceedings of the 2020 XXXIII General Assembly and Scientific Symposium of the International Union of Radio Science, Rome, Italy, 29 August–5 September 2020; pp. 1–4. [CrossRef]
6. Zheng, K.; Luo, R.; Wang, Z.; Liu, X.; Yao, Y. Short-Term and Long-Term Throughput Maximization in Mobile Wireless-Powered Internet of Things. *IEEE Internet of Things J.* **2023**. [CrossRef]
7. Choi, J.; Yang, H.Y.; Cho, D.H. Tempest comeback: A realistic audio eavesdropping threat on mixed-signal socs. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Online, 9–13 November 2020; pp. 1085–1101.
8. Liu, X.; Xu, B.; Zheng, K.; Zheng, H. Throughput Maximization of Wireless-Powered Communication Network With Mobile Access Points. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 4401–4415. [CrossRef]
9. Lavaud, C.; Gerzaguet, R.; Gautier, M.; Berder, O.; Nogues, E.; Molton, S. Whispering devices: A survey on how side-channels lead to compromised information. *J. Hardw. Syst. Secur.* **2021**, *5*, 143–168. [CrossRef]
10. Bergsma, H.; Leferink, F. Using an in-line uninterruptable power supply as TEMPEST 'filter' for naval vessels. In Proceedings of the 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, Germany, 16–22 August 2015; pp. 1106–1110. [CrossRef]
11. Johnson, T.R. *American Cryptology during the Cold War, 1945–1989*; National Security Agency: Fort Meade, MD, USA, 2007.
12. Martin, M.; Sunmola, F.; Lauder, D. Unintentional compromising electromagnetic emanations from IT equipment: A concept map of domain knowledge. *Procedia Comput. Sci.* **2022**, *200*, 1432–1441. [CrossRef]
13. Kuhn, M.G.; Anderson, R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Proceedings of the Information Hiding, Portland, OR, USA, 14–17 April 1998; Aucsmith, D., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 124–142.
14. Lindell, I.V.; Sihvola, A.H. Perfect Electromagnetic Conductor. *J. Electromagn. Waves Appl.* **2005**, *19*, 861–869. [CrossRef]
15. NATO Military Committee Communication; Information Systems Security; Evaluation Agency (SECAN). *NATO Standard (2009) SDIP-27/2: NATO TEMPEST Requirements and Evaluation Procedures*; (Published March 2016 but Not for Public Use, NATOCONFIDENTIAL); NATO: Mons, Belgium, 2016.
16. Kitazawa, T.; Kubo, H.; Hayashi, Y. A Method for Extracting Plausible Images from EM Leakage Measured at Low Sampling Rates. In Proceedings of the 2023 IEEE 7th Global Electromagnetic Compatibility Conference (GEMCCON), Nusa Dua, Indonesia, 19–20 January 2023; p. 34. [CrossRef]
17. Lee, E.; Choi, D.H.; Nam, T.; Yook, J.G. Counter-TEMPEST: Information Spoofing based on the EM-leakage Signature of TMDS System. In Proceedings of the 2023 International Symposium on Electromagnetic Compatibility—EMC Europe, Krakow, Poland, 4–8 September 2023; pp. 1–5. [CrossRef]

18. Kaji, S.; Fujimoto, D.; Kinugawa, M.; Hayashi, Y. Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices. *IEEE Trans. Electromagn. Compat.* **2023**, *65*, 655–666. [CrossRef]
19. Gaita, A.; David, E.; Buzo, A.; Grigore, M.; Burileanu, C.; Cucu, H.; Pelz, G. Convolutional neural network model used for aiding IC analog/mixed signal verification. *UPB Sci. Bull. Ser. C Electr. Eng. Comput. Sci. Politech. Univ. Buchar.* **2023**, *85*, 151–162.
20. Kuhn, M.G. Electromagnetic Eavesdropping Risks of Flat-Panel Displays. In Proceedings of the Privacy Enhancing Technologies, Toronto, ON, Canada, 26–28 March 2004; Martin, D., Serjantov, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 88–107.
21. Boitan, A.; Kubiak, I.; Halunga, S.; Przybysz, A.; Stańczak, A. Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process. *Symmetry* **2020**, *12*, 1908. [CrossRef]
22. Groot, R.; van Meeteren, D.; Leferink, F. TEMPEST Demo for Increasing Awareness. In Proceedings of the 2023 International Symposium on Electromagnetic Compatibility—EMC Europe, Krakow, Poland, 4–8 September 2023; pp. 1–5. [CrossRef]
23. Zwicker, E.; Fastl, H. *Psychoacoustics: Facts and Models*; Springer Series in Information Sciences; Springer: Berlin/Heidelberg, Germany, 2007. [CrossRef]
24. Flanagan, W.A. VoIP and Unified Communications Define the Future. In *VoIP and Unified Communications: Internet Telephony and the Future Voice Network*; Wiley: Hoboken, NJ, USA, 2011; pp. 139–169. [CrossRef]
25. Trip, B.; Butnariu, V.; Velicu, V.; Halunga, S.; Boitan, A. Analysis of the Compromising Audio Signal From the Emission Security Perspective. In Proceedings of the 2020 13th International Conference on Communications (COMM), Bucharest, Romania, 18–20 June 2020; pp. 363–366. [CrossRef]
26. Trip, B.; Butnariu, V.; Vizitiu, M.; Boitan, A.; Halunga, S. Analysis of Compromising Video Disturbances through Power Line. *Sensors* **2022**, *22*, 267. [CrossRef]
27. Vizitiu, A.M.; Trip, B.C.; Butnariu, V.F.; Velicu, V.; Dobrescu, L.; Halunga, S. Analysis of the unintented propagation of audio signal emitted by wireless headphones. *Rev. Roum. Sci. Tech.—Sér. Électrotech. Énergétique* **2022**, *67*, 479–482.
28. Kitazawa, T.; Takano, S.; Hayashi, Y. Reconstruction of Sound Information Leakage Signals Obtained from Multiple Demodulation Methods. In Proceedings of the 2023 IEEE Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMC + SIPI), Grand Rapids, MI, USA, 29 July–4 August 2023; pp. 480–484. [CrossRef]
29. Collins, N. *Handmade Electronic Music: The Art of Hardware Hacking*; Taylor & Francis: New York, NY, USA, 2020.
30. Przybysz, A.; Grzesiak, K.; Kubiak, I. Electromagnetic Safety of Remote Communication Devices—Videoconference. *Symmetry* **2021**, *13*, 323. [CrossRef]
31. Kubiak, I.; Przybysz, A. An RGB Pseudo-Colorization Method for Filtering of Multi-Source Graphical Data. *Electronics* **2023**, *12*, 4583. [CrossRef]
32. Zhang, N.; Lu, Y.; Cui, Q.; Wang, Y. Investigation of Unintentional Video Emanations From a VGA Connector in the Desktop Computers. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1826–1834. [CrossRef]