symmetry

Article

Electromagnetic Safety of Remote Communication Devices—Videoconference

Artur Przybysz, Krystian Grzesiak and Ireneusz Kubiak *

Department of Electromagnetic Compatibility, Military Communication Institute—The State Research Institute, 05-130 Zegrze, Poland; a.przybysz@wil.waw.pl (A.P.); k.grzesiak@wil.waw.pl (K.G.)
* Correspondence: i.kubiak@wil.waw.pl

Abstract: Devices powered by electricity become sources of electromagnetic emissions in the course of their operation. In the case of devices oriented to process information, these emissions can have a character of revealing emissions, i.e., those whose reception and analysis allow for remote reconstruction of related data. The best known example of this phenomenon is the formation of revealing emissions during the operation of imaging devices: monitors, projectors or printers. Increasingly more often, these components are used for communication in the form of videoconferences with other network users. The article presents the result of tests and analyses of threats related to the use of such solutions (monitors, personal computers, VoIP terminals) for the confidentiality of conversations and the data presented during them. The focus is on video signals; however, the potential possibilities of revealing speech signals were also indicated. Such phenomenon causes a huge threat to data confidentiality because the combination of graphics and sound can undoubtedly contain much more information about the protected data than just graphics or sound separately. The presented results of analyses apply to graphic data, possibilities of non-invasive acquisition of such data, similarity of images and of patterns and reconstructed image and image recognition. The results indicate that there is still a risk of loss of data confidentiality due to a phenomenon of an electromagnetic leakage, and specialized instrumentation is not required for its interception under favorable circumstances. This may particularly apply to audio data that may be accidentally received by home radio receivers. In particular, the presented results of analyses apply to a Special Issue of *Symmetry* which is characterized by security and privacy in communication systems and networks, signal processing, video and image processing, multimedia communications and electromagnetic compatibility. All these scientific and technical areas have either symmetrical or asymmetrical approaches, and they have to be taken into consideration as a whole in order to choose the best combinations to protect processed information.

Keywords: protection of information; electromagnetic eavesdropping; screen LCD; electromagnetic emission; reveal emission; sensitive emission; valuable emission; VoIP terminal

check for updates

Citation: Przybysz, A.; Grzesiak, K.; Kubiak, I. Electromagnetic Safety of Remote Communication Devices—Videoconference. *Symmetry* **2021**, *13*, 323. https://doi.org/10.3390/sym13020323

Academic Editor: Albert Ferrando
Received: 8 January 2021
Accepted: 10 February 2021
Published: 16 February 2021

1. Introduction

Many studies and published results concern devices commonly used for information processing. These devices include desktop and mobile computers, monitors, printers and projectors. Such devices use various electrical standards to transmit video signals, which become a source of emissions correlated with the processed information. The occurrence of such phenomenon is described in [1–7]. These papers show not only the essence of the threat but also the methods (solutions) preventing the formation of hazardous emissions. However, with the development of electronic technologies and remote data transmission, new sources of valuable emissions emerge, which should be considered.

The COVID-19 pandemic has changed and is changing our personal and professional lives. Many people were forced to give up their previous activities and habits, both professional and private. Our lives are described by hashtags: #stayathome, #remoteworking,

#remoteteaching, #remotelearning, #remotebanking—in short, #remotelife. Many of us have been forced to quickly acquire knowledge and use technologies that enable remote contact with colleagues or family members. The need to immediately switch to remote work means that all kinds of devices for the transmission of sound and image are used on a massive scale. The devices intended for videoconferencing are breaking sales popularity records. Mass use of such devices automatically increases the risk of losing the confidentiality of the processed data, both company secrets and personal secrets. We use them daily without realizing that they can be sources of unwanted revealing emissions. While the media raise issues related to the broadly understood cryptographic security of the processed data [1,8], the issues related to the so-called electromagnetic penetration [2,3,9–11] are considered irrelevant in the era of digital information processing.

Telecommunications equipment introduced for use in the armed forces shall be tested to determine their degree of protection against electromagnetic information leakage (Tempest, SDIP-27 standards) for different sources of valuable emissions. These sources are graphic systems and interfaces (e.g., DVI/HDMI, DisplayPort, displays of multifunction devices and VoIP terminals) of electronic devices. In contrast to the mentioned standards, commercial devices in the field of unwanted electromagnetic emissions are tested only in terms of electromagnetic compatibility requirements (e.g., EN55022, EN61000). Although military requirements are classified, it is known that they are more restrictive than the corresponding requirements of civil standards. Commercial devices available on the market can therefore be a source of electromagnetic emissions, including those compromising, the levels of which may exceed military requirements. It is known (publicly available fragments of NSTISSAM TEMPEST/1-92 and NSTISSAM TEMPEST/2-95) that the American military requirements define three levels of security for devices that could be used in information processing zones, the R rays of which meet the conditions: $R \leq 20$ m, 20 m < $R \leq 100$ m and $R > 100$ m, and the emission levels are to be measured from a distance of 1 m. This measurement distance is also recommended in the document MIL-STD-461G. Thus, it can be concluded that the compromising emission signals produced by commercial devices can be received at distances of several dozen meters. This is confirmed in practical experiments [4], in which it is possible to recover visual information from a distance of about 80 m.

The best known problem related to the issue of electromagnetic revealing emissions is the issue related to the possibility of intercepting visual information presented on the screens of electronic devices, in the particular case of computer monitors. This phenomenon was presented to the public for the first time in 1985 and concerned Cathode-Ray Tube (CRT) monitors [2,10]. Therefore, one might think that liquid-crystal displays (LCD), which are currently dominant on the market, equipped with digital video data transmission interfaces should be free from this threat. However, as experience shows, this is not true [5,12,13]. Digital signals, just like analogue signals [14,15], are sensitive to the electromagnetic infiltration process and enable non-invasive acquisition of processed information. This phenomenon also applies to other digital standards that are used in the processing of information in electrical form [16]. In any case, the sources of undesirable signals must be protected by applying solutions that prevent the effective conduct of the infiltration process [6,17–19].

The aim of the article is to draw attention to the dangers associated with the massive use of computer equipment in remote work. Commercial solutions introduced to classified military and civilian systems are tested according to the relevant requirements (e.g., SDIP-28), the fulfilment of which guarantees an adequate level of protection. Meanwhile, equipment commonly used by employees forced to work remotely is not subjected to such assessments. Both employees and employers should be aware that in such conditions, its use should be characterized by special judgment.

2. Electromagnetic Compatibility and Protection of Information

The issues of electromagnetic protection of processed data are closely related to an electromagnetic compatibility and generation of electromagnetic emissions (disturbances).

During operation, each electronic device becomes a source of electromagnetic fields, which result from the processing of electrical signals and the operation of components of the device. Therefore, such devices must undergo appropriate tests in order to verify that they meet the relevant requirements of the normative documents. In particular, this concerns the limit levels of electromagnetic emissions arising. These are open requirements. Obtained results can be represented by digit values which respond to values of electromagnetic disturbances over limit lines.

Electromagnetic compatibility tests do not require an evaluation of the measured emissions in terms of their correlation with appropriate sources (e.g., for a printer, such sources may be the display, heater, stepper motor) of the tested device. Such a device is considered as a whole.

However, some electromagnetic emissions can be used for other purposes. If the emissions are correlated with the processed information (e.g., for a printer, this is information about the content contained in a printed document), such emissions can be treated as revealing emissions. They can be used in a non-invasive data acquisition process. In this case, the device is tested according to other normative documents. One of such documents is SDIP-27/2, which is a classified document. Then, the research process focuses on the sources of undesirable emissions and allows assessing the device in terms of its possible use in the processing of protected information. Such tests were carried out on VoIP terminal displays and elements of hands-free mode. Due to the nature of the research, not all results are public, as opposed to electromagnetic compatibility tests. In many cases, they require comparison and evaluation with the requirements that are legally protected. Therefore, the article is limited to presenting the existing threats related not only to the popularly used computer displays (described broadly in [1–4,7,9,15]), but also to the displays of VoIP terminals and hands-free mode. In the case of these devices, there is very little information about the electromagnetic safety of the processed information.

3. Test Conditions

Practical tests were carried out in an anechoic chamber (Figure 1). Attenuation parameters of the chamber were not lower than 100 dB in the range of frequencies from 1 MHz to 10 GHz. A DSI-1550-A receiver (Figure 2a) Microwave Downconverter DSI-1580-A (up to 22 GHz) and a set of R&S antennas (Figure 2b) were used to conduct the tests.

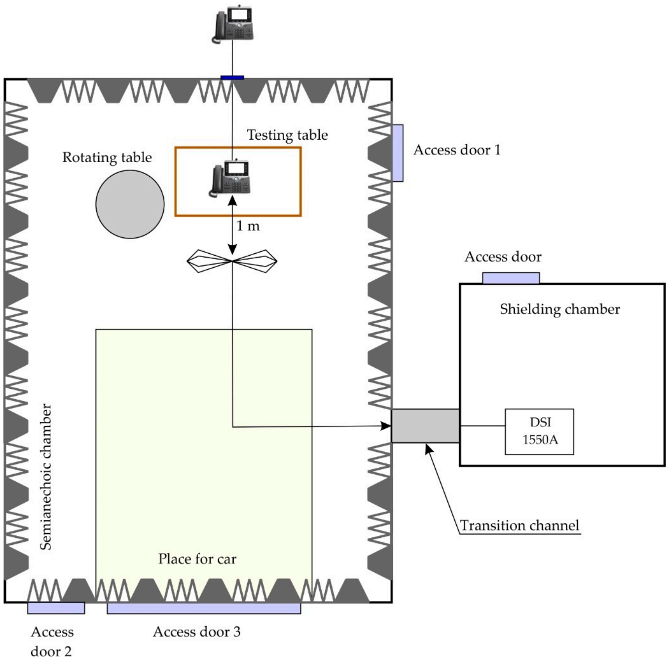
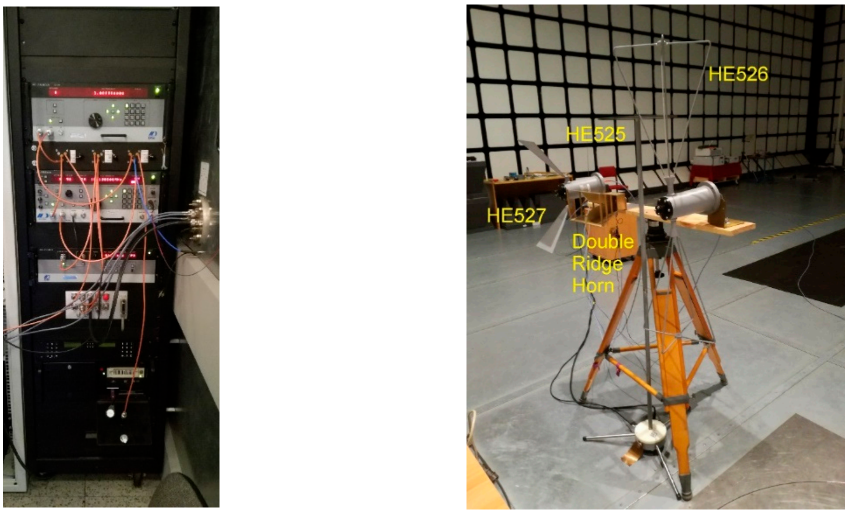


Figure 1. A test system in the field of electromagnetic emissions from the screen of the VoIP terminal in the videoconference mode and for the operation of the VoIP terminal in the hands-free mode.



(**a**) (**b**)

Figure 2. A TEMPEST test system DSI-1550-A (**a**) and antenna system (rod antenna (0.1 kHz–30 MHz), biconical antenna (30–200 MHz), dipole antenna (0.2–1 GHz) and Double Ridge Horn antenna (1–18 GHz) (**b**).

Tested devices were placed on a measuring table. During the tests, the cooperating devices were located outside of the anechoic chamber. The connection between the tested device and the cooperating device was made using a shielded Ethernet Cat.6 cable. Both in the case of VoIP terminals and laptops, during the research of emissions from the audio path, the devices worked in hands-free mode with the use of built-in speakers. The electromagnetic emissions were recorded for a measuring distance of 1 m.

Electromagnetic safety research concerns a variety of electronic devices. In particular, these studies are focused on sources that process data in a graphical manner. In such cases, it is possible to present the reconstructed data also in a graphical manner that is readable and understandable by a human. The effectiveness of undesirable emission sources in the electromagnetic infiltration process depends on many factors, including:

- Voltage (current) amplitude of the primary signal;
- Transmission method (serial, parallel, serial–parallel, differential);
- The effectiveness of emission reduction solutions applied at the source of these emissions (electromagnetic screens, signal and network filters, ferrite filters).

Equipment manufacturers use a variety of solutions primarily to meet the requirements of electromagnetic compatibility. The applied treatments also increase the level of electromagnetic safety of the processed data, but not always. Therefore, it cannot be directly assumed that one or more technological solutions, e.g., signal standards (VGA, DVI/HDMI, DisplayPort), are higher in terms of electromagnetic safety in relation to others. Each device must be assessed and, even more so, so should each design solution that may affect the level of protection of the processed information. The article focuses on VoIP terminal displays or elements of hands-free mode, believing that their common use nowadays should be subject to special caution. Based on the authors' experience, it can be argued that the most effective sources of revealing emission signals are primarily components in which the transmission of the information signal takes place via a wire. Very often cable installations made discordant to the rules (they are exposed to shielding damage or careless assembly and connections) become effective antennas.

4. Tests and Analyses Results

4.1. Theoretical Analysis

The tests focused on the risks associated with the use of typical and widespread monitors with a digital video interface (DVI) or high-definition multimedia interface

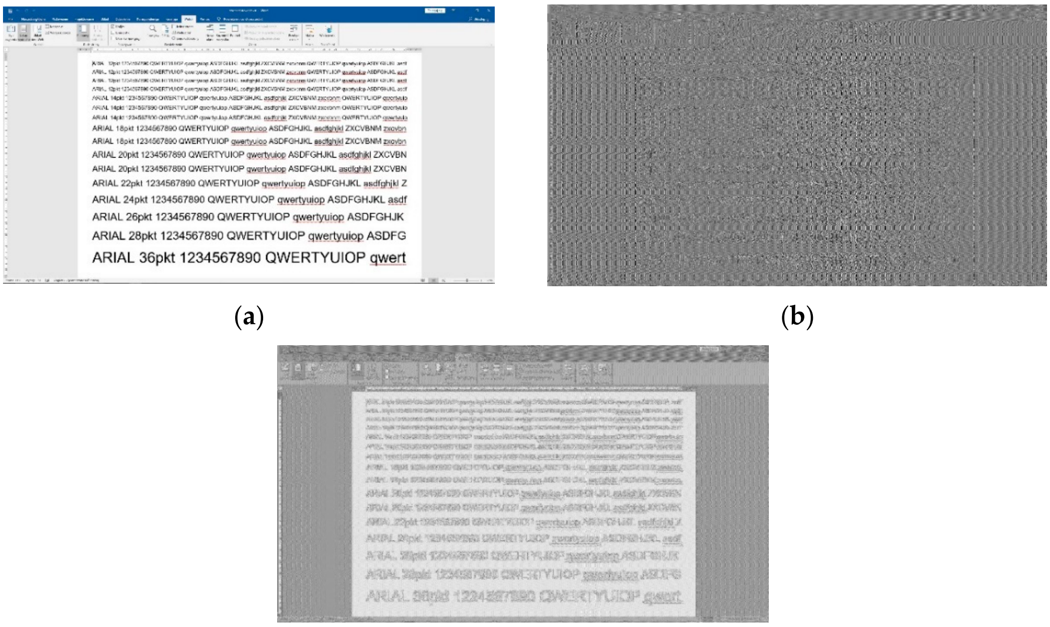
(HDMI) and displays of commercial VoIP terminals. The analogy of VoIP terminal displays with commercial computer monitors is shown from the viewpoint of sensitivity to the process of electromagnetic eavesdropping. In addition, the results of tests of the emissions generated during the processing of audio signals in the mentioned devices—hands-free mode for the VoIP terminals and audio playback on a laptop—are shown, which also become useful in the process of non-invasive data acquisition [20].

4.2. Graphic Data

4.2.1. DVI/HDMI Technology

Currently, LCD monitors with the digital DVI/HDMI interface seem to be the most popular on the market. The output stages of graphics cards are de facto digital chips, and video data could be directly transmitted to digital imaging devices. However, due to the requirements concerning, on the one hand, the transmission speed (required operating mode, i.e., resolution) and, on the other hand, balancing the constant component and minimizing the number of changes in the signal level, they are subjected to 8 b/10 b coding in accordance with the algorithm developed by the Digital Display Working Group (DDWG). This algorithm enables the conversion of 8-bit data describing the color components of a pixel of an image or 2-bit synchronization data into 10-bit code words transmitted in the DVI interface. At this point, it is worth noting that despite the digital nature of the transmission and a fairly advanced encoding mechanism (including the use of two 10-bit representations for most of the 256 possible 8-bit values), it is possible to receive and visualize the information contained in the revealing broadcast generated in the result of the video data transmission [3,21,22]. To produce the visualization, it is not necessary to decode the transmitted data according to the transition-minimized differential signaling (TMDS) algorithm, and the technique of screening received broadcasts, well known since 1985, is sufficient.

Figure 3 shows the effect of the experiment consisting in the software simulation of the effect of the passage of a signal encoded in accordance with the algorithm of the DVI standard through the side channel attack (SCA).


ARIAL 14pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBNM zxcvbnm QWERTYUIOP qwertyuio
ARIAL 18pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBNM zxcvbn
ARIAL 18pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBNM zxcvbn
ARIAL 20pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBN
ARIAL 20pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBN
ARIAL 22pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl Z
ARIAL 24pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdf
ARIAL 26pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJK
ARIAL 28pkt 1234567890 QWERTYUIOP qwertyuiop ASDFG
ARIAL 36pkt 1234567890 QWERTYUIOP qwert

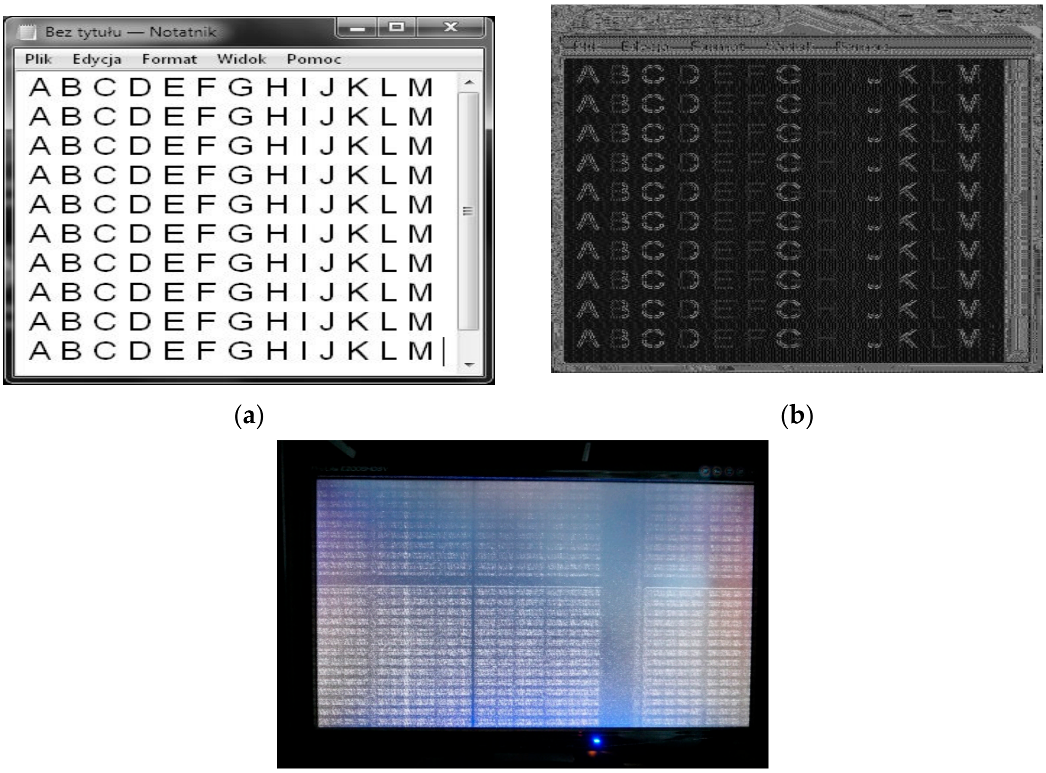
(**a**) (**b**)

(**c**)

Figure 3. A program simulation of the reception of the revealing emission signal resulting from the transmission of the image in the DVI interface: (**a**) reference image, (**b**) image reconstructed from the recorded electrical signal of the DVI/HDMI standard, (**c**) image reconstructed from the recorded electrical signal of the DVI on the output of the theoretical side channel attack (SCA).

While the reconstructed image from raw digital data remains practically unreadable for the human eye, these data subjected to the SCA transfer characteristics (high-pass filter) become readable, especially in the case of standard text data [3].

In the case of a typical computer monitor, it becomes obvious that the security of the data presented on it may be threatened. It also applies to monitors equipped with a DisplayPort (DP) interface, due to their compatibility with other standards and LCD matrix control systems. The information provided to them is decoded to a form compatible with, for example, the LVDS standard [3]. These operations, along with the system of internal video bus connections, become a source of electromagnetic revealing emissions. In Figure 4, the images reconstructed from the revealing emissions generated during the operation of the LCD computer monitor equipped with DVI and DP connectors are presented.


Bez tytułu — Notatnik
Plik Edycja Format Widok Pomoc
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M
A B C D E F G H I J K L M

(**a**) (**b**)

(**c**)

Figure 4. Reconstructed images from revealing emissions arising during working of LCD monitor: (**a**) reference image, (**b**) DVI interface, (**c**) DP interface.

4.2.2. Screen of VoIP Terminal

Internet phones are very popular, especially among business users, for whom not only the operating costs are attractive, but most of all the equipment and the remarkable flexibility of the solution (wireless technology, cloud implementations). VoIP terminals allow making video calls, but sensitive data are not the only content of the call. On the display of the device, apart from the participants of the call, other information may be presented, including the history of calls and details of the device configuration. Important data are also data entered from the keyboard [23].

In the Electromagnetic Compatibility Laboratory of the Military Communication Institute, the security of emissions of various Cisco VoIP phones was tested. At the current stage of research, the authors are not aware of the type of interface that supports displaying information on VoIP terminal screens. However, the size and resolution of the display as well as the quality of the images reproduced from the revealing broadcast signals indicate that it may be an interface of type RGB (TTL). Figure 5 shows exemplary images reconstructed from revealing broadcast signals from the Cisco VoIP Terminal Model 8865 during operation. For comparison, the reference images displayed on the tested devices are also presented (Figure 5).

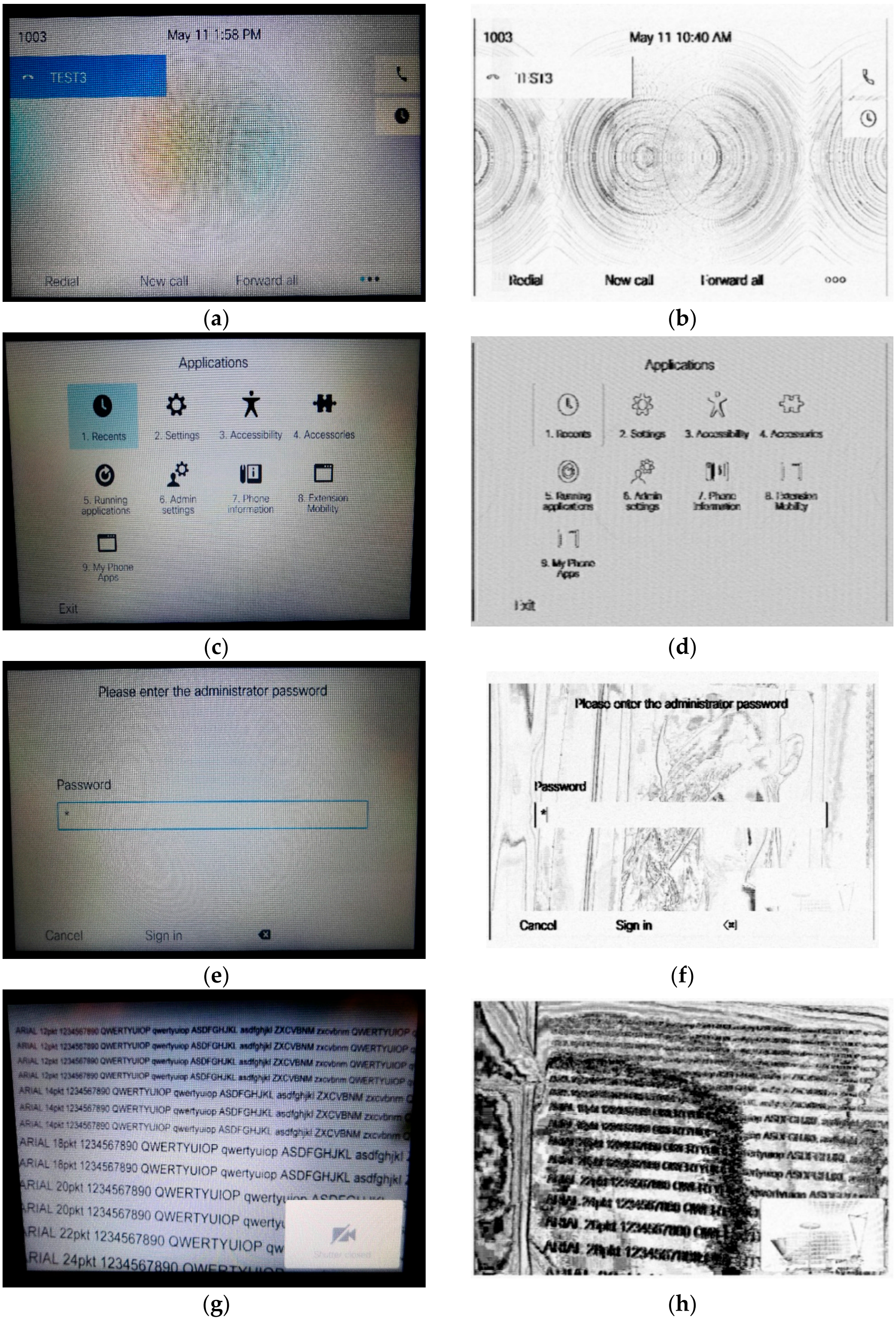

1003
May 11 1:58 PM
TEST3
Redial
New call
Forward all
1003
May 11 10:40 AM
TEST3
Redial
New call
Forward all
Applications
1. Recents
2. Settings
3. Accessibility
4. Accessories
5. Running applications
6. Admin settings
7. Phone information
8. Extension Mobility
9. My Phone Apps
Exit
Please enter the administrator password
Password
Cancel
Sign in
ARIAL 12pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBNM zxcvbnm QWERTYUIOP
ARIAL 14pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl ZXCVBNM zxcvbnm
ARIAL 18pkt 1234567890 QWERTYUIOP qwertyuiop ASDFGHJKL asdfghjkl
ARIAL 20pkt 1234567890 QWERTYUIOP qwertyuiop
ARIAL 22pkt 1234567890 QWERTYUIOP
ARIAL 24pkt 1234567890 QWERTYUIOP
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)

Figure 5. The four original different images presented on the VoIP phone display: (**a**) main screen, (**c**) applications, (**e**) password, (**g**) text captured by the internal camera of the cooperating device and corresponding images (**b**,**d**,**f**,**h**) recreated from the signals of the compromising emanation measured at a frequency f_o = 800 MHz, BW = 20 MHz.

The revealing emissions from the VoIP terminal display systems enabling the reconstruction of their content were recorded in the frequency range from 600 to 800 MHz, in the 50 MHz measurement band. Figure 6 shows the waveforms showing the levels of electromagnetic emissions from two tested devices.

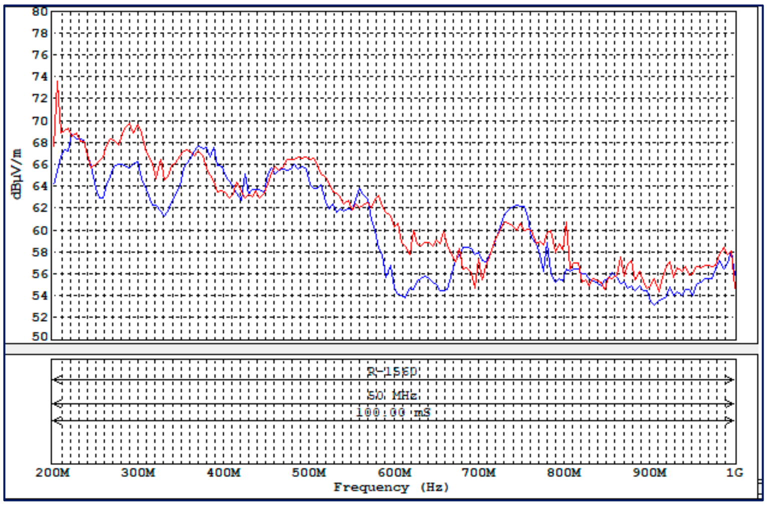
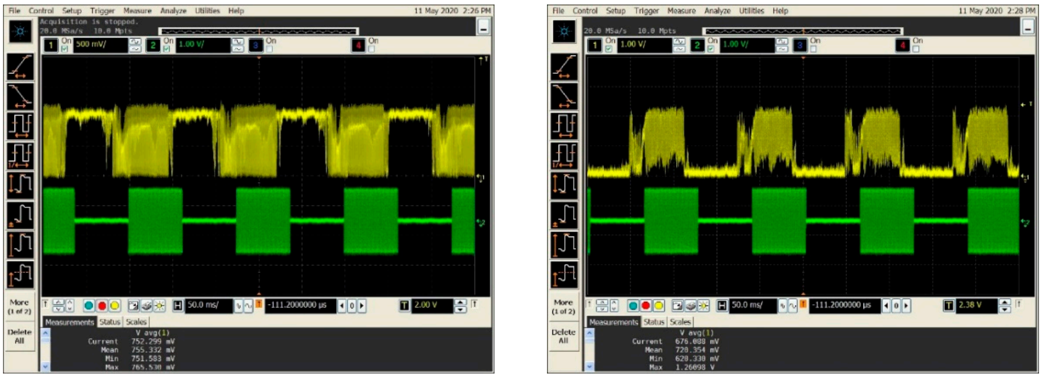


Figure 6. Electromagnetic emissions for two tested VoIP terminals: *BW* = 50 MHz.

4.3. Audio Data

4.3.1. VoIP Terminal—Hands-Free Mode

The use of VoIP terminals may also pose a threat to the confidentiality of the conversation. An attractive feature of this type of device is the possibility of using the hands-free mode, providing the user with greater freedom of movement and freeing them from the need to hold the handset. However, it turns out that in this mode of operation, these devices become sources of additional electromagnetic emissions, which can have features of revealing emissions. During the tests, a strong correlation of the envelope (Figure 7) of the received signals and the envelope of the excitation signal was observed. The excitation signal was an acoustic signal obtained by stimulating an additional loudspeaker with an electrical signal in the form of a sinusoidal waveform with a frequency equal to 1 kHz, keyed by a square wave with a frequency equal to 8 Hz.



```
11 May 2020 2:26 PM
Acquisition is stopped.
20.0 MSa/s   10.0 Mpts
1 On 500 mV/   2 On 1.00 V/   3 On   4 On
H 50.0 ms/   -111.2000000 µs   T 2.00 V
              V avg(1)
     Current  752.299 mV
        Mean  755.332 mV
         Min  751.583 mV
         Max  765.538 mV
```

(**a**)

```
11 May 2020 2:28 PM
20.0 MSa/s   10.0 Mpts
1 On 1.00 V/   2 On 1.00 V/   3 On   4 On
H 50.0 ms/   -111.2000000 µs   T 2.38 V
              V avg(1)
     Current  676.088 mV
        Mean  728.354 mV
         Min  628.338 mV
         Max  1.26098 V
```

(**b**)

Figure 7. Time courses of received revealing emissions (yellow) and an excitation signal stimulating an additional loudspeaker, f_0 = 6.45 MHz, *BW* = 5 kHz, (**a**,**b**) two examples of compromising emanations.

The occurrence of this type of emission was observed in a fairly wide range of frequencies—the strongest emissions were recorded in the range from 20 to 40 MHz.

Figure 8 shows the graphs showing the levels of the electromagnetic emissions from two tested devices.

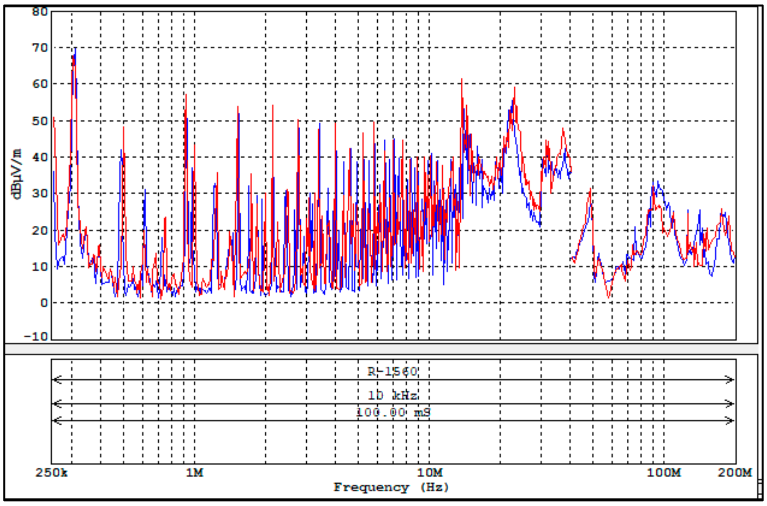


Figure 8. Electromagnetic emissions for two tested VoIP terminals: *BW* = 10 kHz—hands-free mode.

4.3.2. Laptop–Sound from Interior Speaker

The phenomenon of electromagnetic emissions, which may be features of revealing emissions correlated with acoustic signals, was also observed in the case of using devices such as a PC or laptop. Figure 9 shows a comparison of the levels of electromagnetic emissions from a laptop during the playback of an audio file and in the absence of it. There is a clear increase in the emission level associated with playing sound files through the built-in speakers.

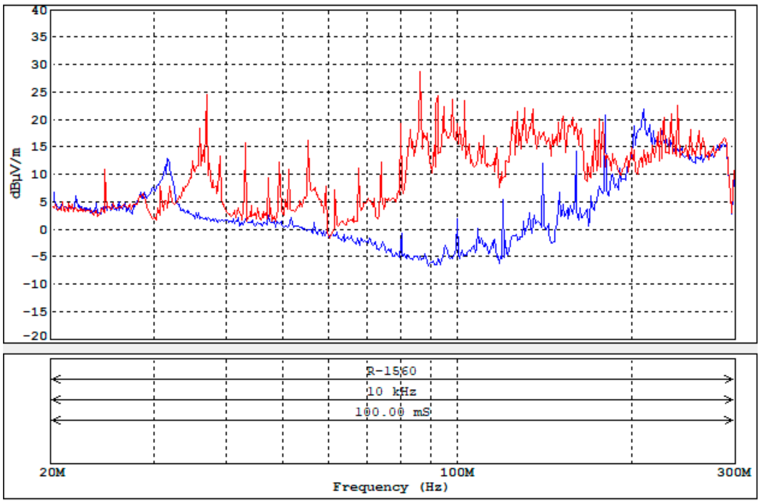
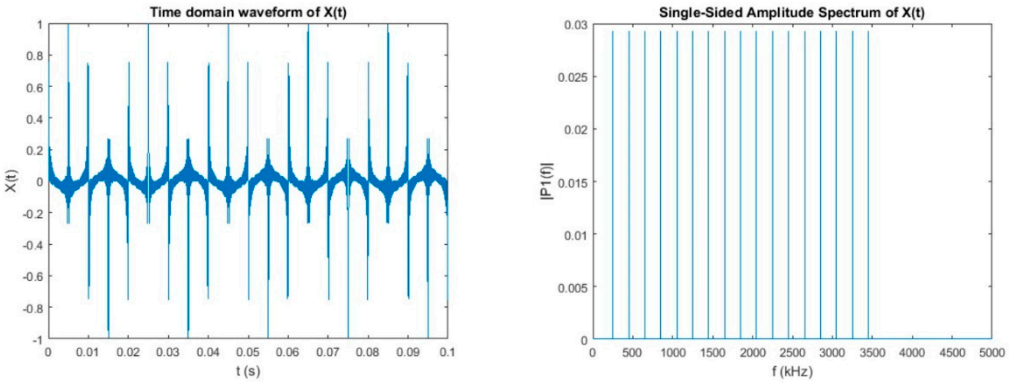


Figure 9. Comparison of levels of electromagnetic emissions measured from laptop during the playback of an audio file (red course) and in the absence of it (blue course), *BW* = 10 kHz.

In order to estimate of the correlation level of the received emissions with the original acoustic signal, measurements were conducted for three types of signals:

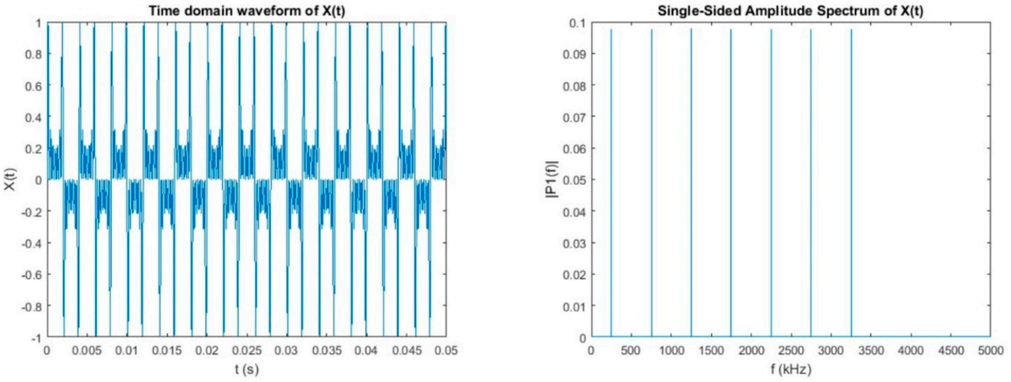
- A signal which is the sum of harmonic waveforms for frequencies in the range from 250 Hz to 3.5 kHz, changing with a step of 200 Hz;
- A signal which is the sum of harmonic waveforms for frequencies in the range from 250 Hz to 3.5 kHz, changing with a step of 500 Hz;
- Speech signal.

For such constructed test signals, their time courses and amplitude spectra obtained from the samples contained in *.wav sound files (Figures 10–12) were visualized.



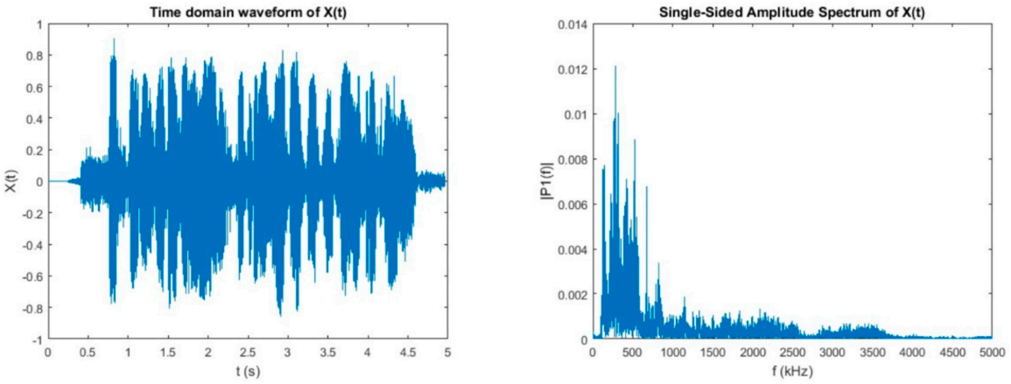
(**a**) (**b**)

Figure 10. Time course (**a**) and amplitude spectrum (**b**) of test signal (*f* = 200 Hz)—*.wav file.



(**a**) (**b**)

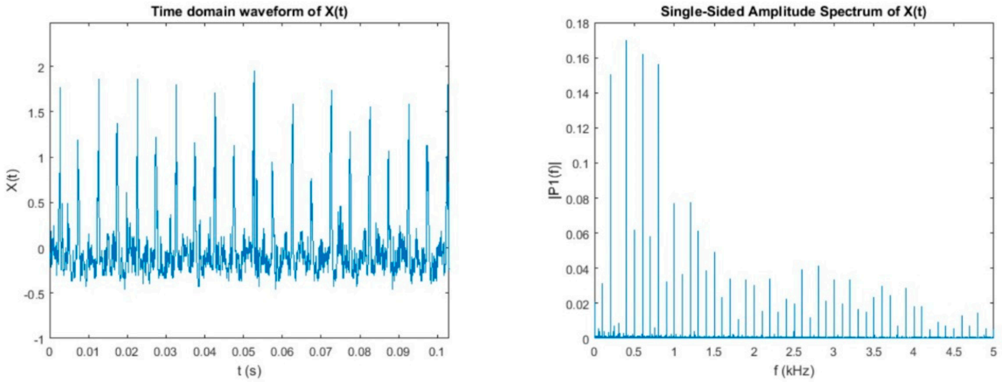
Figure 11. Time course (**a**) and amplitude spectrum (**b**) of test signal (*f* = 500 Hz)—*.wav file.



(**a**) (**b**)

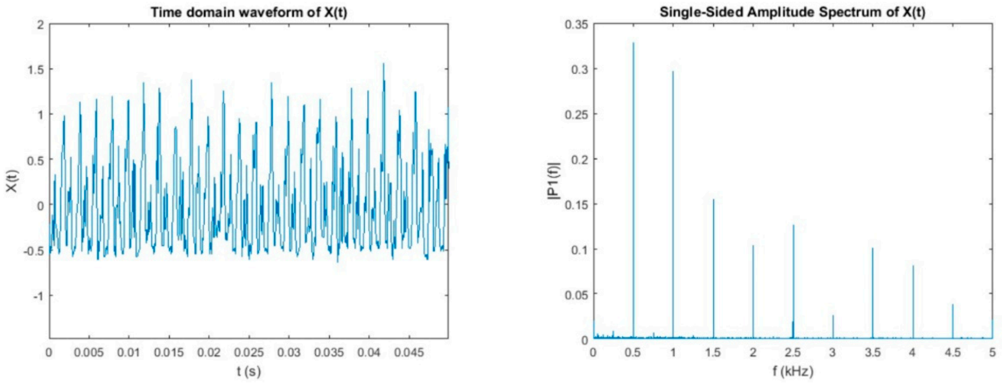
Figure 12. Time course (**a**) and amplitude spectrum (**b**) of test signal *speech*—*.wav file.

Imaging of the time courses and the amplitude spectra of the received emissions on the basis of samples of signals recorded at the audio output of the measuring receiver was proposed. The search for correlated emissions was carried out for both the FM and AM modulation reception modes. Sample results are shown in Figures 13–16. For comparison, the results obtained by sampling the signals directly at the headphone output of the tested laptop are also presented (Figures 17–19).



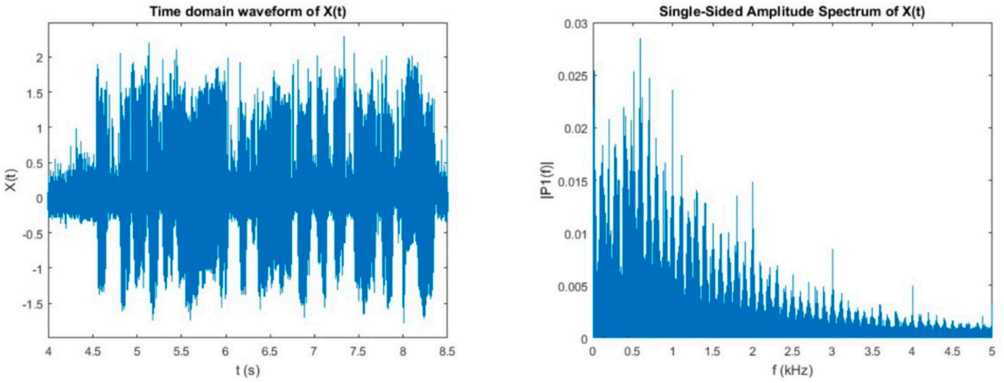
(**a**) (**b**)

Figure 13. Time course (**a**) and amplitude spectrum (**b**) of test signal (f = 200 Hz) recorded on the audio output of the receiver, f_o = 109.2 MHz, BW = 300 kHz, FM reception.



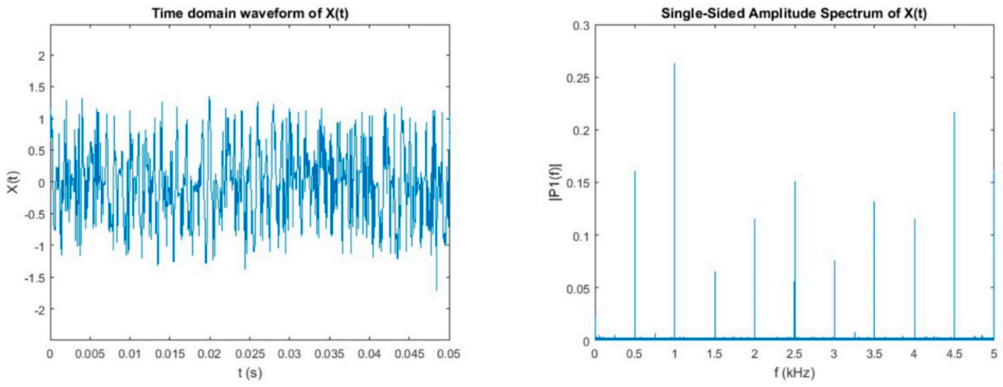
(**a**) (**b**)

Figure 14. Time course (**a**) and amplitude spectrum (**b**) of test signal (f = 500 Hz) recorded on the audio output of the receiver, f_o = 109.2 MHz, BW = 300 kHz, FM reception.



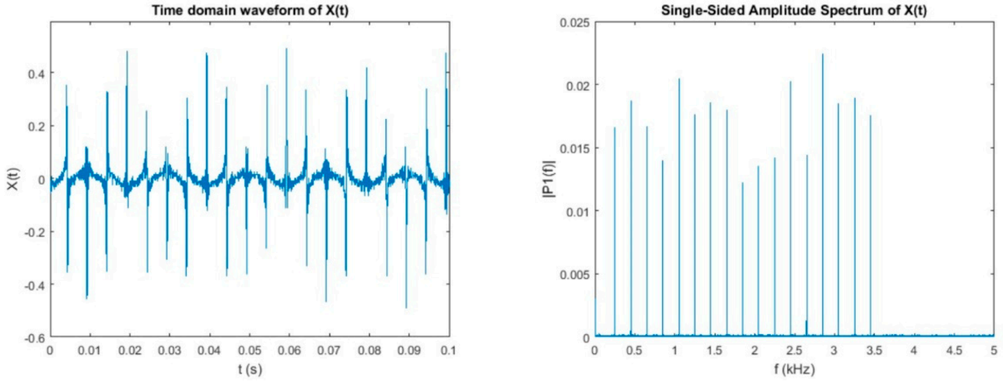
(**a**) (**b**)

Figure 15. Time course (**a**) and amplitude spectrum (**b**) of test signal *speech* recorded on the audio output of the receiver, f_o = 109.2 MHz, BW = 300 kHz, FM reception.



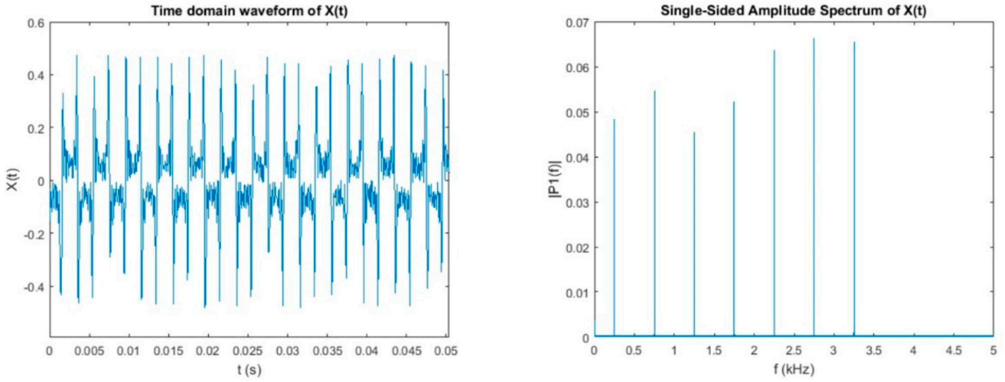
(**a**) (**b**)

Figure 16. Time course (**a**) and amplitude spectrum (**b**) of test signal (*f* = 500 Hz) recorded on the audio output of the receiver, f_o = 123.6 MHz, *BW* = 20 kHz, AM reception.



(**a**) (**b**)

Figure 17. Time course (**a**) and amplitude spectrum (**b**) of test signal (*f* = 200 Hz) recorded on the earphone output of the laptop.



(**a**) (**b**)

Figure 18. Time course (**a**) and amplitude spectrum (**b**) of test signal (*f* = 500 Hz) recorded on the earphone output of the laptop.

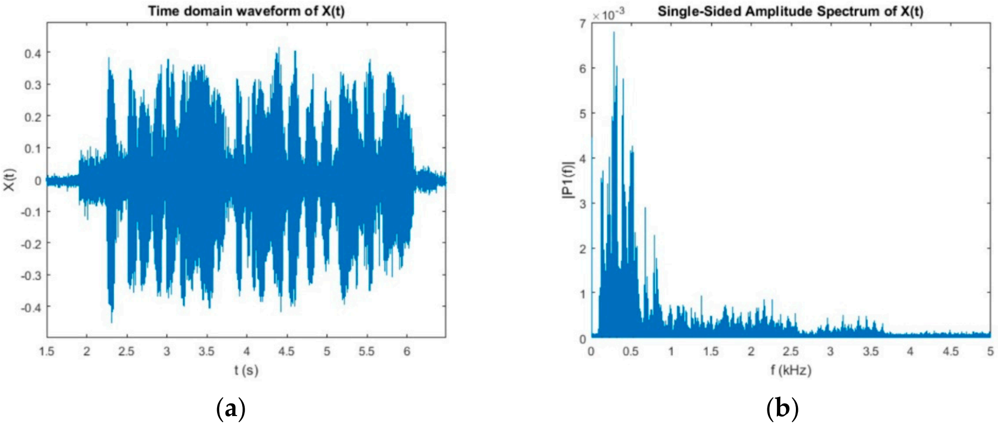


Figure 19. Time course (**a**) and amplitude spectrum (**b**) of test signal *speech* recorded on the earphone output of the laptop.

5. Conclusions

Much space is devoted to the protection of information in terms of the use of commercial graphic display devices for processed data. This mainly applies to computer monitors which use different graphic standards (VGA, DVI, HDMI, DisplayPort), laser printers with different solutions of photosensitive drum exposure systems [7] or optical systems based on LED diodes [24]. Each of the mentioned devices in commercial execution becomes a source of sensitive emissions with distinctive features which allow a non-invasive acquisition of information and presentation of it in a graphic form which can be understandable for humans. Devices not as popular as the mentioned devices are of less interest in the area of analyses related to the risk of loss of confidentiality. We mean devices such as VoIP terminals with a screen or audio circuits. These are solutions very often used to organize connections, such as so-called videoconferencing. Information is often presented during remote meetings, which should also be subject to certain protection against disclosure to a wider group of people.

The article presented the results of tests and analyses related to the screen of a VoIP terminal as the source of unwanted emissions and also the audio systems of a hands-free VoIP terminal and a laptop. In each case, the levels of electromagnetic emissions were measured, and at selected frequencies, analyses of the correlation between the emissions and the processed graphic or sound information were carried out. Electromagnetic emissions correlated with the graphic information of the terminal screen, allowing the reproduction of this information, similarly to computer monitors. The data contained in the reconstructed images are clear and easy to read. In the case of electromagnetic emissions, an increase in the levels of the electromagnetic emissions can be noticed for the hands-free mode (VoIP terminal) and during the playback of the audio file on the laptop.

For the hands-free mode, the occurrence of revealing emissions has been observed in a fairly wide range of frequencies. The highest levels of these emissions were recorded in the range from 20 to 40 MHz. In turn, for the sounds played on the laptop, a correlation of the received emissions with the original acoustic signal, for different test signals, was noticed.

The occurring phenomena confirm the earlier assumptions of the authors of the article related to the risk of loss of confidentiality, e.g., calls in videoconference mode. This mode of operation of VoIP terminals poses a threat related to electromagnetic eavesdropping not only of graphic data but also of audio data. This is a very dangerous phenomenon because the combination of graphics and sound can undoubtedly contain much more protected data than just graphics or sound only.

The next stage of the works in the area presented in the article will concern the possibility of reproducing sounds from the recording of electromagnetic emissions both for the hands-free mode (VoIP terminal) and for listening to an audio file on a laptop. Moreover, attempts will be made to propose solutions counteracting this phenomenon.

Reproducing information from the signals of revealing emissions resulting from image or sound processing does not require access to high-class equipment. As the experiments conducted by the authors have shown, in the case of audio signals, a simple home radio receiver may suffice to capture them from a distance of few meters. Of course, it should enable the reception of radio signals in a wide frequency range (LW, MW, SW and FM bands). Equipping it with appropriate, better-quality antennas would probably increase the reception range to several meters. In the case of video signals, the use of broadband programmable radio modules with an ADC converter card allows implementing a digital image rastering method with an algorithm for improving its quality by summation. For the purposes of the analysis, the authors used a laboratory measuring set, and all measurements were made from a distance of 1 m. The measuring receiver has AM and FM detectors and also allows the user to record the received signal. Signal samples stored in disk files were used to restore video information using the digital rastering method. In the case of audio signal tests, two types of inputs were used, recorded as *.wav files:

- Speech signal;
- A signal in the form of the sum of the sinusoidal waveforms with specific frequencies in the range 100–4000 Hz.

Author Contributions: Conceptualization, A.P., K.G. and I.K.; methodology, A.P.; validation, A.P., I.K. and K.G.; formal analysis, A.P., I.K. and K.G.; investigation, A.P. and I.K.; data curation, A.P. and K.G.; writing—original draft preparation, A.P. and I.K.; writing—review and editing, A.P., I.K. and K.G.; visualization, A.P. and I.K.; supervision, I.K.; project administration, I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Kuhn, M.G. Electromagnetic eavesdropping risks of at-panel displays. In Proceedings of the 4th Workshop on Privacy Enhancing Technologies, Toronto, ON, Canada, 26–28 May 2004; pp. 88–105.
2. van Eck, W. Electromagnetic radiation from video display units: An eavesdropping risk? *Comput. Secur.* **1985**, *4*, 269–286. [CrossRef]
3. Kuhn, M.G. *Compromising Emanations: Eavesdropping Risks of Computer Displays*; University of Cambridge Computer Laboratory: Cambridge, UK, 2003.
4. De Meulemeester, P.; Scheers, B.; Vandenbosch, G.A.E. Eavesdropping a (ultra-)high-definition video display from an 80 meter distance under realistic circumstances. In Proceedings of the 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), Reno, NV, USA, 27–31 July 2021.
5. Guri, M.; Elovici, Y. Exfiltration of information from air-gapped machines using monitors LED indicator. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, Hague, The Netherlands, 24–26 September 2014; pp. 264–267.
6. Kuhn, M.G. Optical time-domain eavesdropping risks of CRT displays. In Proceedings of the 2002 IEEE Symposiumon Security and Privacy, Berkeley, CA, USA, 12–15 May 2002; pp. 3–18.
7. Kubiak, I.; Przybysz, A.; Musial, S. Possibilities of electromagnetic penetration of displays of multifunction devices. *Computers* **2020**, *9*, 62. [CrossRef]
8. Mavroeidis, V.; Vishi, K.; Zych, M. The impact of quantum computing on present cryptography. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 405–414. [CrossRef]
9. Kubiak, I. LED printers and safe fonts as an effective protection against the formation of unwanted emission. *Turk. J. Electr. Eng. Comput. Sci.* **2017**, *25*, 4268–4279. [CrossRef]
10. Mahshid, Z.; Saeedeh, H.T.; Ayaz, G. Security limits for electromagnetic radiation from CRT display. In Proceedings of the Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 28–30 January 2009; pp. 452–456.

11. Meynard, O.; Réal, D.; Guilley, S.; Flament, F.; Danger, J.L.; Valette, F. Characterization of the electromagnetic side channel in frequency domain. In Proceedings of the Information Security and Cryptology International Conference—Lecture Notes in Computer Science, Shanghai, China, 20–24 October 2010; Abstract No. 6584, pp. 471–486.
12. Li, X.; Xu, S.; Hua, X. Pattern recognition of grating perimeter intrusion behaviour in deep learning method. *Symmetry* **2021**, *13*, 87. [CrossRef]
13. Song, T.L.; Jong-Gwan, Y. Study of jamming countermeasure for electromagnetically leaked digital video signals. In Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, Gothenburg, Sweden, 1–4 September 2014. [CrossRef]
14. Zhang, N.; Yinghua, L.; Qiang, C.; Yiying, W. Investigation of unintentional video emanations from a VGA connector in the desktop Computers. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1826–1834. [CrossRef]
15. Boitan, A.; Kubiak, I.; Halunga, S.; Przybysz, A.; Stańczak, A. Method of colors and secure fonts in aspect of source shaping of valuable emissions from projector in electromagnetic eavesdropping process. *Symmetry* **2020**, *12*, 1908. [CrossRef]
16. Sim, D.; Lee, H.S.; Yook, J.G.; Sim, K. Measurement and analysis of the compromising electromagnetic emanations from USB keyboard. In Proceedings of the 7th Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Shenzhen, China, 17–21 May 2016; Volume 1, pp. 518–520.
17. Levina, A.; Mostovoi, R.; Sleptsova, D.; Tcvetkov, L. Physical model of sensitive data leakage from PC-based cryptographic systems. *J. Cryptogr. Eng.* **2019**, *9*, 393–400. [CrossRef]
18. Ometov, A.; Levina, A.; Borisenko, P.; Mostovoy, R.; Orsino, A.; Andreev, S. Mobile social networking under side-channel attacks: Practical security challenges. *IEEE Access* **2017**, *5*, 2591–2601. [CrossRef]
19. De Mulder, E.; Buysschaert, P.; Örs, S.B.; Delmotte, P.; Preneel, B.; Vandenbosch, G.; Verbauwhede, I. Electromagnetic analysis attack on an FPGA implementation of an elliptic curve cryptosystem. In Proceedings of the International Conference on Computer as a Tool (EUROCON), Belgrade, Serbia, 21–24 November 2005; pp. 1879–1882.
20. Kubiak, I.; Przybysz, A.; Stanczak, A. Usefulness of acoustic sounds from 3D printers in an eavesdropping process and reconstruction of printed shapes. *Electronics* **2020**, *9*, 297. [CrossRef]
21. Genkin, D.; Pachmanov, L.; Pipman, I.; Tromer, E. Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation. In Proceedings of the Cryptographic Hardware and Embedded Systems (CHES)—Lecture Notes in Computer Science, Saint-Malo, France, 13–16 September 2015; Abstract No. 9293, pp. 207–228.
22. Prvulovic, M.; Zajic, A.; Callan, R.L.; Wang, C.J. A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 34–42. [CrossRef]
23. Genkin, D.; Pachmanov, L.; Pipman, I.; Tromer, E.; Yarom, Y. Key extraction from mobile devices via nonintrusive physical side channels. In Proceedings of the SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016.
24. Loughry, J. ("Oops! Had the silly thing in reverse")—Optical injection attacks in through LED status indicators. In Proceedings of the International Symposium and Exhibition on Electromagnetic Compatibility EMC Europe, Barcelona, Spain, 2–6 September 2019.