On the Possibilities of Reconstructing Images of Textual Documents Obtained by Detecting Compromised Emanation from Computer Monitors

Borko Đaković[1][0009-0000-4662-3981], Nenad Stojanović[2][0000-0001-9328-5348], Milena Grdović[3][0000-0003-4310-7935] and Jasmina Kovačević[4][0009-0009-7139-0126]

[1] University of Belgrade, School of Electrical Engineering and Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia
[2] University of Defence, Military Academy and Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia
[3] Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia
[4] University of Defence, Military Academy, Belgrade, Republic of Serbia
borko.djakovic@vs.rs
nivzvk@hotmail.com
milena.grdovic@gmail.com
dzesmin_89@hotmail.com

Abstract. The paper shows the feasibility of reconstructing signals from a computer monitor by intercepting its compromising electromagnetic radiation. For the detection and reconstruction process, the pixel clock frequency of the HDMI interface was utilized. Based on this pixel frequency, its integer multiples were calculated, and the corresponding center frequencies were used to detect the unintended emissions. Reconstructed images are presented across six different frequency bands, representing the spectral harmonics of the pixel clock frequency. Furthermore, the paper discusses protective measures to prevent the leakage of sensitive information via compromising electromagnetic emanations.

Keywords: Compromised Emanation, HDMI, Monitors, TEMPEST.

1 Introduction

Modern society is entirely surrounded by electronic devices. These include mobile phones, tablets, and computers, and other smart devices and sensors in households, industry, traffic. All are part of smart home and smart city projects, as well as the concepts of the Internet of Things (IoT) and the Internet of Everything (IoE). In such an environment, a large amount of data is transmitted. A significant portion of this data is security-sensitive. In these situations, information security becomes important, and the application of cryptographic solutions is crucial [1]. However, from an information security perspective, even with cryptographic solutions, sensitive information can still leak. This leakage occurs due to signals emanating from electronic devices before any cryptographic protection is applied [2][3]. This is referred to as Transient Electromagnetic Pulse Emanation Standards (TEMPEST) security. In this way, data is compromised despite the various protection [4].

Research Paper
DOI: https://doi.org/10.46793/BISEC25.230DJ
Part of ISBN: 978-86-89755-40-4

The beginnings of signal detection and reconstruction from unintended device emissions emerged during World War I. The German military intercepted Allied voice communications by tapping into the earth return circuits of their field telephones. After discovering this eavesdropping method, the US Army initiated a project aimed at finding protection for data that could be collected through compromised emissions. These projects were strictly confidential, and a large portion of the results has remained unavailable to the wider scientific community to this day [5].

Regarding the academic community, the first research results appeared in the mid-1980s. The reconstruction of images from Cathode Ray Tube (CRT) screens at a distance using low-cost, home-built equipment was demonstrated in [6]. This was the first time the general public's attention was drawn to this phenomenon. Research in this field has developed in recent years, and the findings are now available to the wider scientific community. This is of exceptionally importance for developing simple and effective protection methods.

Furthermore, signals successfully reconstructed from side-channel attacks have been documented for various other devices, including different types of monitors [7][8][9], keyboards [10][11], power cables [12], multifunction devices [13], surveillance cameras [14], USB storage devices [15], projectors [16], and laser printers [17]. It has also been shown that the characteristics of the detected signals can be enhanced in post-processing [18].

The aim of this paper is to show that the detection of compromising emanations and subsequent signal reconstruction can be performed across several different spectral sub-bands using a Software-Defined Radio (SDR). Furthermore, it is important to highlight protective measures against potential information leakage through unintended electromagnetic radiation from electronic devices.

Section 2 provides a brief description of the video standards used for displaying images on computer monitors. Section 3 describes used emission measurement setup. The obtained results are presented in Section 4, while the most important conclusions are highlighted in Section 5.

2 Video Standards

2.1 VESA and CEA (CTA) Standards

The Video Electronics Standards Association (VESA) and Consumer Electronics Association (CEA), now known as the Consumer Technology Association (CTA) represent a set of standards that define the Display Monitor Timing (DMT) for a range of different resolutions used by computer monitors, televisions, and home devices.

For different video signal display formats, the standards define the frame rate, the horizontal frequency, and the pixel frequency. The horizontal frequency determines the rate at which a scan line is drawn on the screen, and the pixel frequency defines the rate at which pixels are drawn. In addition to defining the dimensions of the active video transmission, the standards also specify the dimensions of the blanking pixels, which are used for image synchronization. For example, according to the CEA-861

standard, one of the most commonly used monitor's resolution is 1920×1080 pixels with a frame rate of 60 Hz, a pixel frequency of 148.5 MHz, and a horizontal frequency of 67.5 kHz, resulting in a total screen resolution, including blanking pixels, of 2200×1125 pixels.

2.2 HDMI

The High Definition Multimedia Interface (HDMI) is the standard which is used for transmitting video from a computer to a monitor. The HDMI contains multiple communication channels, such as Transition Minimized Differential Signaling (TMDS), Display Data Channel (DDC), Audio Return Channel (ARC), HDMI Ethernet Channel (HEC), and Consumer Electronics Control (CEC). For the purpose of video display, the TMDS channels are of primary interest.

The TMDS channels are used for transmitting packets of audio, video, and auxiliary data. During the video data period, information related to pixel display is transmitted, while during the blanking period, audio and auxiliary data are transmitted. HDMI utilizes four TMDS channels: three channels for each of the color components (red, green, and blue) and one clock channel. Each channel consists of three conductors and employs a differential signaling principle. There is one conductor for the signal, another for the differential (inverted) signal, and a third for the ground. This design ensures signal robustness against noise because, on the receiver's side, the noise is suppressed on the differential signal [19].

Each pixel consists of a 10-bit packet: 8 bits for color intensity and 2 control bits. The first control bit determines whether an XOR or XNOR function has been performed on the 8-bit packet to reduce signal transitions. If the packet contains fewer than 4 logical ones, XOR is applied; otherwise, XNOR is used. If there is an equal number of logical ones and zeros, XOR is applied if the first bit is a logical one, and XNOR if it is a logical zero. The 9th control bit takes the value 1 if XOR was performed, or 0 if XNOR was performed. The 10th control bit indicates whether bit inversion was performed to maintain the DC bias. It checks the difference in the number of logical ones in previously transmitted pixels and inverts the bits if necessary. Bit inversion is performed if both the current and the cumulative running disparity are either greater than or less than zero [20].

2.3 Electromagnetic Radiation

Unintentional electromagnetic radiation occurs during the transition state, specifically during the switch from a logical zero to a logical one and vice versa. Detecting this radiation enables the reconstruction of the image displayed on the monitor. During detection, sampling of the average radiated power per pixel is performed, which determines the pixel intensity of the reconstructed image [21][22].

3 Emission Measurement Setup

Compromising electromagnetic radiation from a computer monitor was captured under laboratory conditions using a log-periodic antenna and a SDR as shown in Fig.

1. As pointed out in [18], white Gaussian noise dominates the test environment. For the research purposes, a monitor with a resolution of 1920×1080 pixels and a 60 Hz frame rate was used, which standardization is described in the previous section.

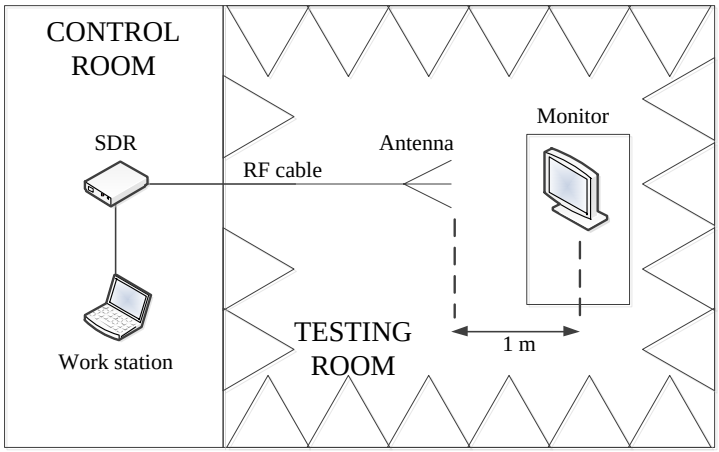


Fig. 1. Laboratory setup for compromised emission measurement.

The log-periodic antenna, vertically polarized with an operational range of 250 MHz to 1300 MHz and a gain of up to 5 dBi, was positioned 1 meter away and directed toward the rear of the monitor, where a vertically oriented HDMI connector was located, connected to an HDMI cable. The HDMI cable extended vertically below the plane of the desk on which the monitor was placed and was connected to a Raspberry Pi, which served as the signal source for transmitting the image to the monitor.

For the purposes of the research, an Ethus Research USRP x310 SDR was used, with an operational frequency of 0 to 6 GHz, and baseband bandwidth up to 200 MHz. I/Q signal samples were captured and subsequently processed for image reconstruction.

The pixel frequency can be defined as:

$$f_p = X \cdot Y \cdot FR \tag{1}$$

where X is the total number of vertical lines, Y is the total number of horizontal pixels (including blanking pixels), and FR represents the frame rate. For the monitor used in this work, the pixel frequency is $f_p = 2200 \cdot 1125 \cdot 60 = 148.5$ MHz.

Signal detection was performed at center frequencies corresponding to integer multiples of the pixel frequency. Images were reconstructed from the 3rd to the 8th harmonic, corresponding to center frequencies (f_c) of: 445.5 MHz, 594 MHz, 742.5 MHz, 891 MHz, 1039.5 MHz, and 1188 MHz. The number of samples was reduced to achieve a sampling rate corresponding to the number of pixels per second. This ensures that the intensity of a single sample corresponds to the average radiated power per pixel. After determining the number of pixels per frame and per image line [21], the

samples were reorganized, mapped to the range [0, 1], and the reconstructed image can be displayed.

4 Results

The obtained results are presented through reconstructed screen images. Fig. 2 shows a screen image that was detected and reconstructed via compromising electromagnetic radiation. The image depicts a text file being processed on a computer monitor. It shows text in various sizes and colors, as well as text highlighted with different colors.

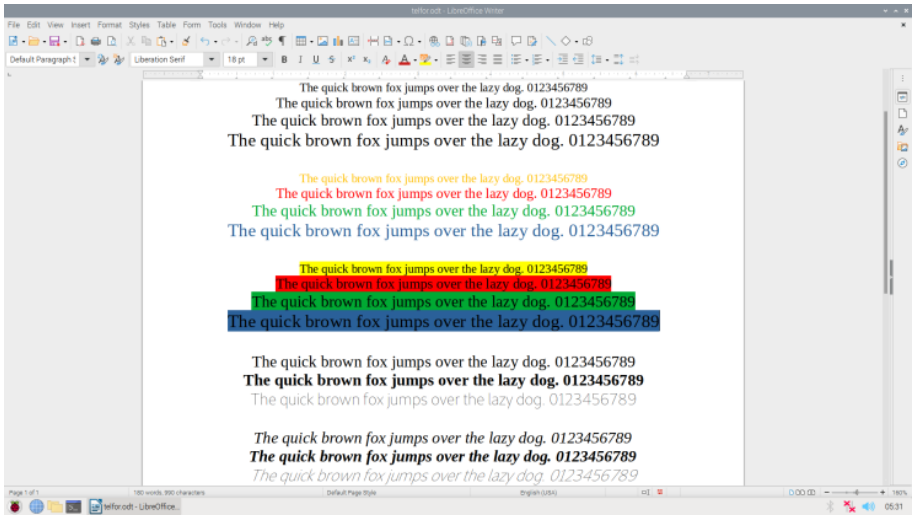
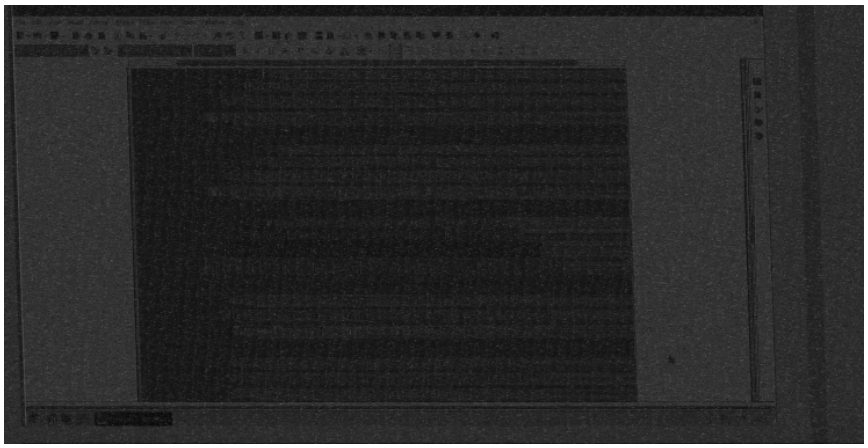


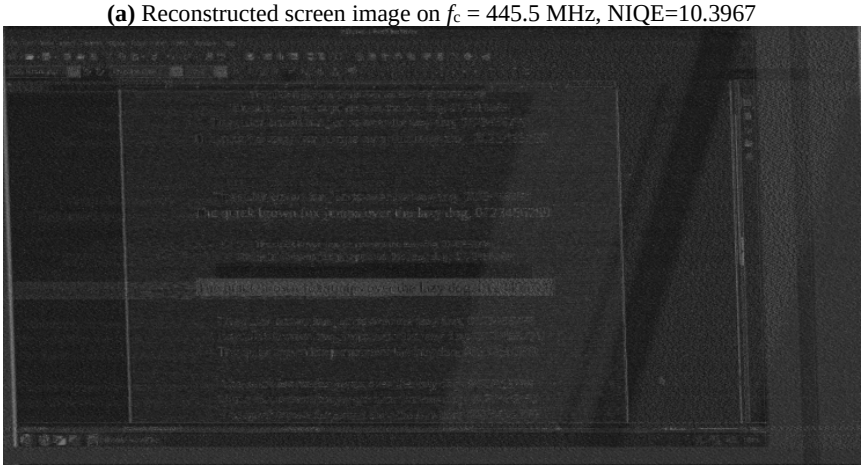
Fig. 2. Original screen image

Fig. 3 displays the reconstructed images. Each image was reconstructed at a different center frequency, which is indicated alongside the respective figure. It can be observed that the images reconstructed at lower frequencies are of poorer quality and darker. The contours of the text being processed are very difficult to discern in these images. However, at higher frequencies, the reconstructed images are of better quality and significantly brighter, which allows for insight into the text being processed.

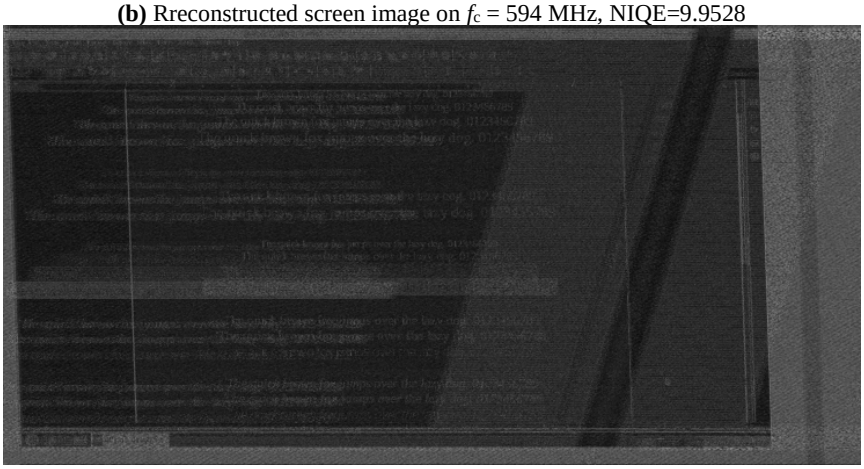
To confirm the author's observations, an objective quality assessment metric called the Natural Image Quality Evaluator (NIQE) was used. The obtained results are presented alongside the corresponding image in Fig. 3. For this metric, lower values indicate better objective quality. Consequently, the best objective quality was obtained for the image reconstructed at f_c = 1039.5 MHz, which aligns with the subjective observations where the processed text is most legible. It should be noted here that during measurements under controlled laboratory conditions, the noise level does not change; therefore, very similar results are obtained even for different images displayed



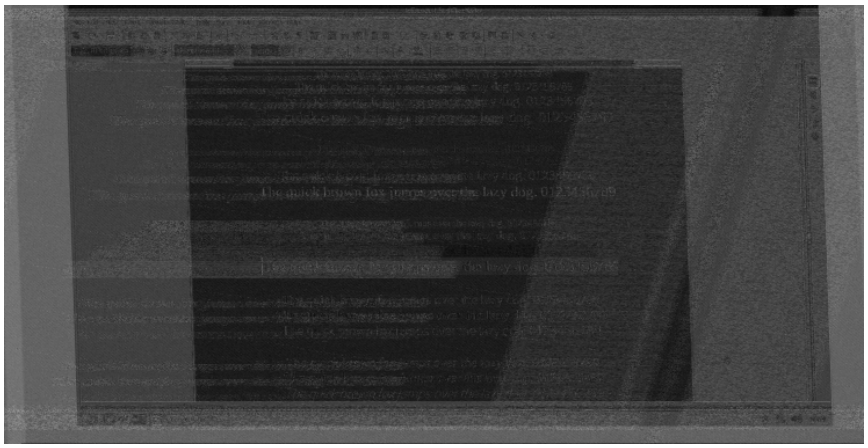
(a) Reconstructed screen image on f_c = 445.5 MHz, NIQE=10.3967



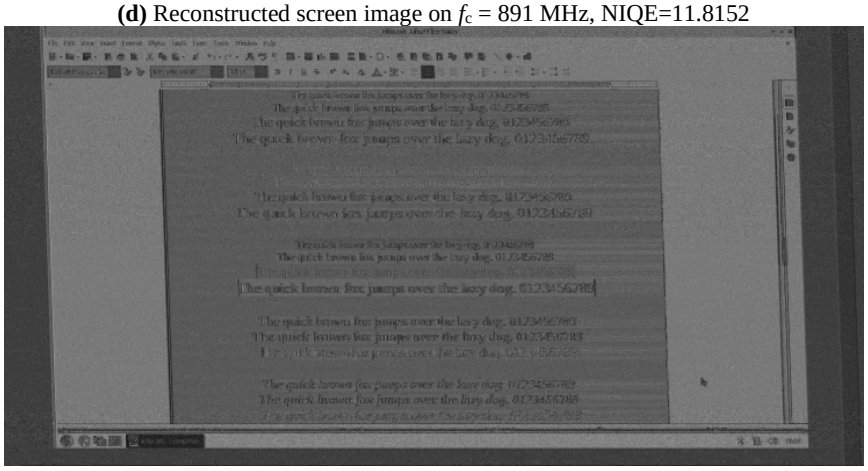
(b) Rreconstructed screen image on f_c = 594 MHz, NIQE=9.9528



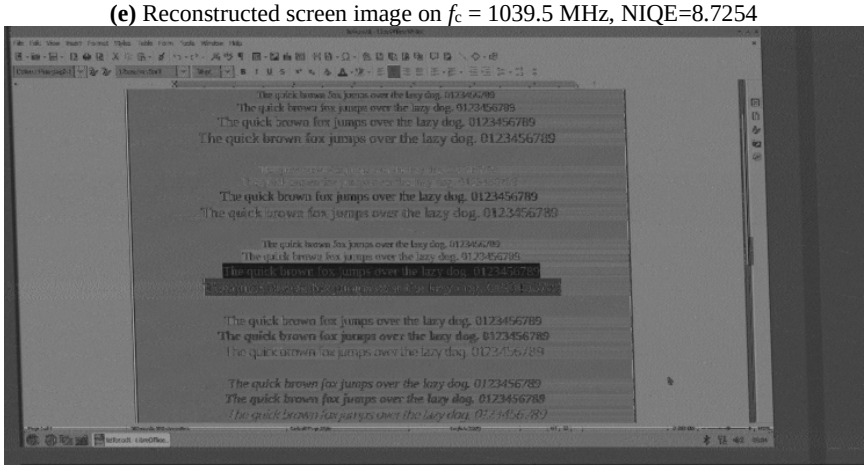
(c) Reconstructed screen image on f_c = 742.5 MHz, NIQE=10.9326



(d) Reconstructed screen image on f_c = 891 MHz, NIQE=11.8152



(e) Reconstructed screen image on f_c = 1039.5 MHz, NIQE=8.7254



(f) Reconstructed screen image on f_c = 1188 MHz, NIQE=9.5316

Fig. 3. Reconstructed screen images on different central frequencies.

on the computer monitor, with remark that the textural complexity of the displayed image can influence the quality. However, images that show text processing do not differ from each other to a great extent, so this single example illustrates the typical result.

By comparing the original image with the reconstructed ones, it can be observed that text typed in different colors affects the reconstruction of that part of the image differently. For instance, in Fig. 3(e) and 3(f), the text typed in blue and green, as well as the parts of the text highlighted with these colors, are clearly visible. However, text colored in yellow and red cannot be discerned in any of the analyzed spectral sub-bands. This phenomenon is explained by the fact that yellow, red, and white pixels have very similar values of average radiated power per pixel. It should be noted that in the mentioned text document, red was a pure color (with the maximum value in the red channel and minimal values in the others), while blue and green were not pure colors. Given that the yellow color is very similar to white and is problematic for text processing, from a security perspective, and based on the obtained results, the use of the red color for text characters is recommended.

In addition to using different colors for text characters, recommended TEMPEST countermeasures also include the use of various fonts for text characters, then shielding, zoning, filtering, and jamming [24][25][26][27].

The use of appropriate fonts for text characters can be a protective measure against unwanted information leakage. This countermeasure falls under the category of soft TEMPEST. Although characters can sometimes be difficult to discern due to the effective choice of font, such fonts are often not user-friendly as they obstruct work efficiency. However, soft TEMPEST measures are the most cost-effective solution [24].

Shielding is based on the enclosure of devices or rooms used for processing crucial information. This enclosure is performed using appropriate materials that will reduce unwanted emissions. However, shielding can be very costly and difficult to implement, especially when dealing with rooms or entire buildings. Therefore, shielding is most often performed in combination with zoning. Zoning defines the area around the devices and rooms where confidential data is processed, which needs to be physically secured, and beyond which it would be impossible to access the data being processed via compromising emanations. In this way, sufficient signal attenuation is achieved, making any potentially detected signals impossible to decode [26][27].

Radiation emission can also be reduced through filtering. However, the use of filters only affects a portion of the potential compromising emanations. Filters can be applied to communication interfaces or to power supply cables. Nevertheless, this method only covers the emanations originating from the interfaces and not the radiation emitted by the device's internal electronics themselves. Consequently, complete protection against potential information leakage is not achieved [25][27].

Jamming is a form of active protection against information leakage via unwanted radiation. It is crucial to ensure that the jamming signal's power is higher than that of the compromising emanation. However, it is equally important that the jammer does not in any way interfere with the normal operation of the device being protected or with other equipment in the environment. Jamming is most often implemented using

an additional device, which also makes it suitable for mobile applications and, in the absence of shielded devices, for cables and other potentially unprotected operational equipment that could lead to the leakage of significant information. One drawback of this method is the need to cover a broad part of the electromagnetic spectrum or, alternatively, to focus on the part of the spectrum assessed as being the most compromised. Another important consideration is the choice of the jamming signal, which must effectively disrupt eavesdropping attempts without interfering with the users and the functionality of their equipment [25][27].

5 Conclusion

The paper shows that using simple equipment, it is possible to detect and subsequently reconstruct signals obtained from compromising electromagnetic radiation. Image reconstruction of the monitor's display can be performed across several spectral sub-bands, but a clearer image is obtained at higher frequencies.

Due to the potential leakage of sensitive information, it is crucial to raise awareness about TEMPEST security and diligently apply protective measures. The paper shows that using the red color for characters during text document processing, makes it significantly more difficult to detect the actual text content compared to when black, green, or blue characters are used.

In further work, a more detailed analysis of pixel intensity on the reconstructed image is planned, depending on the signal sent to display the pixels on the monitor. Additionally, the creation of a database of reconstructed images with various screen resolutions and test images is planned, which would serve as a reference for future research on this topic.

Acknowledgments. This research has been a part of the project No. CPME/2/21-25 supported by the Ministry of Defence, Republic of Serbia.

Disclosure of Interests. The authors declare that they have no known competing financial or any other interests or personal relationships that have appeared to influence the work reported in this paper.

References

1. Jovanović, B., Tot I., Ilić, S.: Contemporary cryptography: Recent achievement and research perspectives. In: 11th International Scientific Conference on Defensive Technologies (OTEH), pp. 376-380, Tara, Serbia, October 09-11 (2024), doi: 10.5937/OTEH24067J
2. Antić, V., Protić, D., Stanković, M., Prodanović, R., Manić, M., Ostojić, G., Stankovski, S., Kučević, D.: Protecting data at risk of unintentional electromagnetic emanation: TEMPEST profiling. Applied Sciences, **14**, 4830 (2024), doi: 10.3390/app14114830
3. Hayashi, Y.: State-of-the-art research on electromagnetic information security. Radio Science, **51**(7), 1213-1219 (2016), doi: 10.1002/2016RS006034
4. Meulemeester, P. De., Scheers, B., Vandenbosch, G. A.: Reconstructing video images in color exploiting compromising video emanations. In: International Symposium on Elec-

tromagnetic Compatibility-EMC EUROPE, pp. 1-6, Rome, Italy, September 23-25 (2020), doi: 10.1109/EMCEUROPE48519.2020.9245775
5. Ulas, C., Sahin, S., Memisoglu, E., Asık, U., Karadeniz, C., Kılıc, B., Sarac, U.: Automatic tempest test and analysis system design. Internatinal Journal on Cryptography and Information Security (IJCIS), **4**(3), 1-12 (2014), doi: 10.5121/ijcis.2014.4301
6. Van Eck, W.: Electromagnetic radiation from video display units: An eavesdropping risk? Computers & Security, **4**(4), 269-286 (1985), doi: 10.1016/0167-4048(85)90046-X
7. Grdović, M., Protić, D., Antić, V., Jovanović, B.: Screen reading: electromagnetic information leakage from the computer monitor. Vojnotehnički glasnik/Military Technical Courier, **70**(4), 836-855 (2022), doi: 10.5937/vojtehg70-38930
8. Vizitiu, A. M., Sandu, M. A., Dobrescu, L., Focsa, A., Molder, C. C.,: Comparative approach to de-noising TEMPEST video frames. Sensors, **24**, 6292 (2024), doi: 10.3390/s24196292
9. Fernández, S., Martínez, E., Varela, J., Musé, P., Larroca, F.: Deep-TEMPEST: Using deep learning to eavesdrop on HDMI from its unintended electromagnetic emanations. In: 13th Latin-American Symposium on Dependable and Secure Computing, pp. 91-100, Recife, Brazil, November 26-29 (2024), doi: 10.1145/3697090.3697094
10. Jovanović, S., Protić, D., Antić, V., Grdović, M., Bajić, D.: Security of wireless keyboards: Threats, vulnerabilities and countermeasures. Vojnotehnički glasnik/Military Technical Courier, **71**(2), 296-315 (2023), doi: 10.5937/vojtehg71-43239
11. Peng, Y., Zhang, J., Mao, J., Cui, M.: A signal-denoising method for electromagnetic leakage from USB keyboards. Electronics, **12**, 3647 (2023), doi: 10.3390/electronics12173647
12. Trip, B., Butnariu, V., Vizitiu, M., Boitan, A., Halunga, S.: Analysis of compromising video disturbances through power line. Sensors, **22**(1), 267 (2021), doi: 10.3390/s22010267
13. Kubiak, I., Przybysz, A., Musial, S.: Possibilities of electromagnetic penetration of displays of multifunction devices. Computers, **9**(3), 62, 2020, doi: 10.3390/computers9030062
14. Long, Y., Jiang, Q., Yan, C., Alam, T., Ji, X., Xu, W., Fu, K.: EM eye: Characterizing electromagnetic side-channel eavesdropping on embedded cameras. In: ACM the Network and Distributed System Security (NDSS), San Diego, CA, USA, February 26-March 01 (2024), doi: 10.14722/ndss.2024.24552
15. Boitan, A., Halunga, S., Bindar, V., Fratu, O.: Compromising electromagnetic emanations of usb mass storage devices. Wireless Personal Communications, **126**(1), 97-122 (2022), doi: 10.1007/s11277-020-07329-8
16. Boitan, A., Kubiak, I., Halunga, S., Prybysz, A., Stańczak, A.: Method of colors and secure fonts used for source shaping of valuable emissions from projector in electromagnetic eavesdropping process. Symmetry, **12**, 1908 (2020), doi: 10.3390/sym12111908
17. Kubiak, I.: Laser printer as a source of sensitive emissions. Turkish Journal of Electrical Engineering and Computer Sciences, **26**(3), 1354-1366 (2018), doi: 10.3906/elk-1704-9
18. Đaković, B., Stojanović, N., Grdović, M., Vujatović, B.: Analysis of restoration of images captured by detecting unintentional computer monitor emanation using simple tools. (In Serbian), In: LXIX Conference on Electrical, Electronic and Computing Engineering, ETRAN, pp. 108-113, Čačak, Serbia, June 9-12 (2025), doi: 10.69994/69E25020
19. Sun, X., Zheng, Y., Xi, W., Chen, Z., Chen, Z., Hao, H., Jiang, Z., Zhong, S.: TEMPEST-LoRa: Cross-technology covert communication. arXiv preprint arXiv:2506.21069, June (2025), doi: 10.48550/arXiv.2506.21069
20. Choi, D. H., Lee, E., Yook, J. G.: Reconstruction of video information through leaked electromagnetic waves from two VDUs using a narrow band-pass filter. IEEE Access, **10**, 40307-40315 (2022), doi: 10.1109/ACCESS.2022.3162686

21. Liu, T., Li, Y.: Electromagnetic information leakage and countermeasure technique. Translated by Liu Jinming, Liu Ying, Zhang Zidong, Liu Tao. Springer (2019), doi: 10.1007/978-981-10-4352-9
22. Durakovskiy, A. P., Kessarinskiy, L. N., Simakhin, E. A.: Detection of compromising radiation from modern data transfer interfaces using the example of high definition multimedia interface. In: IOP Conference Series: Materials Science and Engineering, **1069**(1), 012026 (2021), doi: 10.1088/1757-899X/1069/1/012026
23. Mittal, A., Soundararajan, R. Bovik, A. C.: Making a "completely blind" image quality analyzer. IEEE Signal Processing Letters, **20**(3), 209-212 (2013), doi: 10.1109/LSP.2012.2227726
24. Kubiak, I., Boitan, A. Halunga, S.: Assessing the security of TEMPEST fonts against electromagnetic eavesdropping by using different specialized receivers. Applied Sciences, **10**(8), 2828 (2020), doi: 10.3390/app10082828
25. Suzuki, Y., Masugi, M., Tajima, K., Yamane, H.: Countermeasures to prevent eavesdropping on unintentional emanations from personal computers. NTT Technical Review, **6**(10), 6-12 (2008), doi: 10.53829/ntr200810sf2
26. Martin, M., Sunmola, F., Lauder, D.: Unintentional compromising electromagnetic emanations from IT equipment: A concept map of domain knowledge. Procedia Computer Science, **200**, 1432-1441 (2022), doi: 10.1016/j.procs.2022.01.344
27. ITU Recommendation ITU-T K.115, Mitigation methods against electromagnetic sequrity threats, Series K: Protection against interference, ITU-T Telecommunication Standardization Sector of ITU: Geneva, Switzerland (2015).