Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 4268 – 4279
© TÜBİTAK
doi:10.3906/elk-1701-128

LED printers and safe fonts as effective protection against the formation of unwanted emission

Ireneusz KUBIAK*
Military Communication Institute, Zegrze, Poland

Received: 13.01.2017 • **Accepted/Published Online:** 18.05.2017 • **Final Version:** 05.10.2017

Abstract: Due to the widespread use of computer equipment, electromagnetic protection of processed data is still an issue. Structurally modified commercial equipment is used to protect devices against this phenomenon. The acquisition costs of such modified devices are enormous. However, the market offers information devices with very low susceptibility to electromagnetic infiltration. Safe fonts are a new solution in the protection of sensitive information against electromagnetic infiltration processes. The use of safe fonts not only increases resistance to electromagnetic eavesdropping but also makes it impossible. These devices are computer printers that use a slat with hundreds of LEDs arranged in several rows during the process of photoconductor exposure. The solution in the form of safe fonts is a universal method that protects process information against electromagnetic penetration. Safe fonts are effective not only for printers with slat LED. The solution can also be used for the protection of analog standard VGA, digital standard DVI, and printers with one diode and two diode laser systems.

Key words: Slat light-emitting diode, printer, unwanted emission, electromagnetic infiltration

1. Introduction

Computer printers of various types are an essential part of computer sets and take part in almost every step of information processing. Many believe that the first reading of created documents must be based on their paper versions. Therefore, most often, every document, even an electronically distributed one, is printed. However, is this element of the entire process of information processing safe [1]?

We often try to adequately protect files stored on a drive by protecting them against the possibility of opening. If there is no such need, we do not connect the computer to the Internet network [2]. State and private institutions pay increasing attention to the need for special computing solutions for the processing of especially important information [3]. We begin to realize, due to the appearance of so much information, the dangers related to revealing emission and the possibility of using it in noninvasive information acquiring [4,5]. This particularly refers to sources of video signals in the form of computer graphic tracks such as the graphic card, video cable [6], and monitor [7,8]. It is extremely disturbing that information can be so easily recreated and presented in a form that is understandable to humans. Earlier emerging information about the electromagnetic protection of LCD monitors or the DVI standard proved to be untrue [8,9].

Another no less dangerous source of electromagnetic emission, formidable from the point of view of the possibility of conducting electromagnetic “watch”, is the computer printer [10–12]. It should be noted that studies on various technical and software solutions that would allow for adequate protection of processed

*Correspondence: i.kubiak@wil.waw.pl

information without undue financial outlays have still not been carried out. It should also be noted that the cost of acquiring a single computer set, referred to as belonging to the TEMPEST class, is an expense of several thousands of dollars. This is why "software solutions", based on the use of "safe fonts", are mentioned more and more often. As shown by the results of conducted studies, classified information processed with their use becomes safe for sources in both the form of video track standard VGA and DVI and the video track of laser printers (Figure 1).

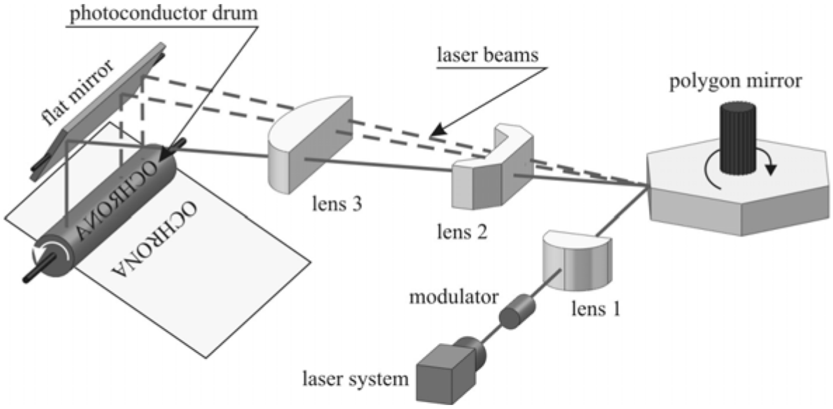


Figure 1. Photoconductor exposure in laser printers in a one diode laser system.

Nevertheless, the simultaneous use of additional solutions, enhancing the protection of electromagnetically processed information without incurring additional costs, is not redundant. This only increases the reliability of the system in protecting our information. The said solution is realized by commercial computer printers, commonly available on the market, with photoconductor exposure technology based on a slat of LEDs (Figure 2) controlled by a parallel-serial signal [13].

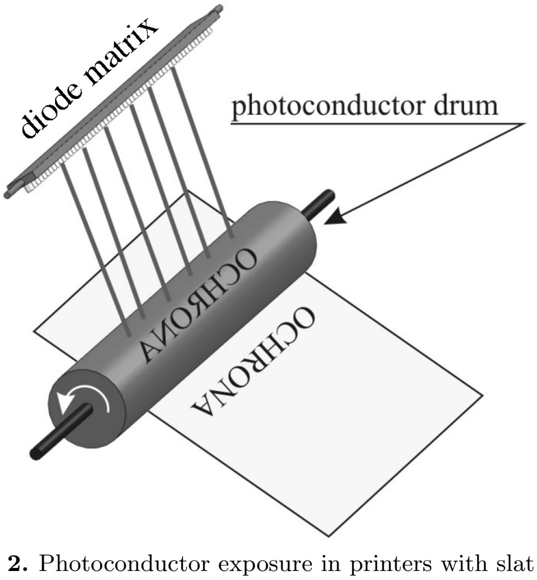


Figure 2. Photoconductor exposure in printers with slat LEDs.

Due to such a solution, the registered revealing emission signal does not have as clearly distinctive features as a signal that comes from a single laser diode controlled by serial signal or the VGA or DVI video standard [14].

2. Sources of revealing emission of computer printers

The most commonly used office printers are laser printers. We can distinguish two basic types of such printers, classified according to the photoconductor exposure technology used. The first type is a printer based on the use of a dual laser diode that is controlled by a serial signal (Figure 3). Here, the source of revealing emission is simple and may be easily subject to electromagnetic infiltration. In such a case, a single line of text is exposed point by point until its end is reached. The process is then repeated for subsequent lines [15].

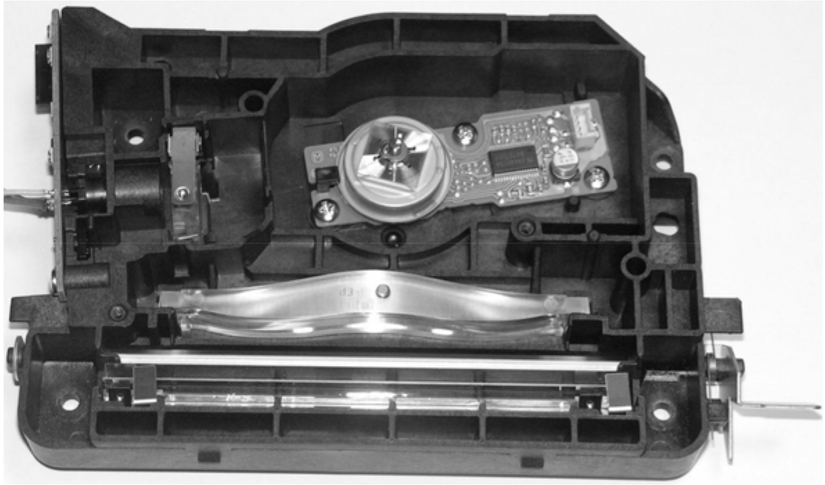


Figure 3. Example of a photoconductor exposure system used in standard laser printers (HP LaserJet P2035).

The other type of printer is based on a solution using a slat of LEDs (Figure 4), which is controlled via a parallel-serial signal (partial analogy to line printers). The LEDs are arranged in a few lines with several hundreds of diodes per line. As it may be seen, the source of emission is more complex; therefore, the recreation of information requires more attention.

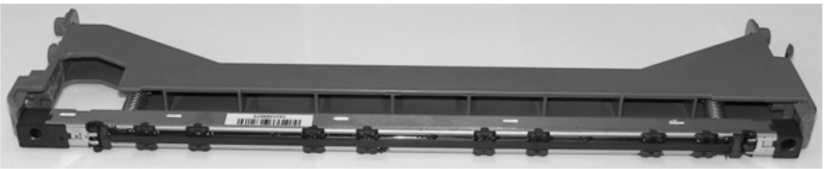


Figure 4. Example of photoconductor exposure system in the form of slat LEDs (OKI B401a).

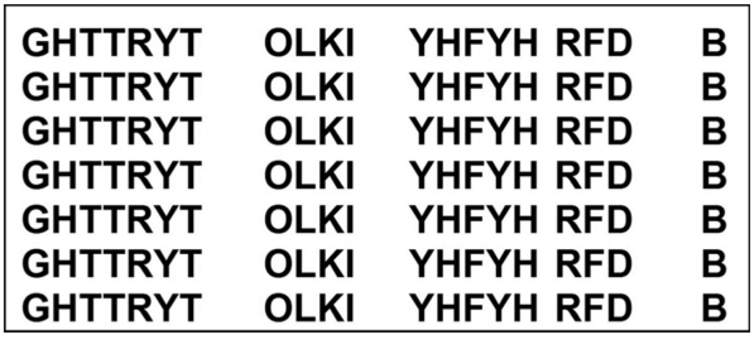
The slat is controlled in a parallel manner; however, the signal supplied to the array is a serial signal. This means that from the point of view of electromagnetic infiltration such a solution may be safer than the conventional single or dual laser diode exposure systems. Moreover, it results in a lower failure frequency from the device and, due to the smaller number of mechanical components, it is more compact.

Additional use of safe fonts (symmetrical safe, asymmetrical safe, or simple safe [16,17]) in text information processing, with an electric form devoid of distinctive features as compared to typical computer fonts, reduces the degree of susceptibility to electromagnetic eavesdropping of printers.

3. Results of revealing emission testing

3.1. Testing conditions

Due to the photoconductor exposure technology used, tests for the viability of electromagnetic eavesdropping were conducted on two types of printers: a dual laser diode and a slat (array) of LEDs. The printed document contained a text written in the Arial font (Figure 5). In order to establish the suitability of safe fonts in the protection of processed electromagnetic information, research was also conducted for a text written in the symmetrical safe, asymmetrical safe, and simple safe fonts, which are similar to the Arial font.



GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B
GHTTRYT OLKI YHFYH RFD B

Figure 5. Fragment of a text printed during the testing of electromagnetic infiltration susceptibility of computer printers.

The measurement of revealing emission, in the system shown in Figure 6, was made over a distance of 1 m from the source, in accordance with MIL-STD-461F “Requirements for the control of electromagnetic interference. Characteristics of subsystems and equipment”, in an anechoic chamber. In this way, the source of emission was separated from additional unwanted sources of electromagnetic disturbances [18]. The computer used was in the TEMPEST class. The controlled measuring bands were 5 MHz, 10 MHz, 20 MHz, and 50 MHz, and the signal sampling frequencies were 15 Ms/s, 62.5 MHz, and 125 Ms/s. This allowed for the observation of the impact of technological solutions of the printers and the fonts used in the form of recreated images. At the same time, it also allowed for classification of the suitability of design and software solutions in the electromagnetic protection of printing devices.

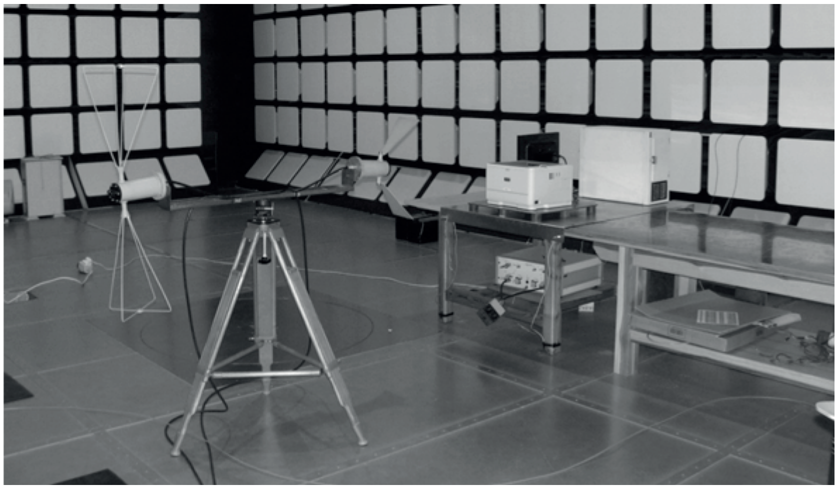


Figure 6. Actual measuring system in an anechoic chamber.

Moreover, a series of tests related to printout quality was conducted for the printer with an LED array. The tested printer produced a printout of the following quality:

- ProQ 1200 dpi ×120 dpi
- High quality 1200 dpi × 600 dpi
- Normal 600 dpi × 600 dpi
- Draft 300 dpi × 300 dpi

Each of the options may be additionally supported by the possibility to select a toner save option.

According to the data obtained from the manufacturer, the printing quality, e.g., 300 dpi × 300 dpi, means that there are 300 LEDs for each 2.54 cm of a line's length. For text with a width of 160 mm (between 210 mm (the width of the A4 paper format) and 50 mm (total left and right margin)), this results in about 1890 diodes. However, for a quality of 1200 dpi × 1200 dpi, the number of diodes is 7560. Therefore, does printing quality impact the change of electromagnetic infiltration capability? Does it directly translate into the quality of recreated images? The obtained data are presented later in the article.

3.2. Results of analyses

In typical laser printers (single laser diode), the laser is controlled by a serial signal. An important element, in terms of commercial device susceptibility to infiltration, is the form of the signal that controls the operation of the laser. The printout (photoconductor exposure) of a single horizontal line is related to the control signal with a pulse structure. The number of pulses is related to the number of exposed points, which also depends on printing resolution. In this case, we are not dealing with a single pulse of duration corresponding to the length of the exposed line (analogous to the analogue video standard VGA [19]). As a result of photoconductor exposure, graphic elements included in the recreated images are filled with contours in a color that is different from the background (Figure 7).

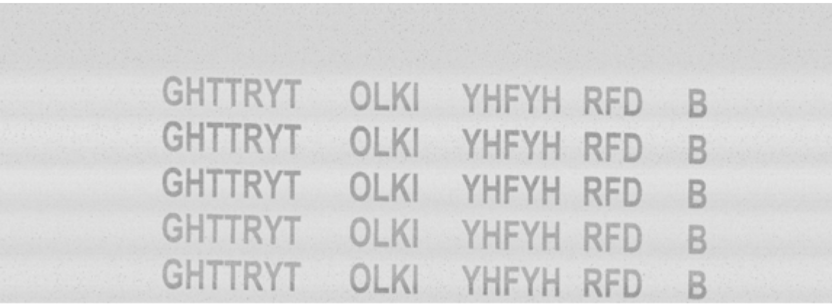


Figure 7. Fragment of a recreated image for revealing emission source in the form of a typical laser printer (image inversion, original character size of 26 points); reception frequency f_o = 145 MHz, BW = 10 MHz; sampling frequency f_s = 62.5 Ms/s.

This impacts the high level of the efficiency of electromagnetic infiltration and can be compared to the situation that occurs when trying to eavesdrop on electromagnetic digital standard DVI (Figure 8) [1]. The essence of this research, however, is studying the possibility of infiltration of computer printers, based on the solution of exposing a photoconductor to a slat of LEDs. Due to the form of the recreated images, the tested printer has four lines of LEDs. It is demonstrated by the fact that the obtained images contain four identical horizontal sets of graphic characters of the printed document, a fragment of which is shown in Figure 5. In addition, the structure of the graphic characters contained in the recreated images is very different than in the case of a typical laser printer.

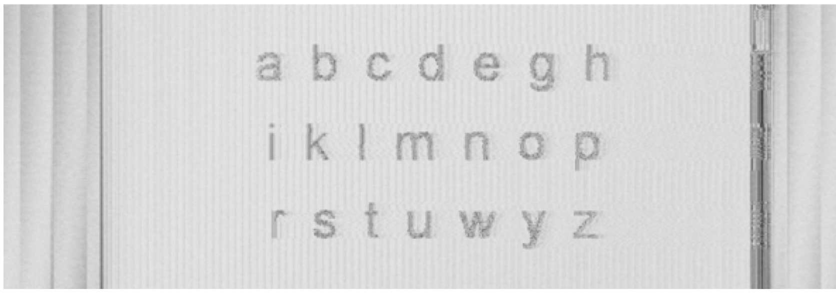


Figure 8. Fragment of a recreated image for revealing emission source in the form of digital video standard DVI (image inversion, original character size of 36 points); reception frequency $f_o = 365$ MHz; BW = 50 MHz; sampling frequency $f_s = 125$ Ms/s.

The dissimilarity prevents data reading. This is caused by the LED slat operating method, which is not controlled by a typical series signal. This detailed solution is not made available by the manufacturer. One should suppose, however, that it is a parallel-serial signal, and the nature of the waveform is similar to the analog video standard VGA. Consequently, a horizontal line of a predetermined length is exposed to a continuous signal (stimulation of the corresponding number of LEDs in the slat) with constant voltage, unlike a typical laser printer. The recreated image shows only the vertical and diagonal edges of the contained graphic signs (Figure 9).

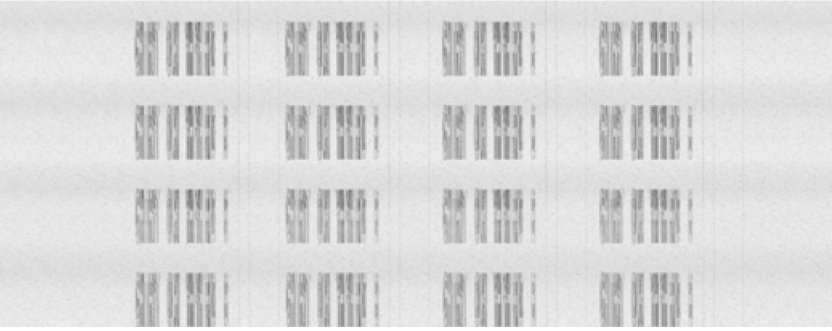


Figure 9. Fragment of a recreated image for revealing emission source in the form of a laser printer with an LED slat (image inversion, original character size of 26 points, capital letters); reception frequency $f_o = 145$ MHz, BW = 20 MHz; sampling frequency $f_s = 250$ Ms/s.

The appropriate recalibration of a fragment of an image (Figure 9) allows us to obtain more legible characters (Figure 10). It should be emphasized, however, that the size of the printed characters was 26 points. When printing the characters at a size of 14 points, similar to the commonly used 12 points, the obtained degree of readability is not as high (Figure 11). The strings merge and form unreadable clusters of pixels of a different color, which cannot be directly identified with the printed characters.

Many earlier publications discussed issues related to safe fonts as software support for the protection of information against electromagnetic penetration. Their usefulness has been demonstrated in a wide range of applications, ranging from sources in the form of graphic tracks of the analog standard VGA to the digital DVI standard, and ending with sources in the form of conventional laser printers (one- and two-diode). Safe

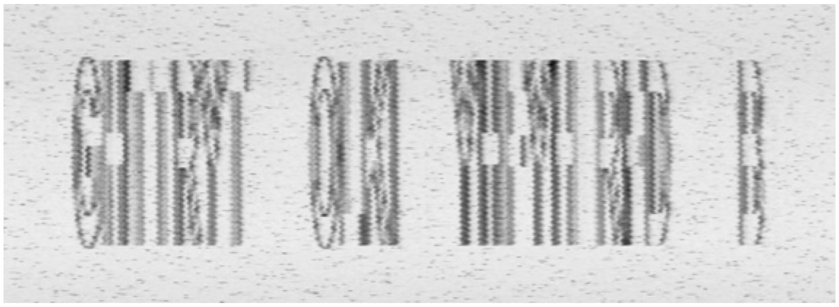


Figure 10. Calibrated fragment of the image presented in Figure 9.

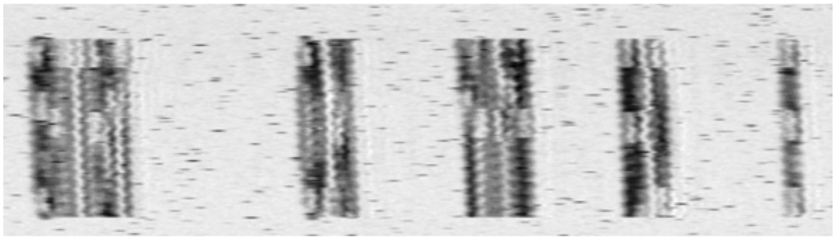


Figure 11. Calibrated fragment of an image containing strings corresponding to the original size of 14 points (capital letters, image inversion); reception frequency f_o = 145 MHz, BW = 10 MHz; sampling frequency f_s = 125 Ms/s

fonts have also become resistant to the operation of optical character recognition software, without taking the learning stage into consideration.

When analyzing the commercial solution of photoconductor exposure technology, based on a slat of LEDs, appropriate tests were also conducted for printing safe font characters. The strings were similar to the characters presented in Figure 3. Due to the structure of safe font characters that have been designed with the consideration of differential characteristics of the information penetration channel and drum exposure technology, revealing emission signals are devoid of distinctive features that could help decide about correlating them with the original information. Therefore, graphic elements that would indicate the occurrence of a given character (Figures 12–14) cannot be identified in the obtained images.

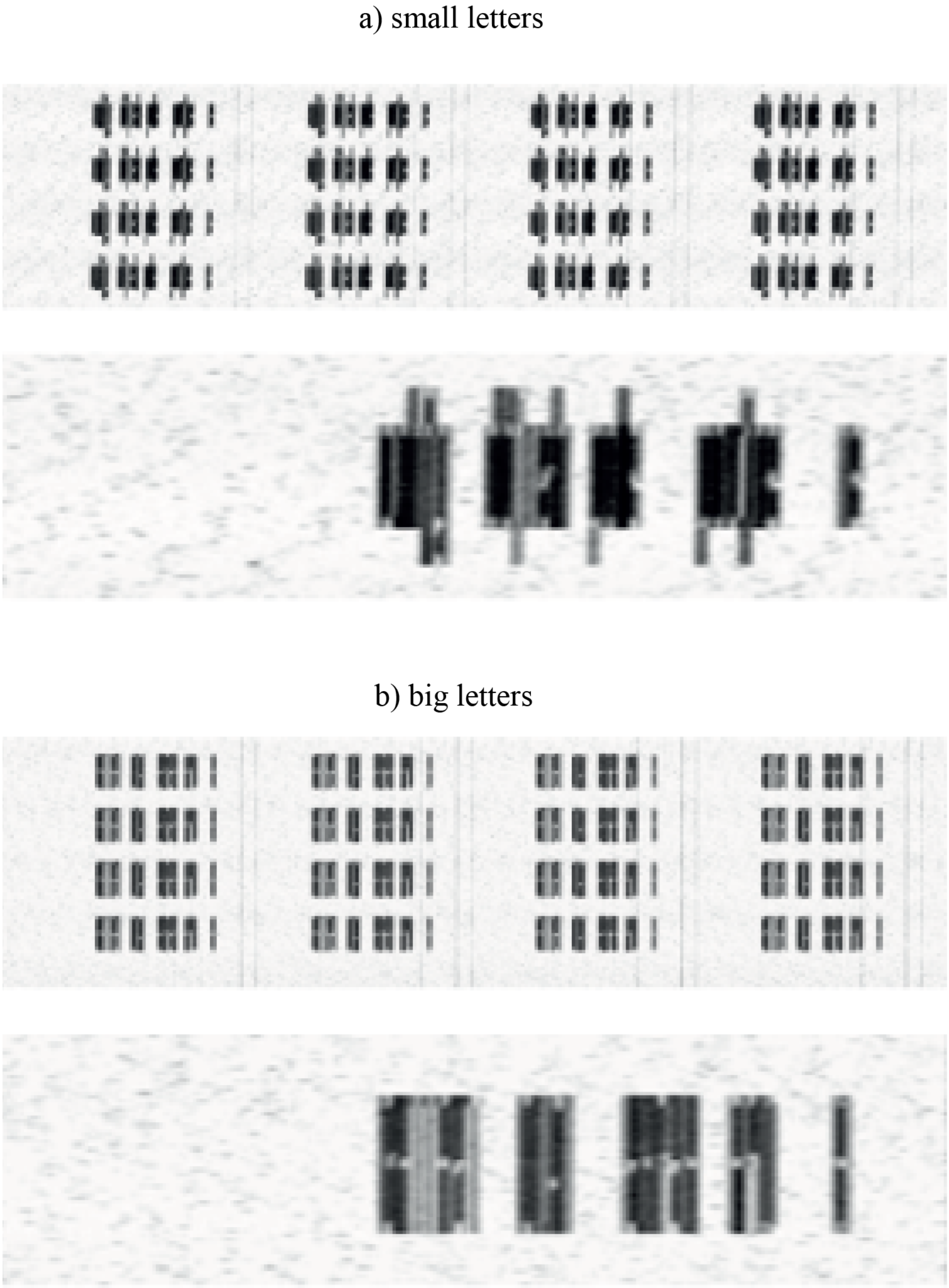
It should be noticed that the property already occurs in the case when the signal–noise relation is determined by the following relation:

$$SNR = 10\log_{10}\frac{P_s}{P_{sz}}, \tag{1}$$

where P_S is the signal power and P_{sz} is the noise power, reaching values much higher than 0. This means that the only information that is carried by the revealing emission is the fact that the printing device is in operation. For printers based on a single laser diode and the use of safe fonts, the lack of effectiveness of the electromagnetic infiltration process may be referred to when the SNR value is less than 0 [20,21].

4. Conclusion

As shown by many events everywhere in the world, the protection of information is currently a huge challenge. This is especially true in cases where there is a possibility of noninvasive, i.e. unnoticed by the owner of the protected data, acquisition of information. This is possible due to the occurrence of electromagnetic emissions having characteristics of electronically processed information [22].



a) small letters

b) big letters

Figure 12. Fragment of a recreated image and its enlarged part for revealing emission source in the form of a laser printer with an LED slat for the printout of “symmetrical safe” font letters (image inversion, original character size of 26 points); reception frequency f_o = 145 MHz, BW = 5 MHz; sampling frequency f_s = 62.5 Ms/s: a) small letters, b) big letters.

The costs of limiting the possibilities of the occurrence of revealing emission are extremely high. They arise from the need to introduce structural changes to commercial devices, which are the basis for the special solutions commonly known as TEMPEST solutions. Therefore, researchers are seeking new solutions that will reduce the cost of information protection without reducing its capability level. Thus, all new technological

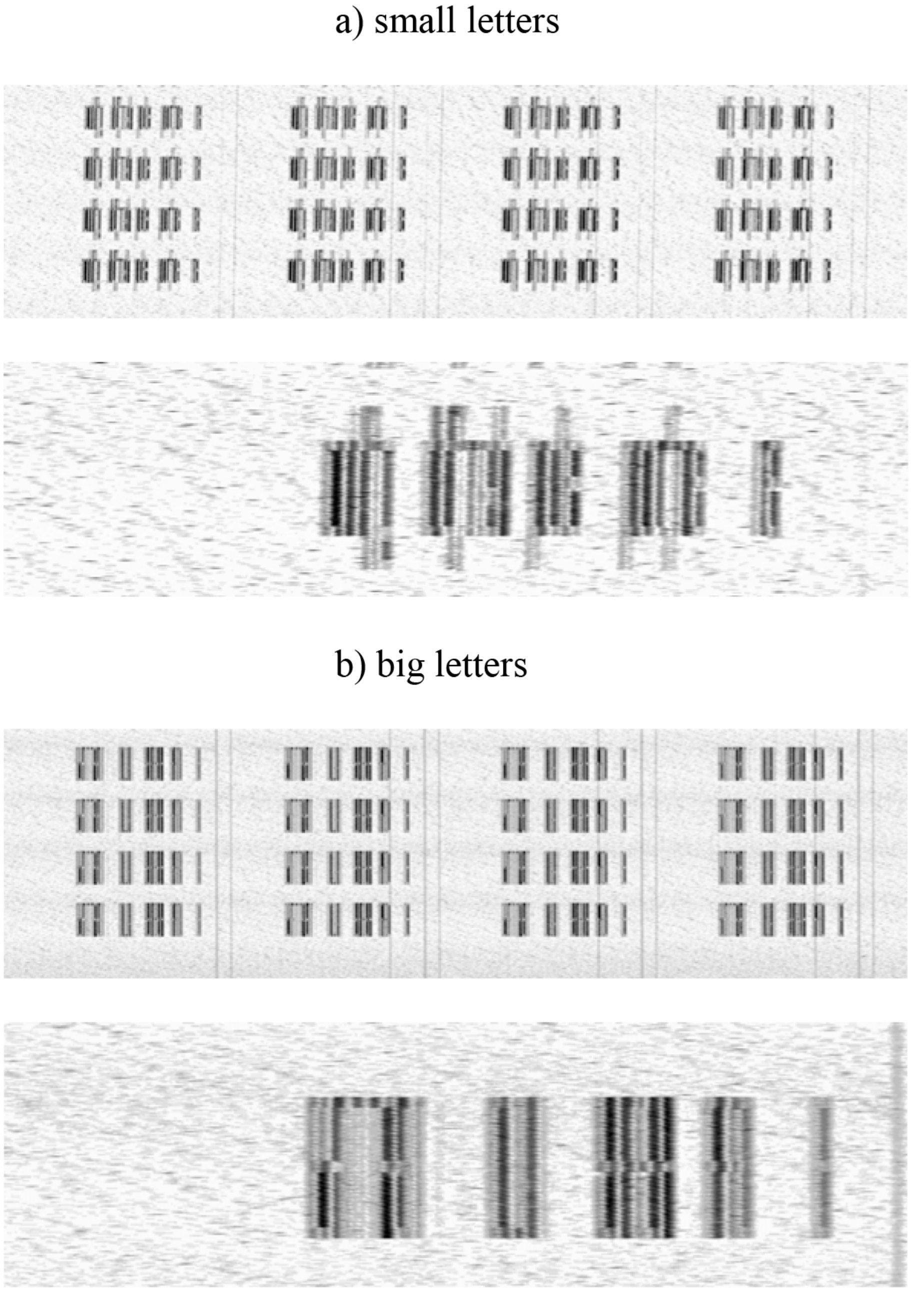


Figure 13. Fragment of a recreated image and its enlarged part for revealing emission source in the form of a laser printer with an LED slat for the printout of "asymmetrical safe" font letters (image inversion, original character size of 26 points); reception frequency f_o = 145 MHz; BW = 5 MHz, sampling frequency f_s = 62.5 Ms/s: a) small letters, b) big letters.

devices appearing on the commercial market are now being analyzed. Some of them may prove useful throughout the cycle of projects determining the level of protected information.

This article presents the results of research on revealing emission, analyses of images recreated based on the emission, and the probability of electromagnetic eavesdropping of computer printers. The study involved two

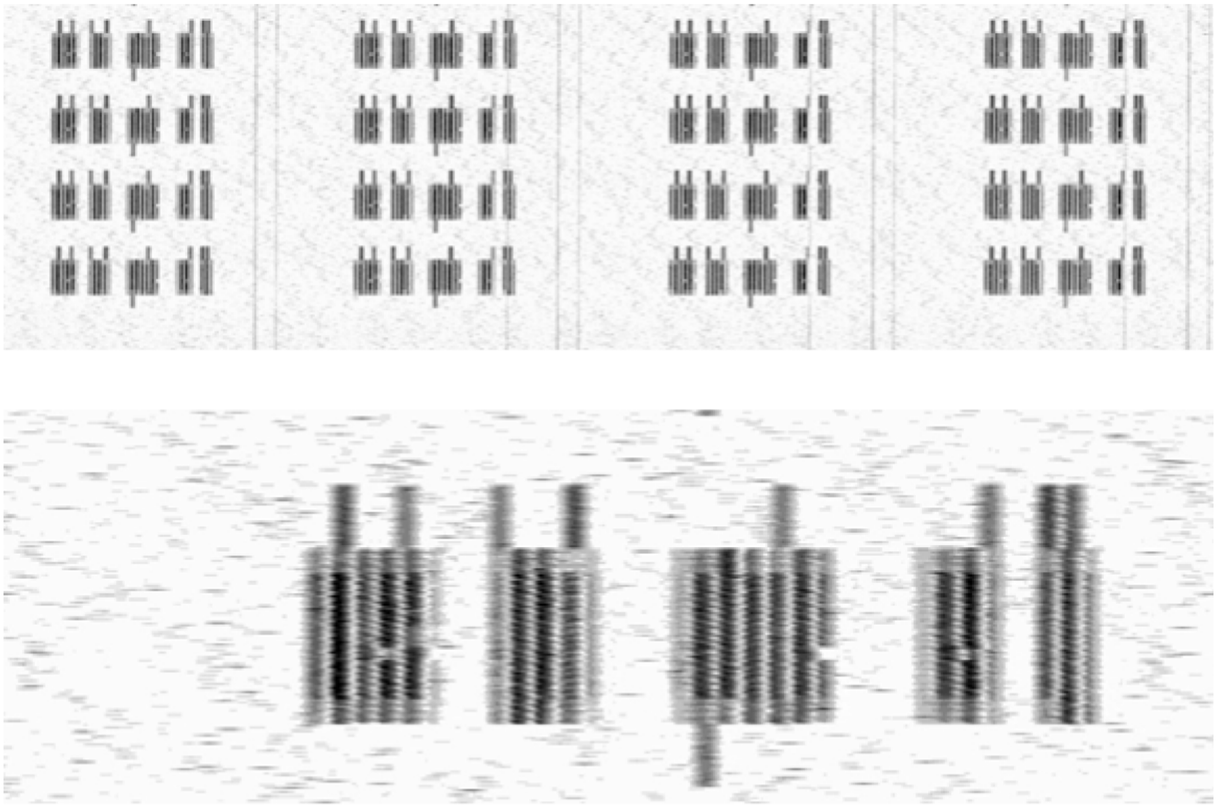


Figure 14. Fragment of a recreated image and its enlarged part for revealing emission source in the form of a laser printer with an LED slat for the printout of “simple safe” font letters (image inversion, original character size of 26 points); reception frequency $f_o = 145$ MHz; BW = 5 MHz, sampling frequency $f_s = 62.5$ Ms/s.

types of printers: a printer using single diode laser technology for photoconductor exposing and a printer based on LED slat technology. The text printed during the research and registration of unwanted signals contained characters written in the commercial font Arial. Safe fonts (symmetrical safe, asymmetrical safe, and simple safe) were also tested.

The research results show that photoconductor exposure technology, based on a slat of LEDs, is a solution worthy of attention in terms of its capability to reduce the distinctive features of revealing emissions. Solutions using slat LED technology and safe fonts provide a high level of protection against noninvasive data acquisition. The use of only printers with LED slats makes the readability of data written with traditional fonts, as compared to typical printers (single laser diode), much more difficult (Table).

Table. Comparison of susceptibility to infiltration of computer printers, depending on the font used in the processed text document.

Font type	Printer using a one diode laser system	Printer based on slat LED technology
Arial	Susceptible	Little resistance
Symmetrical safe	Resistant	Resistant
Asymmetrical safe	Resistant	Resistant
Simple safe	Resistant	Resistant

The additional use of safe fonts prevents any perception (extracting elements from the background) of text data. Printers with a single laser diode, for traditional fonts, are not a solution that can be considered completely safe in terms of electromagnetism.

References

[1] Choudary O, Kuhn MG. Template attacks on different devices. In: International Conference on Constructive Side-Channel Analysis and Secure Design; 2014. pp. 179-198.

[2] Kubiak I, Przybysz A. Electromagnetic protection of information and communication technology systems and networks. Telecommunication Review and Telecommunication News 2006; 12: 371-374 (article in Polish with an abstract in English).

[3] Ketenci S, Kayikçioğlu T, Gangal A. Recognition of sign language numbers via electromyography signals. In: Signal Processing and Communications Applications Conference; 16–19 May 2015; Malatya, Turkey. pp. 2593-2596.

[4] Kuhn MG. Compromising Emanations: Eavesdropping Risks of Computer Displays. Technical Report. Cambridge, UK: University of Cambridge Computer Laboratory, 2003.

[5] Kuhn MG. Optical time-domain eavesdropping risks of CRT displays. In: Proceedings of the 2002 IEEE Symposium on Security and Privacy; 12–15 May 2002; Berkeley, California, USA. pp. 3-18.

[6] Kubiak I. Video signal level (colour intensity) and effectiveness of electromagnetic infiltration. Bulletin of the Polish Academy of Sciences - Technical Sciences 2016; 64: 207-218.

[7] Kubiak I. The unwanted emission signals in the context of the reconstruct possibility of data graphics. International Journal of Image, Graphics and Signal Processing 2014; 11: 1-9.

[8] Kuhn MG. Electromagnetic eavesdropping risks of flat-panel displays. In: Proceedings of the 4th Workshop on Privacy Enhancing Technologies; 26–28 May 2004; Toronto, Canada. pp. 88-105.

[9] Przybysz A. Emission security of DVI and HDMI interface. Telecommunication Review and Telecommunication News 2014; 7: 669-673 (article in Polish with an abstract in English).

[10] Grzesiak K, Przybysz A. Software raster generator. Telecommunication Review and Telecommunication News 2011; 11: 1596-1600 (article in Polish with an abstract in English).

[11] Cihan U, Aşık U, Cantürk K. Analysis of information leakages on laser printers in the media of electromagnetic radiation and line conductions. In: International Conference on Information Security and Cryptology; 30–31 October 2015; Ankara, Turkey. pp. 8-14.

[12] Cihan U, Aşık U, Cantürk K. Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines. Comput Secur 2016; 58: 250-267.

[13] Kubiak I, Przybysz A. The impact of commercial equipment design to electromagnetic protection of data process. Prz Elektrotechniczn 2015; 11: 41-44 (article in Polish with an abstract in English).

[14] Kubiak I. Digital (DVI) and analog (VGA) graphic standard in electromagnetic protection of text information. Telecommunication review and Telecommunication News 2014; 6: 413-416 (article in Polish with an abstract in English).

[15] Grzesiak K, Przybysz A. Emission security of laser printers. In: Military Communications and Information Systems Conference; 27–28 September 2010; Wroclaw, Poland. pp. 353-363.

[16] Kubiak I. Computer font resistant to electromagnetic infiltration process. Prz Elektrotechniczn 2014; 6: 207-215 (article in Polish with an abstract in English).

[17] Kubiak I. Null Pointer computer font–electromagnetic safe or not? Telecommunication Review and Telecommunication News 2015; 1: 11-18 (article in Polish with an abstract in English).

[18] Cihan U, Aşık U, Cantürk K, Sarhat S, Bilal K, Ugur S. Automatic tempest test and analysis system design. International Journal on Cryptography and Information Security 2014; 4: 1-12.

[19] Kubiak I, Musial S. Hardware Raster Generator as a tool that supports electromagnetic infiltration. Telecommunication Review and Telecommunication News 2011; 11: 1601-1607 (article in Polish with an abstract in English).

[20] Ketenci S, Gangal A. Automatic reduction of periodic noise in images using adaptive Gaussian star filter. Turk J Electr Eng Co 2017; 25: 2336-2348.

[21] Song TL, Jeong YR, Yook JG. Modeling of leaked digital video signal and information recovery rate as a function of SNR. IEEE T Electromagn C 2015; 57: 164-172.

[22] Loughry J, Umphress DA. Information leakage from optical emanations. ACM T Inform Syst Se 2002; 5: 262-289.