We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Electromagnetic Eavesdropping

Ireneusz Kubiak

Abstract

Protection of information against electromagnetic penetration is a huge challenge. Especially this issue applies to computer station that processes protected information and that is a source of electromagnetic disturbances. These disturbances could be correlated with processed graphic information. Therefore, very often, they are called valuable or unintentional emissions. To protect the information, different methods of engineering of electromagnetic compatibility are used, e.g. electromagnetic gaskets, signal and power filters and electromagnetic shielding. The use of these methods causes a special device to become very heavy, and the looks of such device aren't nice. A new universal solution based on safe fonts is proposed. Safe fonts protect processed information against electromagnetic penetration in each case of graphic source of valuable emissions. These fonts protect not only Video Graphics Array (VGA) but also Digital Video Interface (DVI) standards. These fonts are also useful from electromagnetic protection's point of view in the case of the use of laser printers. All analyses are based on images reconstructed from valuable emissions. These emissions are measured in a range of frequencies from 100 MHz to 1.5 GHz. Safe fonts are simple solution that counteract electromagnetic eavesdropping process. They can replace expensive solutions based on shielding, zoning and filtering.

Keywords: electromagnetic eavesdropping, leakage information, protection of information, valuable (sensitive) emission, electromagnetic infiltration process, image and signal processing, data acquisition, identification, recognition

1. Introduction

Protection of information against electromagnetic eavesdropping in modern electronic systems is a big challenge. Such kind of eavesdropping is connected with electromagnetic emissions which are correlated with processed information [1–3]. This problem increases with a higher and higher use of electronic devices for processing and transmitting information. It results from the fact that each electronic device is the source of electromagnetic disturbances in particular unintentional emission of electromagnetic energy transited in surrounding space. Very often signals of unintentional emission could be correlated with processed information. The electromagnetic emissions with distinctive features can arise at any stage of processing of information (e.g. transmission, displaying on screen, printing) which occur in the electric form [1, 4–8]. Video signals are particularly dangerous (**Figure 1**) [9, 10].

Video graphics array (VGA) and digital video interface (DVI) [11, 12] are video standards currently used among other things in nonpublic information systems (other elements—keyboard, screen and main unit—of computer station could be also sources of sensitive emissions [13, 14]). But the graphic lines (VGA, DVI and laser printers) are most susceptible to electromagnetic eavesdropping. These
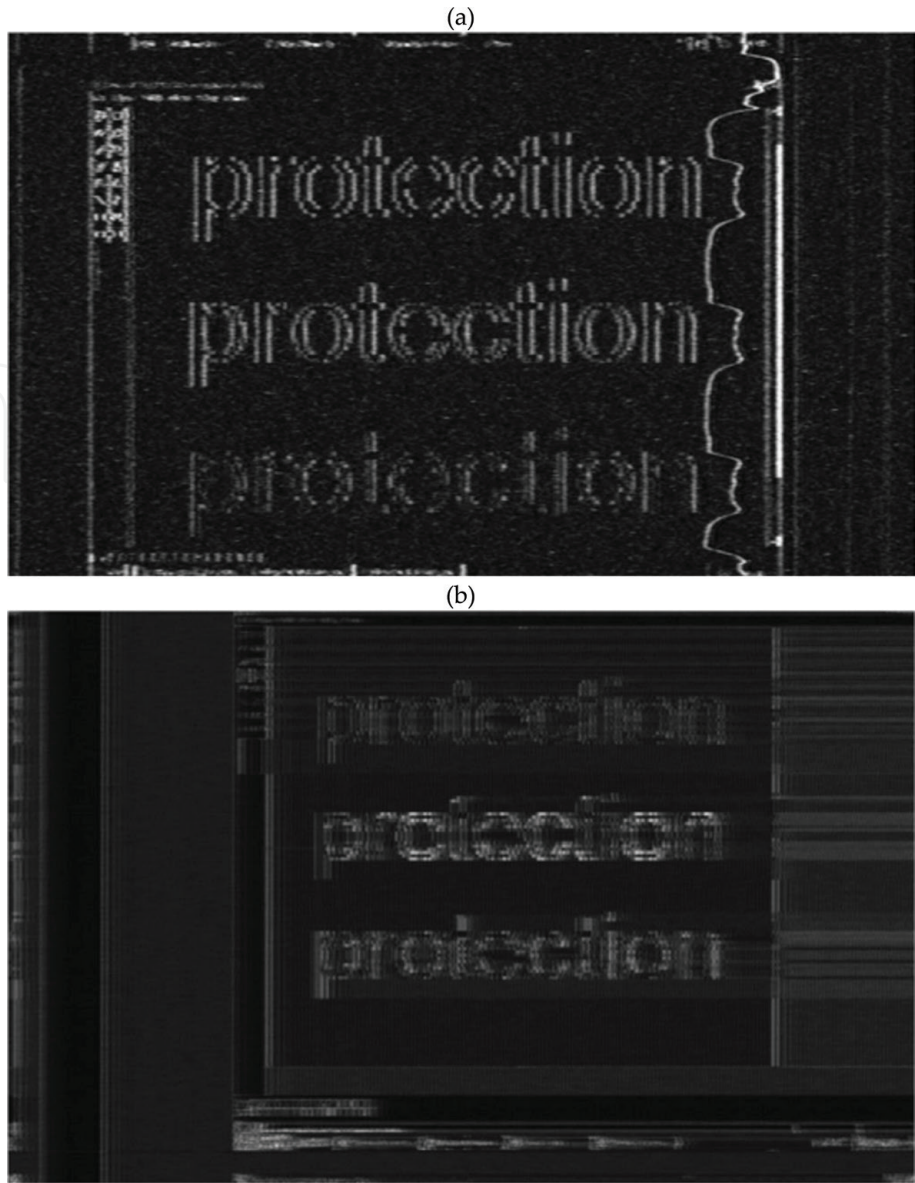
(a)

(b)

Figure 1.
Examples of reconstructed images for sources of sensitive emissions in the form of (a) VGA standard (receiving frequency f_o = 681 MHz, measure bandwidth BW = 10 MHz) and (b) DVI standard (receiving frequency fo = 852 MHz, measure bandwidth BW = 50 MHz).

standards are the object of the research on solutions that effectively protect processed graphical data. Most frequently, the only solutions used for electromagnetic data protection are those design-related which decrease the level of unwanted emissions at a source. Many people consider which standard is safer.

Another no less dangerous source of electromagnetic emission, formidable from the point of view of the possibility of conducting electromagnetic "watch", are computer laser printers [15, 16]. They translate the electronic form of processed data into graphical form during the printing process. As with every electronic device, printers are sources of electromagnetic emanations [17]. Besides control signals, which carry no information (e.g. directing the operation of stepper motors or heaters), there are other signals (useful signals) that are correlated with the information being processed. Such emissions are called "sensitive" or "valuable" or "compromising" emanations from the point of view of electromagnetic protection of processed information. Processed data may be information displayed on a computer screen or printed (**Figure 2**).

Organizational and technical solutions are the most often used methods for limiting infiltration sensitivity of devices. Technical solutions are limited to changes in
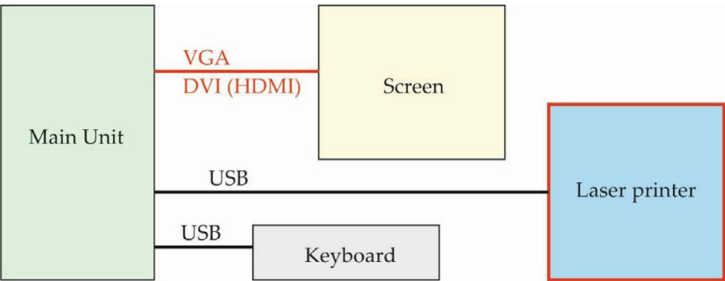
Figure 2.
Sources of sensitive emissions on an example of a personal computer (PC).

the design of devices that typically increase the cost of such devices and sometimes limit their functionality. Therefore, it is desirable to find solutions that avoid these drawbacks and at the same time allow "safe" processing of classified information. An example of an organizational solution might be the establishment of a "control zone" around susceptible devices, relying on distance to attenuate signals below levels that can be received outside the control zone. Both solutions aren't acceptable by users of these devices.

Note that the costs of acquiring a single computer set, referred to as TEMPEST class, are an expense of several of thousand dollars. That 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 the use of them becomes safe for sources in both the form of video track standard VGA and DVI and video track of laser printers. In the case of laser printers, one technical method that is commonly used in the field of electromagnetic compatibility—both to reduce the amount of electromagnetic interference emitted from the device and the susceptibility of the device to electromagnetic disturbance—is the use of differential-mode signals. This solution protecting printed information was described in [18].

Currently there are new searched methods based on software solutions. Such solutions could change the character of radiation source. The methods could be used to support other solutions or they could be used alone. One of them is safe fonts [19, 20]. Very often such fonts are called TEMPEST fonts. There are three proposed sets of such fonts: Symmetrical Safe font, Asymmetrical Safe font and Simply Safe font (**Figure 3**). These sets of fonts differ in properties of construction of font characters.

Usefulness of these fonts was confirmed from electromagnetic protection's point of view for analogue graphic standard VGA, digital graphic standard DVI and laser printers. The collections of these fonts also are resistant to optical character recognition (OCR).

A side-channel attack (SCA) plays a very important role in the electromagnetic eavesdropping process. The SCA is built from a source of emission, a receiver of emission and space between these two mentioned elements (**Figure 4**).

This type of SCA has the characteristics of a high-pass filter, which is an important property from the protection of information against electromagnetic infiltration process' point of view. The SCA is described by formula.

$$y'(t) = \lim_{\Delta t \to 0} \frac{x(t - \Delta t) - x(t)}{\Delta t}, \qquad (1)$$

where $y(t)$ is the signal (sensitive emission) on the output of SCA and $x(t)$ is the signal on the input of SCA. Very often on the output of receiver, a module $y''(t)$ of the signal $y(t)$ exists:

$$y''(t) = \left| \lim_{\Delta t \to 0} \frac{x(t - \Delta t) - x(t)}{\Delta t} \right|. \tag{2}$$

In real conditions we cannot forget about noises $s(t)$ and electromagnetic disturbances $d(t)$ which could disturb sensitive emissions $y'''(t)$ measured on the output of the SCA [21]. Then.

$$x^{'(t)} = x(t) + s(t) + d(t), \tag{3}$$

$$y'''(t) = \left| \lim_{\Delta t \to 0} \frac{x'(t - \Delta t) - x'(t)}{\Delta t} \right|. \tag{4}$$

On the output of SCA, only vertical and diagonal edges (rising edges and falling edges of pulses of electrical video signals, as on **Figure 1a**) are visible on reconstructed images. There are no visible horizontal edges. It is a very important feature from electromagnetic penetration process' point of view.
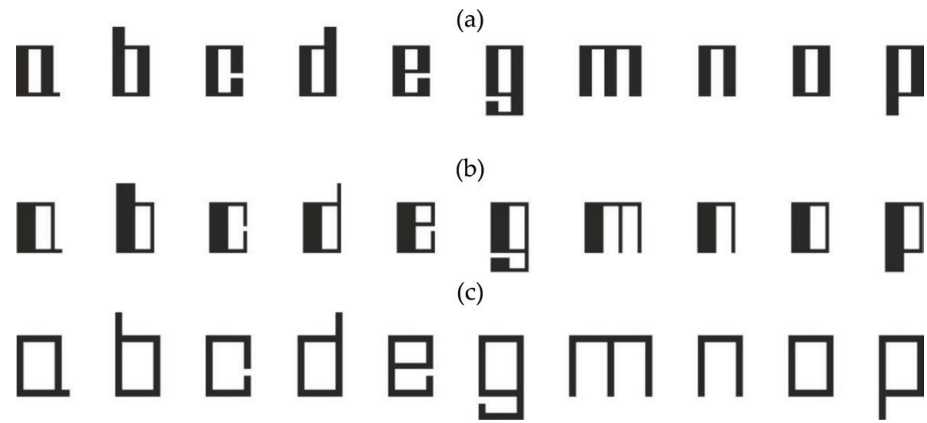

Figure 3.
Examples of characters of safe fonts: (a) symmetrical safe font, (b) asymmetrical safe font and (c) simply safe font.
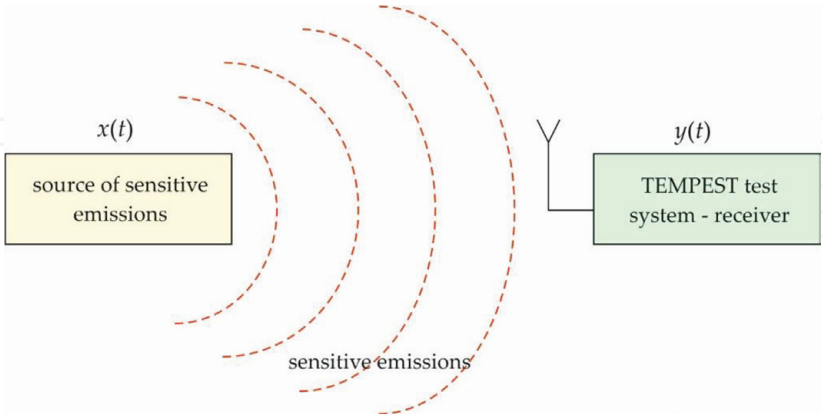

Figure 4.
A scheme of side-channel attack.

2. TEMPEST fonts

2.1 Introduction

An important element of daily processing of text information is the use of computer fonts. Traditional Arial and Times New Roman fonts are the most

popular. Characters of these fonts have decorative elements such as an ear, a bowl, an eye, a serif, a tail, a terminal, a bracket, a loop, etc. The characters are oval, and angles between the individual elements of characters aren't equal to 90° [22, 23]. In addition, the widths of lines building characters are variable. During the processing of text data, each character of font has its representation in the form of electrical signal. This signal is transmitted from a computer to a screen or to a laser printer. In this case, this signal becomes a source of electromagnetic emissions which have characteristics of this signal.

Safe fonts are designed according to safety criteria [24, 25]:

- Lines building the characters intersect at a right angle (each character is built only from vertical and horizontal lines).

- Font characters are devoid of decorative and diagonal elements.

- General contour of characters of safe font has a rectangle shape.

The safe fonts are fully usable. They are resistant to electromagnetic infiltration process as well as OCR process.

The traditional fonts do not meet the mentioned requirements (**Figure 5**).

2.2 Symmetrical safe font

The font characters are devoid of decorative and diagonal elements. The lines building the characters intersect at a right angle. Each character is built from lines about two widths (**Figure 6**). Wider lines are vertical lines of the character; thinner lines are horizontal lines of the character. Simultaneously the right proportions of the line width and the clearance of each character of the font are maintained. It means that the distance between two wider vertical lines is equal to the width of vertical line. The corresponding characters have ascender and descender. There aren't unnecessary decorative elements. This makes that the characters of the font are similar with each other with high values of correlation coefficient between characters.

2.3 Asymmetrical safe font

Similar to the Symmetrical Safe font, this font could be used in printing process and computer techniques. The characters of this font are devoid of decorative and diagonal elements. The lines building the characters intersect at a right angle. Each character is also built from lines about two widths (**Figure 7**). However, the location of the lines in the characters is different than for the Symmetrical Safe font. Wider lines are vertical lines but only as a left part of the character. Thinner lines appear as horizontal lines of the character and as a right element of the character. It means that the width of wider vertical line is the equal sum of distance between vertical lines and width of thinner vertical line. Simultaneously the right proportions of the width of the lines and the clearance of each character of font are maintained. The corresponding characters have ascender and descender.

Figure 5.
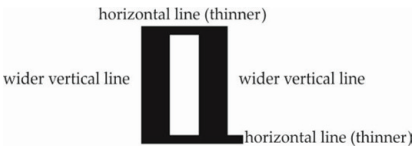*Distinctive features of times new Roman font on an example of "a" character.*

Figure 6.
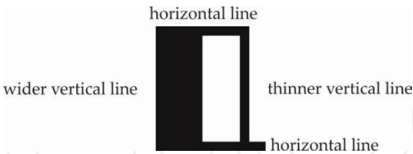*A construction of characters of symmetrical safe font.*

Figure 7.
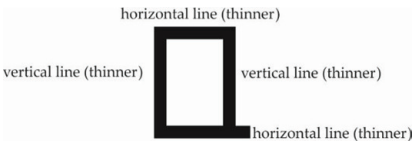*A construction of characters of asymmetrical safe font.*

Figure 8.
A construction of characters of simply safe font.

2.4 Simply safe font

The Simply Safe font is the third set of safe fonts. The characters of this font are devoid of decorative and diagonal elements. The lines building the characters intersect at a right angle. Each character is built from lines about one width (**Figure 8**). This feature distinguishes this font from two others. Simultaneously the right proportions of the width of the lines and the clearance of each character of font are maintained. The corresponding characters have ascender and descender.

3. Sensitive emissions and possibilities of reconstruction of primary information

3.1 Introduction

To assess sensitive emissions from electromagnetic protection of information's point of view, a lot of tests were carried out. The tests were conducted in special conditions without additional unwanted sources of electromagnetic disturbances [26, 27]. Such conditions exist inside an anechoic chamber (**Figure 9**). Such type of chamber is built from metal sheets. Internal walls of the chamber are covered with special hybrid material. These materials (graphite tiles and so-called cones containing graphite compounds) absorb an energy of electromagnetic waves. There is lack of secondary electromagnetic waves.

Sensitive emissions are measured in the range of frequency from about 100 to 1500 MHz. The upper limit of frequency is pointed by digital video standard. For analogue standard the upper limit is equal to about 800 MHz. Of course, it depends on the parameters of image displayed on a screen.

Corresponding tests were carried out to show the effectiveness of the tempest fonts in the protection of information against electromagnetic penetration process. In
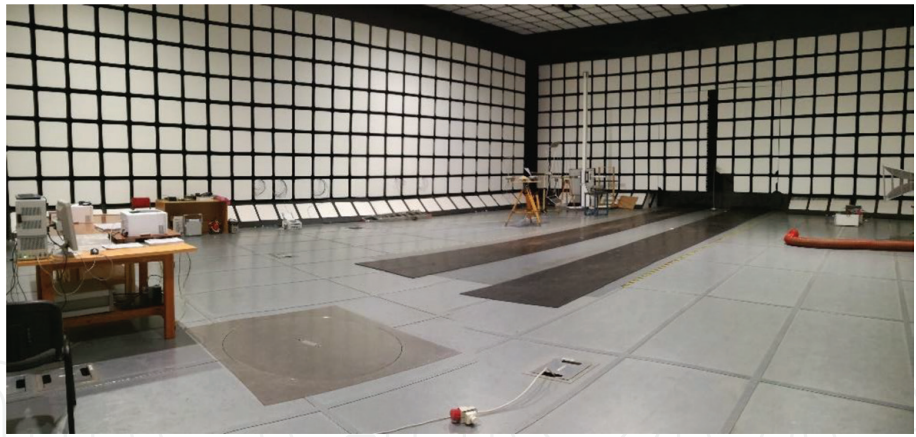
Figure 9.
A view of anechoic chamber with hybrid material.

analyses we can use a visual method. It applies to images obtained based on sensitive emissions measured on corresponding frequencies (**Figure 10**, selected frequencies).

Parameters of displayed image:

- Resolution (1024 × 768/60 Hz)

- Size of font characters (22 p.)

- Magnification (600%)

Analyzing the images we have to remember the size of characters and the magnification. For typical parameters, i.e. 12 p. of the size and 200% of the magnification, the recognition process is much harder and even impossible for safe fonts. Very often a coefficient of character error rate (CER)

$$CER = \frac{m + k}{q} = \frac{m + (u - n)}{q}, \tag{5}$$

where u is the number of characters looked for in an analyzed image, m is the number of characters incorrectly recognized, n is the number of characters correctly recognized, k is the number of unrecognized but looked for characters in an analyzed image ($k = u - n$), and q is the number of all characters existing in an analyzed image and is used for precise assessment. The values of this parameter were shown on **Table 1**.

3.2 VGA standard

Signal compatible with the VGA standard has an amplitude ranging from 0 to 0.7 V, and the maximum number of signal levels, when using all 8-bits to encode the brightness of each component of the pixel's color, is equal to 256. This means 16, 777, 216 colors are possible to be displayed with the red, green and blue (RGB) color palette and correspond to the true color (24-bits) graphic card work mode.

Video signal of the VGA standard has a characteristic structure which enables to distinguish unique signatures, which allow its identification, both in the time and the frequency domain.

A sensitive emission was measured among other things on the frequency equal to 417 MHz (**Figure 10a**). The emission allowed to reconstructed primary information [28–30] which was shown on **Figure 11**.
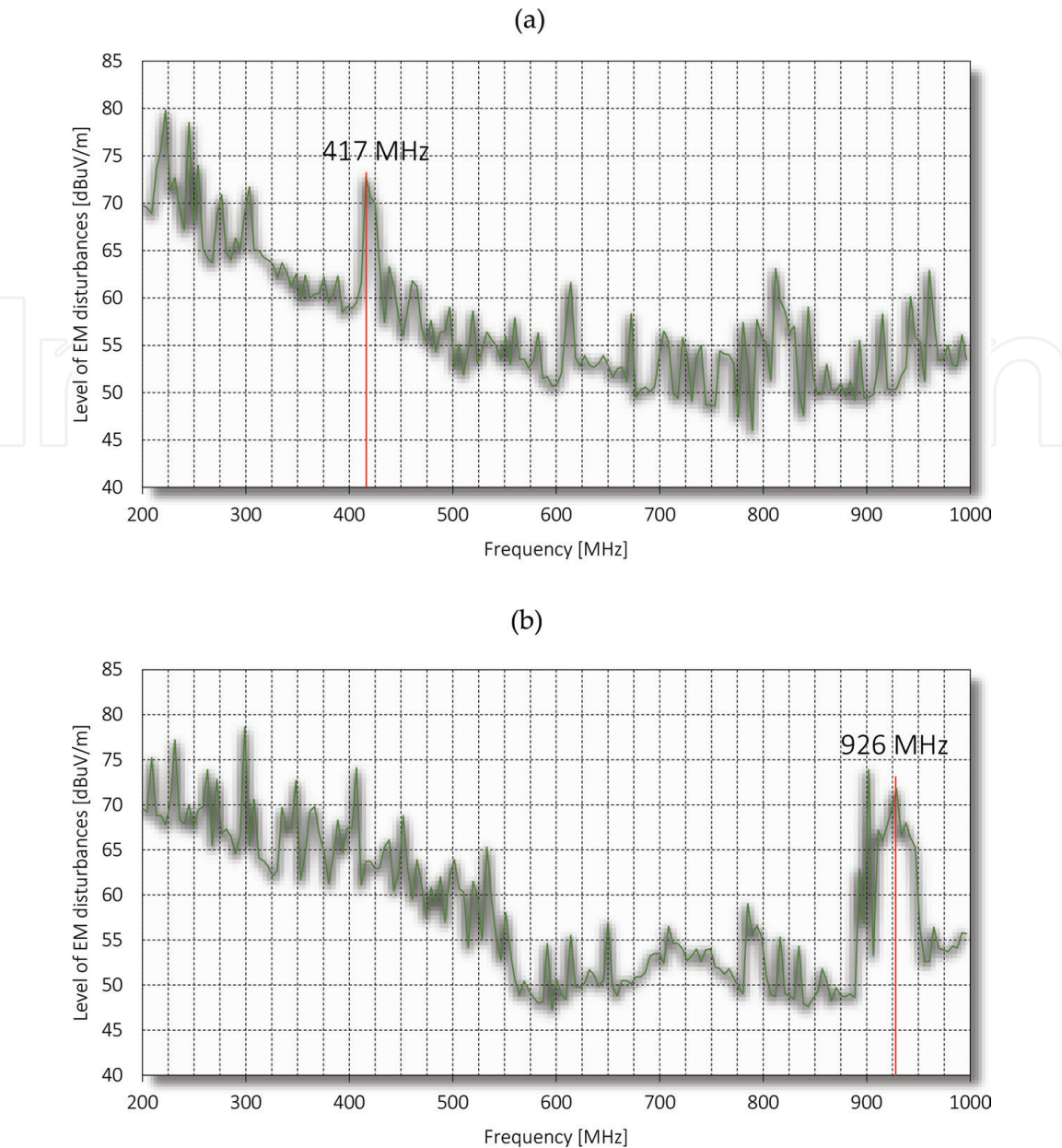
(a)

(b)

Figure 10.
Levels of electromagnetic emissions measured in frequency domain: (a) VGA standard (b) DVI standard.

3.3 DVI standard

DVI standard specification, developed by the Digital Display Working Group (DDWG), gathering many leading hardware manufacturers, was published in 1999 [11]. In this encoding method, 8-bit RGB data are converted in the graphic card's transmitter into a 10-bit format using transition minimalization and constant component balancing (DC-balanced sequence) techniques. However, that does not mean that transition-minimized differential signalling (TMDS) encoding and extension DVI standard are impervious to electromagnetic eavesdropping. An electric signal in the form of a series of zeros and ones is a source of sensitive emissions. Radiated emission propagates in the space surrounding the source and is subjected to the effects of a high-pass filter (SCA). As a result of the original signal (TMDS) distortions of this kind, the form of sensitive emission signal becomes usable for electromagnetic eavesdropping.

Time series of signals responsible for transmission of information on pixels' color components in DVI standard show that the DVI interface retains the framing principles of signals from the VGA interface. Bit (impulse) series corresponding to individual pixels of the image are transmitted in accordance with the TMDS clock in

Character	Arial font	Times new roman font	Symmetrical safe font	Asymmetrical safe font	Simply safe font
VGA standard					
d	0	0	0	371	1
e	1	6	122	354	48
i	43	17	1	128	115
o	3	9	339	212	174
u	1	2	369	45	107
DVI (HDMI) standard					
d	4	4	25	95	72
e	4	4	140	45	65
i	46	14	42	15	153
o	36	7	60	236	351
u	7	3	104	562	6

Table 1.
Values of character error rate for selected characters of traditional and safe fonts.
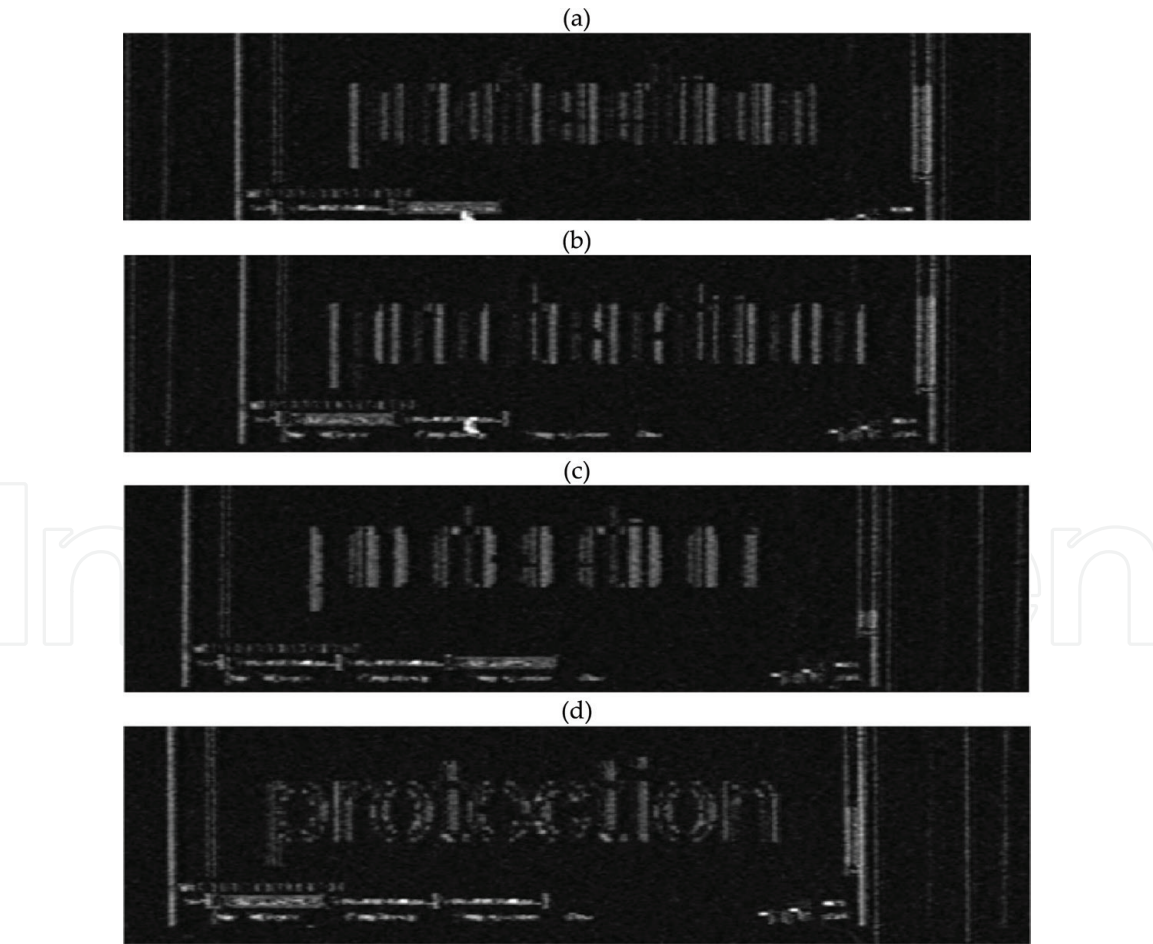

Figure 11.
Fragments of reconstructed images including characters of (a) symmetrical safe font, (b) asymmetrical safe font, (c) simply safe font and (d) Arial font.

strictly defined time periods. Those periods reflect horizontal and vertical synchronization signals of the analogue VGA signal.
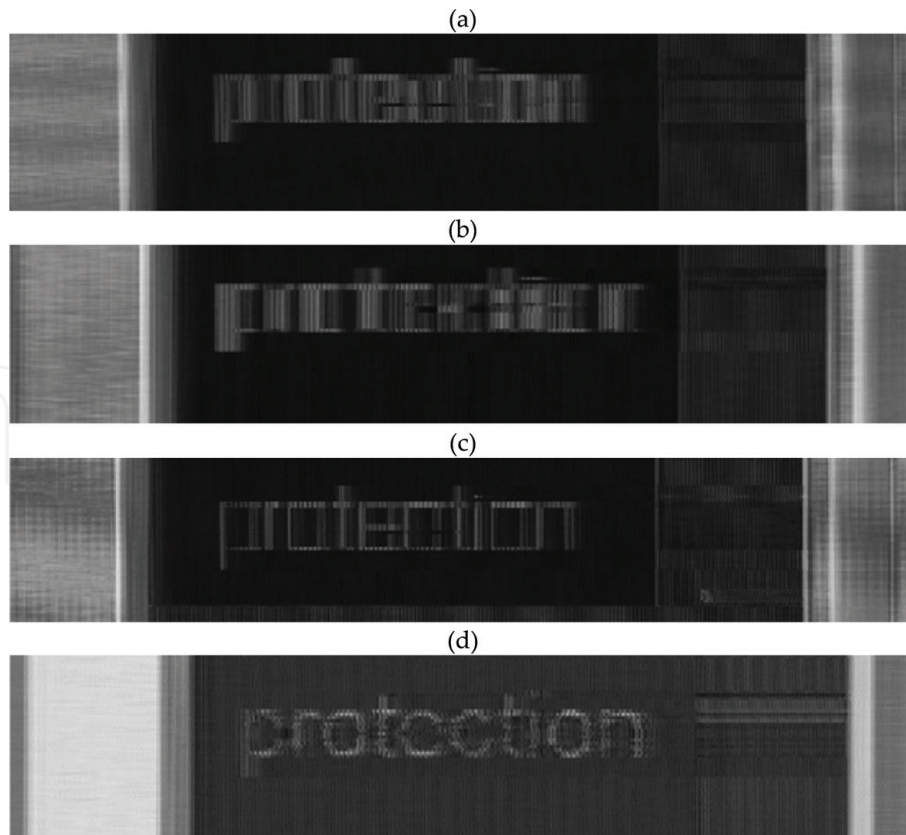
(a)

(b)

(c)

(d)

Figure 12.
Fragments of reconstructed images including characters of (a) symmetrical safe font, (b) asymmetrical safe font, (c) simply safe font and (d) Arial font.

A sensitive emission was measured among other things on the frequency of 926 MHz (**Figure 10b**). The emission allowed to reconstructed primary information which was shown in **Figure 12**.

4. Conclusions

In this chapter the possibilities of electromagnetic penetration for sources of sensitive emissions in the form of analogue (VGA) and digital (DVI, HDMI) video standards were described. A solution, which protects processed text information, was shown. The solution is based on three sets of tempest font: Symmetrical Safe font, Asymmetrical Safe font and Simply Safe font.

Each font is free from distinctive features. Characters of fonts are characterized by very high level of similarity. Values of correlation coefficient are more than 0.7, but the level of legibility is acceptable by potential users. The high level of similarity of characters on the input of SCA causes that on the output of SCA the recognition of characters is very difficult. For traditional fonts (e.g. Arial or Times New Roman), the infiltration process is possible and data acquisition is not difficult (**Figure 13**) [31, 32]. Additionally the tempest fonts counteract the penetration process of laser printers. Therefore the new solution is called as a universal solution.

An application of new solution is very easy. Only an installation corresponding set font on a computer is necessary [19]. The solution can replace present solutions basing on shielding (very heavy elements), filtering, grounding and so on.

The safe fonts obtained protection of the Polish Office Pattern in the form of Industrial Design (No. 24487, **Figure 14a**) and Patent (No. 231691, **Figure 14b**) [24, 25].
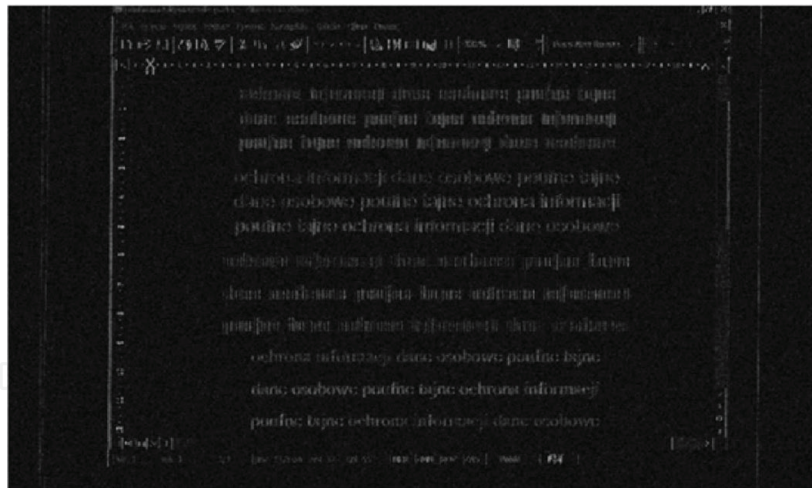
Figure 13.
Example of reconstructed image for text size 14 p. and magnification 160% written using safe and traditional fonts.

(a)   (b)

Figure 14.
A certificate of Industrial Design (a) and a Patent (b) for safe fonts.

Conflict of interest

The author declares no conflict of interest of this book chapter.

Author details

Ireneusz Kubiak
Military Communication Institute, Poland

*Address all correspondence to: i.kubiak@wil.waw.pl

IntechOpen

References

[1] Lee HK, Kim JH, Kim SC. Emission security limits for compromising emanations using electromagnetic emanation security channel analysis. IEICE Transactions on Communications. 2013;**E96-B**(10):2639-2649. DOI: 10.1587/transcom.E96.B.2639

[2] Nan Z, Yinghua L, Qiang C, Yiying W. Investigation of unintentional video emanations from a VGA connector in the desktop computers. IEEE Transactions on Electromagnetic Compatibility. 2017;**59**(6):1826-1834

[3] Jinming L, Jiemin Z, Taikang L, Yongmei L. The reconstitution of LCD compromising emanations based on wavelet denoising. In: 12th International Conference on Computer Science and Education (ICCSE); 22-25 August 2017; Houston, USA. pp. 294-297. DOI: 10.1109/ICCSE.2017.8085505

[4] Kubiak I. Laser printer as a source of sensitive emissions. Turkish Journal of Electrical Engineering and Computer Sciences. 2018;**26**(3):1354-1366. DOI: 10.3906/elk-1704-263

[5] Kubiak I. LED printers and safe fonts as an effective protection against the formation of unwanted emission. Turkish Journal of Electrical Engineering and Computer Sciences. 2017;**25**(5):4268-4279. DOI: 10.3906/elk-1701-128

[6] Litao W, Bin Y. Analysis and measurement on the electromagnetic compromising emanations of computer keyboards. In: Seventh International Conference on Computational Intelligence and Security; 3-4 December 2011; Sanya. pp. 640-643. DOI: 10.1109/CIS.2011.146

[7] Tokarev AB, Pitolin VM, Beletskaya SY, Bulgakov AV. Detection of informative components of compromising electromagnetic emanations of computer hardware. International Journal of Computer Technology and Applications. 2016;**9**:09-19

[8] Boitan A, Bărtușică R, Halunga S, Bîndar V. Video signal recovery from the laser printer LCD display, Proceedings Volume 10977, Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies IX, 2018. Event: Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies IX, 2018, Constanta, Romania. DOI: 10.1117/12.2324759

[9] Butnariu V, Trip B, Macovei A, Rosu G, Boitan A, Halunga S. Power line compromising emanations analysis. Annals of the University of Craiova, Electrical Engineering Series. Vol. 48. 2018

[10] Macovei A, Boitan A, Trip B, Halunga S. Detection of electromagnetic emissions transmitted on the power line through electrical conduction. In: International Conference on Applied and Theoretical Electricity (ICATE 2018); DOI: 10.1109/ICATE.2018.8551437

[11] Digital Visual Interface DVI Revision 1.0. Available from: http://www.cs.unc.edu/~stc/FAQs/Video/dvi_spec-V1_0.pdf

[12] HDMI Specification Ver.1.3a. Available from: https://www.hdmi.org/manufacturer/specification.aspx

[13] Jun S, Yongacoglu A, Degang S, Dong W. Computer LCD recognition based on the compromising emanations in cyclic frequency domain. In: IEEE International Symposium on Electromagnetic Compatibility, Ottawa, Canada; 25-29 July 2016; pp. 164-169

[14] Kubiak I. Video signal level (colour intensity) and effectiveness of

electromagnetic infiltration. Bulletin of the Polish Academy of Sciences—Technical Sciences. 2016;**64**:207-2018. DOI: 10.1515/bpasts-2016-0023

[15] Kubiak I. The influence of the structure of useful signal on the efficacy of sensitive emission of laser printers. Measurement. 2018;**119**:63-76. DOI: 10.1016/j.measurement.2018.01.055

[16] Loughry J, Umphress DA. Information leakage from optical emanations. ACM Transactions on Information and System Security. 2002;**5**:262-289

[17] Michael JM. The pentagon worries that spies can see its computer screens, someone could watch what's on your VDT. The Wall Street Journal. 2000;**8**:1-2

[18] Kubiak I, Loughry J. LED Arrays of Laser Printers as Sources of Valuable Emissions for Electromagnetic Penetration Process, arXiv:1808.03007v1 [cs.CR]; 9 August 2018

[19] Kubiak I. TEMPEST font counteracting a non-invasive acquisition of text data. Turkish Journal of Electrical Engineering and Computer Sciences. 2018;**26**(1):582-592. DOI: 10.3906/elk-1704-9

[20] Kubiak I. Influence of the method of colors on levels of electromagnetic emissions from video standards. IEEE Transactions on Electromagnetic Compatibility. 2018:1-9. DOI: 10.1109/TEMC.2018.2881304

[21] Song TL, Jeong YR, Jo HS, Yook JG. Noise-jamming effect as a countermeasure against TEMPEST during high-speed signaling. IEEE Transactions on Electromagnetic Compatibility. 2015;**57**(6):1491-1500

[22] Shainir A, Rappoport A. Extraction of typographic elements from outline

representations of fonts. Computer Graphics Forum. 1996;**15**(3):259-268. DOI: 10.1111/1467-8659.1530259

[23] Nanxuan Z, Ying C, Lau WH. Modeling fonts in context: Font prediction on web designs. Computer Graphics Forum. 2018;**37**(7):385-395. DOI: 10.1111/cgf.13576

[24] Kubiak I. Industrial Design No. 24487, Polish Pattern Office, 10 September 2018

[25] Kubiak I. Pattern No. P.408372 Method for protecting transmission of information, Polish Pattern Office, 3 December 2018

[26] Song TL, Jong-Gwan Y. Study of jamming countermeasure for electromagnetically leaked digital video signals. In: IEEE International Symposium on Electromagnetic Compatibility; 1-4 September 2014; DOI: 10.1109/EMCEurope.2014.6931078

[27] Yuan K, Grassi F, Spadacini G, Pignari SA. Crosstalk-sensitive loops and reconstruction algorithms to eavesdrop digital signals transmitted along differential interconnects, IEEE Transactions on Electromagnetic Compatibility. 2017;**59**(1):256-265

[28] Juric I, Nedeljkovic U, Novakovic D, Pincjer I. Visual experience of noise in digital images. Tehnicki Vjesnik-Technical Gazette. 2016;**23**(5):1463-1467

[29] Lorencs A, Sinica-Sinavskis J. One method of image processing and its numerical analysis. Elektronika IR Elektrotechnika. 2010;**103**(7):25-30

[30] Manson J, Schaefer S. Wavelet rasterization. Computer Graphics Forum. 2011;**30**(2):395-404. DOI: 10.1111/j.1467-8659.2011.01887.x

[31] Zoric A, Perisic D, Obradovic S, Spalevic P. Virtual multisensors data

acquisition and analysis system design.
Elektronika IR Elektrotechnika.
2011;**116**(10):49-54. DOI: 10.5755/j01.
eee.116.10.879

[32] Kuusik A, Reilent E, Lõõbas I,
Luberg A. Data acquisition software
architecture for patient monitoring
devices. Elektronika IR Elektrotechnika.
2010;**105**(9):97-100