DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process

Ireneusz Kubiak
Electromagnetic Compatibility Department
Military Communication Institute
05-130 Zegrze Poludniowe, Poland
i.kubiak@wil.waw.pl

Artur Przybysz
Electromagnetic Compatibility Department
Military Communication Institute
05-130 Zegrze Poludniowe, Poland
a.przybysz@wil.waw.pl

***Abstract*—Increasingly common usage of new technologies in information processing generates escalating threat of confidentiality loss. Utilizing current VGA analog standard based means raises many doubts. It is a widely held view that this standard is highly susceptible to electromagnetic infiltration. Digital technologies are supposed to ensure a higher security level. This also applies to data processed in graphic form, especially those being transmitted to graphic display devices, such as computer monitors using DVI and DisplayPort standards. This article presents a comparative analysis of graphic technologies (DVI and DisplayPort) in terms of the electromagnetic safety of processed data. Analyses shown are based both on simulations results and practical study. The products of recreating the data using registered sensitive emission signals for studied graphical standards are presented.**

Keywords—Digital Video Interface; DisplayPort, electromagnetic safety; information leakage; electromagnetic eavesdropping; sensitive emission; Side Channel Attack

I. INTRODUCTION

Every electronic device is a source of electromagnetic disturbances. They develop unintentionally. Those disturbances often possess the same features as the data being processed [1]. When it comes to devices such as personal computers (mobile or stationary), particularly unreliable in terms of confidentiality of processed data are information display circuits [2, 3, 4]. Those circuits consist of graphics cards, display monitors and signal cables. Exceptional threat lies in the fact that the information is presented on the display in overt form and only a „glimpse" on the screen or its replica is enough to intercept it. Such a replica can be created based on side electromagnetic emissions occurring during video circuits operation. It is enough to mention that by virtue of Maxwell's equations every circuit with changing electric current is a source of changing electromagnetic field. When shifts in current waveform parameters (amplitude, impulse length) directly reflect information of interest, reconstructing it proves elementary. Under those circumstances, it is possible to consider non-invasive information gathering and evaluate the effectiveness of electromagnetic eavesdropping [5, 6].

II. INFORMATION DISPLAY CIRCUITS

Typical means of displaying data processed by the computer utilize the raster technique. An area of a screen is a matrix of $M \times N$ spots (M rows of N elements). Every spot (pixel) on the screen reflects the colour intensity of the corresponding image fragment.

Old CRT displays were built using screens consisting of a set number of spots covered in phosphor. A substance capable of emitting light waves when exposed to a stream of electrons generated by a thermionic tube. In the case of colour monitors, hue representation requires transmission of information on three components of colour (R – Red, G – Green, B – Blue). Signals carrying the information about the brightness and colour of every pixel are sent in series, which drastically facilitates electromagnetic eavesdropping [7, 8].

Modern display monitors utilize LCD or LED screens, which procure given hue by controlling colour filters. Those filters pass or suppress the stream of photons generated by the fluorescent lamp or a set of LEDs located behind the filter matrix. The requirement of filter control simplification, display monitors and graphics cards compatibility and economic reasons prevent the usage of separate signals managing filters responsible for brightness and hue of every spot on the screen. However, like in CRTs, first the adequate (next) rows are activated with a common signal and then filter control systems of individual pixels are triggered. The filters' control signals (input signals) are sent in series which, as previously stated, facilitates electromagnetic eavesdropping [9, 10].

III. VGA ANALOG INTERFACE

CRT display monitors are analog devices. Because of that, the intensity of each of the components of colour for each pixel is defined as the amplitude of a corresponding electric signal. The higher the signal level the brighter the colour [11]. Therefore, the output system of graphics cards (digital devices) with a VGA interface is equipped with a digital to analog converter, changing the digital video signal to a form acceptable by the input system of the display monitor. Signal compatible with the VGA standard has an amplitude ranging from 0 V 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 colour, equals 256. This means 16 777 216 colours possible to display with the RGB colour palette and corresponds to the *true colour* (24-bits) graphics card work mode.

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

IV. DVI AND DISPLAYPORT DIGITAL INTERFACES

As previously mentioned, graphics cards output systems are digital structures. Digital interfaces would allow for the generated signals to be transmitted to the display systems unchanged. The need to accommodate users' requirements (high resolutions) means that more sophisticated methods of

978-1-7281-0594-9/19/$31.00 © 2019 IEEE

preparing the bit streams for transmission are used. It is a compromise between the transmission speed requirements, balancing the signals constant component and minimizing electromagnetic emissions. Those interfaces utilize 8b/10b encoding and differential signalling.

A. DVI Interface

DVI (Digital Visual Interface) standard specification, developed by the Digital Display Working Group (DDWG), gathering many leading hardware manufacturers, was published in 1999 [12]. In this encoding method, 8-bit RGB data are converted in the graphics card's transmitter into a 10-bit format using transition minimalization and constant component balancing (DC-balanced sequence) techniques.

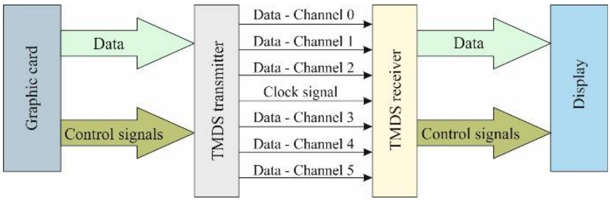


Fig.1. Signal transmission utilizing TMDS protocol

10-bit TMDS (Transition Minimized Differential Signalling) code words can represent 8-bit colour component data or 2-bit synchronization data transmitted in periods of time corresponding to image or line suppression (Fig.1). All 1 024 possible combinations of 10-bit code words are utilized in the following way:

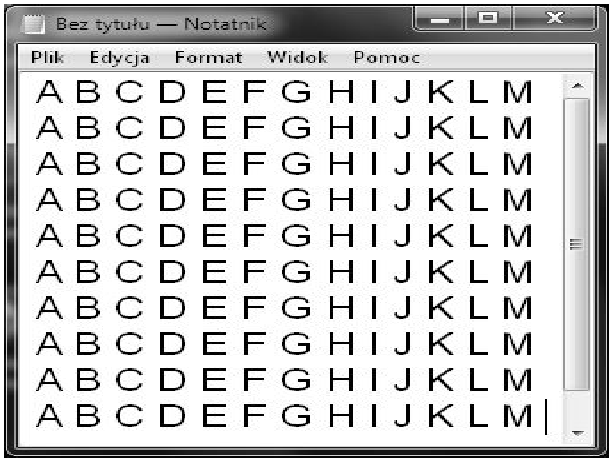
- 460 combinations used for 8-bit information data transmission; most of the 256 possible 8-bit combinations has two 10-bit equivalents (Table I);
- 4 combinations representing 2-bit control signals for synchronization purposes;
- 2 combinations used as a special marking of HDMI (High Definition Multimedia Interface) data transmission [13];
- 558 combinations reserved for future use.

TABLE I. EXEMPLARY JUXTAPOSITION OF 8-BIT AND 10-BIT CODE WORDS IN TMDS

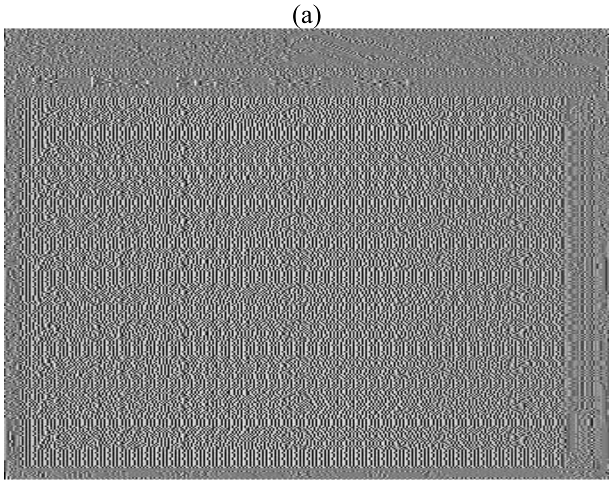
Encoding: 8-bit data to 10-bit TMDS			
Pixel		***TMDS Characters***	
Dec.	***Binary 8-bits msb-lsb***	***Char 1 lsb-msb***	***Char 2 lsb-msb***
0	00000000	0100000000	1111111111
1	00000001	0111111111	1100000000
2	00000010	0111111110	1100000001
...	...	...	...
255	11111111	0011111111	1000000000

Until recently common was the notion regarding electromagnetic safety of the DVI digital standard, steaming from the conviction that in order to recreate the information sent using it (Fig.2a) necessary would be the correct recreation of its original bit structure and subjecting it to decoding consistent with the TMDS algorithm. Indeed, the image recreated with the raster method from a signal encoded with the TMDS algorithm recorded from the interface's signal line is practically unreadable to the human eye (Fig.2b).

However, that does not mean that TMDS encoding and by 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.



(a)



(b)

Fig.2. (a) Tested image and (b) image recreated from a signal encoded in accordance with the TMDS algorithm

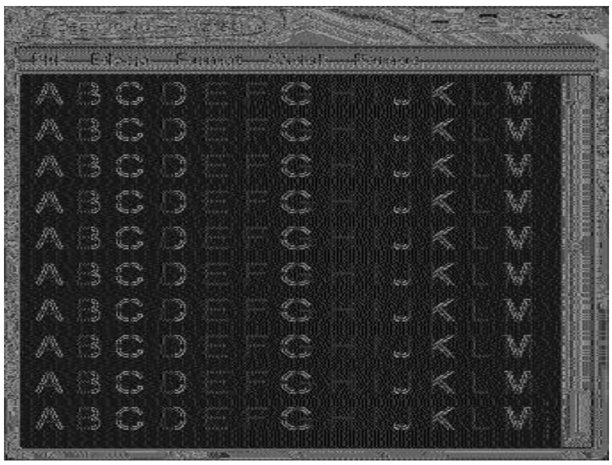
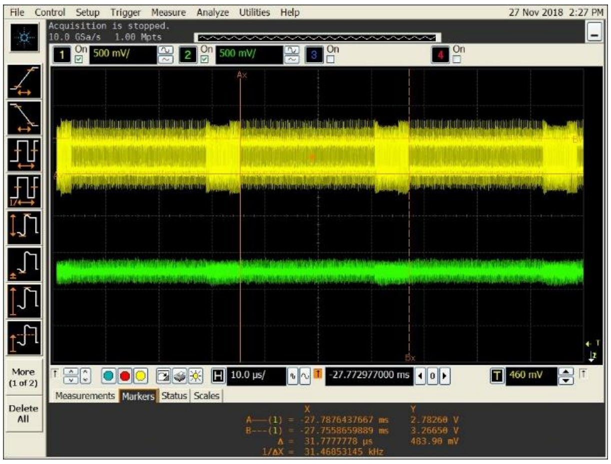


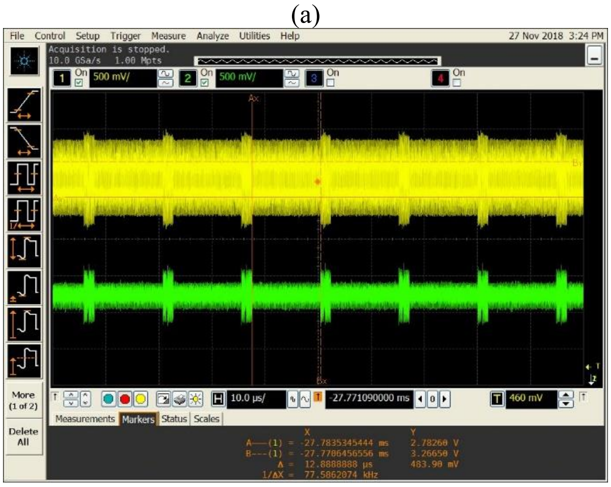
Fig.3. Image reconstructed with differentiation operation

Radiated emission propagates in the space surrounding the source and is subjected to the effects of a high-pass filter (Information Leakage Channel). As a result of the original (TMDS) signal distortions of this kind, the form of sensitive emission signal becomes usable for electromagnetic eavesdropping. Fig.3 demonstrates image reconstructed from signal shown on Fig.2b subjected to differentiation operation (equivalent to the effects of a high-pass filter).

Time series of signals responsible for transmission of information on pixels' colour components in DVI standard show that the DVI interface retains the framing principles of signals from the VGA interface (Fig.4).



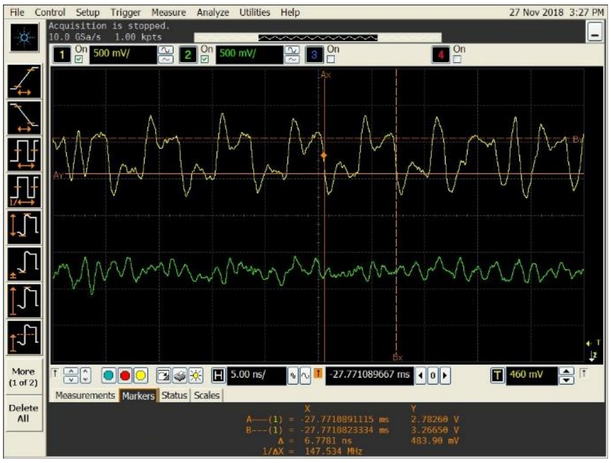
(a)



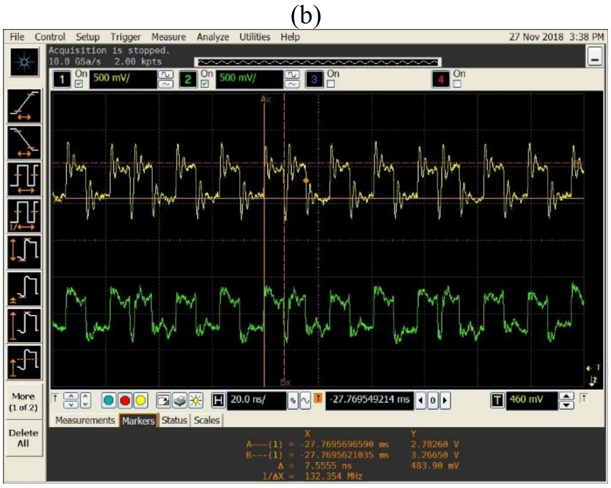
(b)

Fig.4. Time series of GREEN signal from DVI interface in (a) 640×480/60 and (b) 1920×1080/60 modes, corresponding to one line of the image displayed on the screen (upper course – Channel 0, lower course – Channel 1)

(a)



(b)



(c)

Fig.5. Time series of GREEN signal from DVI interface in 640×480/60, (b) 1920×1080/60 and (c) 2560×1440/60 modes, corresponding to one 10-bit code word of a line of the image displayed on the screen (upper course – Channel 0, lower course – Channel 1)

Bit (impulse) series corresponding to individual pixels of the image are transmitted in accordance with the TMDS clock in strictly defined time periods. Those periods reflect horizontal and vertical synchronization signals of the analog VGA signal.

DVI information signals have a constant amplitude (Fig.5). This feature prevents the counteraction of electromagnetic eavesdropping by the means of simple contrast and colour forming (signal level difference minimalization) [6].

Simultaneously, forming of the signal slopes (reducing the volume of harmonics) of digital signals can lead to transmission errors (lack of image clarity) or even a cut-off [14, 15].

TMDS algorithm doesn't safe a video signal. A bit form of this signal allows to acquisition of processed information. Fig.6 shows an reconstructed image for source of sensitive emission in shape of HDMI standard. The standard also uses TMDS algorithm to code video signal.

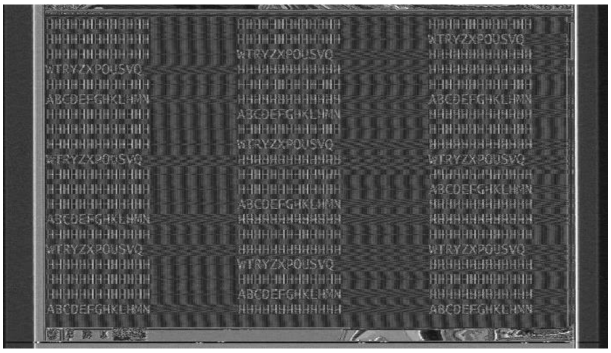


Fig.6. Image reconstructed from the sensitive emission signal for the data transfer via the HDMI interface; frequency of occurring of the sensitive emission signal f_o = 419 MHz, BW = 50 MHz

B. DisplayPort Interface

DisplayPort (DP) standard specification was developed by VESA (Video Electronics Standards Association) in 2006 and launched on the market in 2008 [16]. In contrast with the DVI it is a video signal transmission standard based on data packets transfer (like the Internet network) This interface, much like DVI, employs 8B/10B encoding (ANSI X3.230-1994, clause 11, Information Technology – Fibre Channel – Physical and Signalling Interface) but the data are previously scrambled using a 16-bit shift register (XOR).

As previously mentioned, data are transmitted in packets. They are arranged in blocks (Transfer Units) which ensures a fixed size of the packets, 64 symbols. Transmission speed does not depend on the operating mode. Packets are transmitted isochronously. Unlike DVI, DP standard uses dual-channel transmission as early as in the Full HD (1920 × 1080) mode. Data can be transferred via a dedicated channel (SST – Single Stream Transport) or a shared one (MST – Multi-Stream Transport) in which case up to 63 receiving devices can be handled by the broadcasting device (packet addressing).

DisplayPort link consists of the Main Link, supplementary link (AUX CH) and a signal line (Hot Plug Detect) (Fig.7). Main Link, used for transmission of uncompressed, isochronous streams of audio and video data, is a unidirectional channel. It can contain four data lines. Auxiliary channel is bidirectional and used for managing links and operating devices. HPD signal is used for detecting connection with the receiving device.

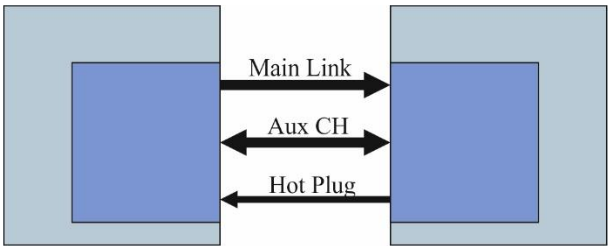


Fig.7. DisplayPort link structure

DisplayPort interface utilizes packet transmission. Data corresponding to audio or video information are grouped into packets in accordance with specified rules so that the data streams could be correctly reconstructed in their original format and per their time base by the receiving device. The data stream to Main Link mapping is suited for utilizing different amounts of link's lines.

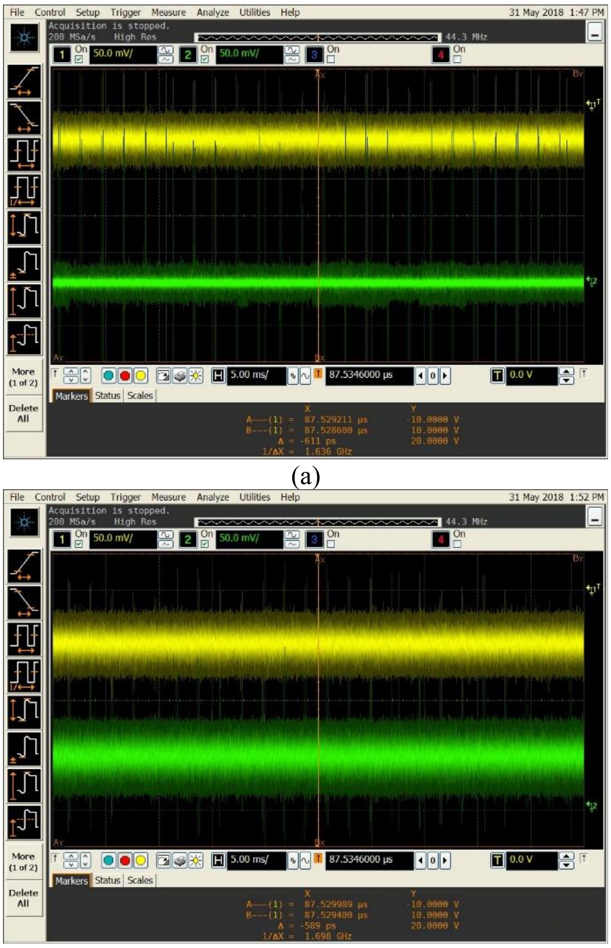
Table II shows how information data are directed to different Main Link's lines depending on the number of lines used (1, 2 or 4).

TABLE II PIXEL PLACEMENT IN DP LINK'S LINES

Lane	Pixel
1	All pixels to Lane 0
2	Pixel 2N to Lane 0 Pixel 2N+1 to Lane 1
4	Pixel 4N to Lane 0 Pixel 4N+1 to Lane 1 Pixel 4N+2 to Lane 2 Pixel 4N+3 to Lane 3

Lack of a separate clock channel and scrambling of data symbols before ANSI 8B/10B encoding provides a reduction of electromagnetic disruption which is vital when video stream contains a static image (for example, many letters 'H' scattered across the screen – typical EMI testing image).

The nature of registered time series of signals responsible for transmission of information on colour components from the DP interface shows that this interface does not retain the framing principles of signals from the VGA interface.

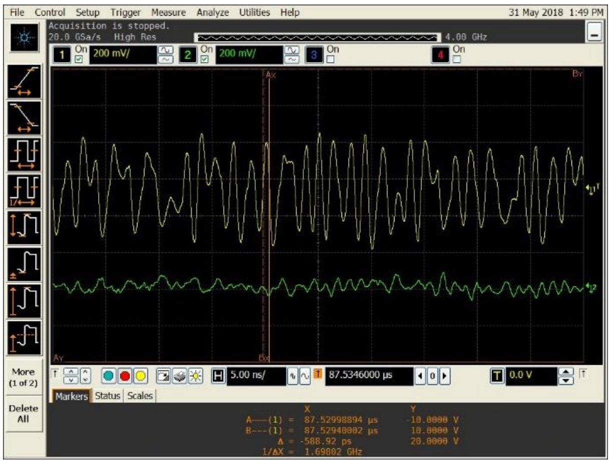


(a)

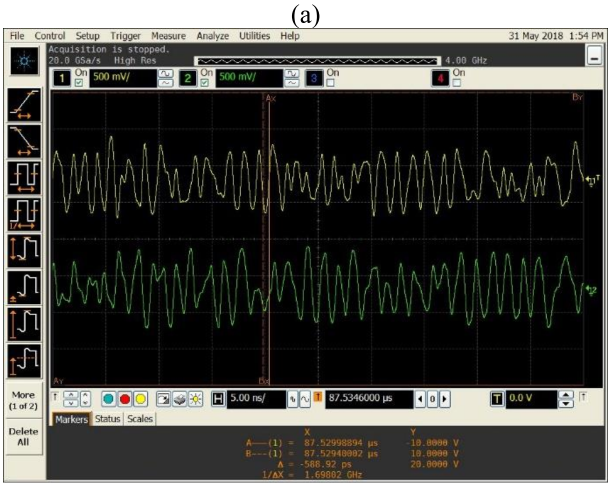
(b)

Fig.8. Time series of GREEN signal from DP interface in (a) 640×480/60 and (b) 1920×1080/60 modes, corresponding to the whole image displayed on the screen (upper course – Channel 0, lower course – Channel 1).

Bit (impulse) series corresponding to the image's pixels are being sent continuously and it is not possible to distinguish the characteristic time periods, connected with the synchronization signals, in their structure (Fig.8 and 9).



(a)



(b)

Fig.9. Time series of GREEN signal from DP interface in (a) 640×480/60 and (b) 1920×1080/60 (right) modes, corresponding to one bit of a 10-bit symbol of a pixel of the image displayed on the screen (upper course – Channel 0, lower course – Channel 1)

Fig.10. Image reconstructed from the sensitive emission signal for the data transfer via the DP interface; frequency of occurring of the sensitive emission signal f_o = 849MHz, BW = 200 MHz

In contrast with the VGA and DVI interfaces, the duration of individual information signal impulses does not depend on the operating mode but solely on the quality of the link (cable). The initial study of the DP's electromagnetic safety proved it superior to both VGA and DVI standards. Data sent from the computer's central unit to the display monitor can't be reconstructed [17]. It is, however, possible to identify them (access whether they are being transmitted or not) (Fig.10).

Further analysis of the obtained results shows that the sensitive emission, which enables the reconstruction of the outline of the data, does not originate from the transmission medium (DP cable). The source of those emissions is the monitor displaying the data. Thus, even when using packet transmission, the necessity of data protection from electromagnetic passage still holds true.

V. Tests conditions

In order to verify the above hypothesis, for DVI and DP standards, practical studies were conducted in a screened anechoic chamber (Fig.8), which attenuation parameters within the scope of studies i.e. from 1 MHz to 10 GHz was not lower than 100 dB. Compromising emanations were recorded by using the DSI-1550-A receiver along with Microwave Downconverter DSI-1580-A (up to 22 GHz) and with a set of R&S antennas: rod antenna HE525 (100 Hz ÷ 30 MHz), biconical antenna HE526 (30 MHz ÷ 200 MHz), dipole antenna HE527 (200 MHz ÷ 1 GHz) and the EMCO Double Ridge Horn antenna (1 GHz ÷ 18 GHz). The measurement bandwidths (BW) used for measurements include 50 MHz, 100 MHz and 200 MHz.

A Hardware Raster Generator (HRG) was used to generate the image of measured emissions correlated with data processed [18]. This is an external source for vertical and horizontal sync signals of the measurement monitor image. A Signatec PDA1000 data acquisition card fitted with an 8-bit ADC converter was used to record the analysed radiated emissions. The card allows users to take signal samples at a throughput of up to 1 GB/s.

During tests the monitor including its cable, being a transmission medium for DVI and DP standards video signals, operated together with a special (TEMPEST class) computer CPU. It allowed us to eliminate the computer impact on the recorded signals of video signal correlated emissions. The data displayed on the monitor included characters letters. The measurement distance was equal 1 meter and met the requirements presented in document [19].

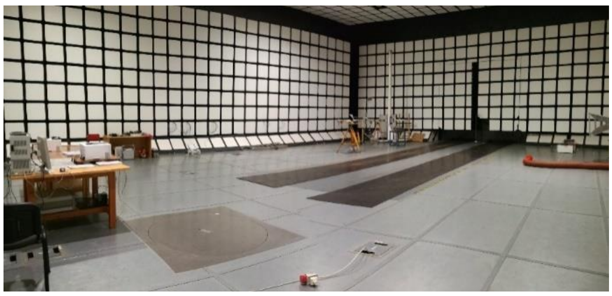


Fig.11. An anechoic chamber

VI. Conclusions

Obtained results and carried out analyses of images reconstructed from sensitive emission signals, connected with operating DVI and DisplayPort interfaces, proved the conjecture that the safest in terms of electromagnetic security is the utilization of the DisplayPort interface. Although emissions connected to it operating propagate in a wide range of frequencies reaching a few gigahertz but because of the continuous character of the transmission and data scrambling it seems to be impossible to recreate a clear image. Acquired partially decipherable images appear to relate to emission signals generated not by the transmission of data compatible with the DP standard but by processing them in the LCD display control systems. In this case, another conversion occurs to accommodate controlling the display matrix by the LVDS driver. This conclusion seems to be backed by a visual comparison of images recreated based on recordings created using DP cable with damaged and intact screening. In the first case, reconstructed images had slightly worse quality, which can possibly be attributed to DisplayPort transmission related signals obstructing the sensitive emission signals related to the LVDS interface.

In the case of DVI and VGA interfaces, it has been observed that the range of measuring frequencies, allowing for registering sensitive emission signals enabling reconstruction of images displayed on the screen, is directly connected with the display monitor operating mode (image resolution). Higher operating mode (higher pixel frequency and narrower impulses) correlates with a higher frequency range of sensitive emission signal propagation. When it comes to signals related to the DVI interface and 1920×1080/60 operating mode, the maximum frequency of sensitive signals equals approximately 4 GHz (and 1 GHz for the VGA interface).

In the case of registering signals connected with the operating digital interfaces, which single pulse repeat frequencies reach a few GHz, the quality of reconstructed images is largely determined by the quality of the devices used to receive and record the signals and to recreate the information from them. The first limitation is the bandwidth of the receiving device. For the DSI-1550A receiver used in this study, the maximal BW reaches 200 MHz. Such value allows for registering only fragments of the spectrum of studied signals. The second parameter is the download speed of the analog to digital converter used for registering signals. It is especially important when registering original signals directly from the lines of examined interfaces. Simultaneous download of many samples creates a need to operate on large quantities of data in cases of raster images and their software quality improvement (addition, filtration).

References

[1] J. Loughry, D.A. Umphress, Information Leakage from Optical Emanations. ACM Transactions on Information Systems Security, 2002; 5: 262-289.

[2] I. Kubiak, A. Przybysz, The impact of commercial equipment design to electromagnetic protection of data process, Przeglad Elektrotechniczny, 2015; 11: 41-44, doi:10.15199/48.2015.11.12.

[3] M.G. Kuhn, Compromising emanations: eavesdropping risks of computer displays, Technical reports published by the University of Cambridge Computer Laboratory, 2003.

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

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

[6] L. Ho Seong, Y. Jong-Gwan, S. Kyuhong, Analysis of information leakage from display devices with LCD, URSI Asia-Pacific Radio Science Conference 2016, August 21-25, 978-1-4673-8801-6/16/$31.00 ©2016 IEEE.

[7] Z. Mahshid, H.T. Saeedeh, G. Ayaz, Security limits for Electromagnetic Radiation from CRT Display, Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 28-30 January 2009, pp. 452-456.

[8] I. Kubiak, 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.

[9] L. Hee-Kyung, K. Yong-Hwa, K. Young-Hoon, K. Seong-Cheol, Emission Security Limits for Compromising Emanations Using Electromagnetic Emanation Security Channel Analysis, IEICE Transactions on Communications, 01 October 2013, Vol.E96-B, No.10, pp.2639-2649.

[10] A. Przybysz, Emission security of DVI and HDMI interfaces, Telecommunication review and Telecommunication news, 7/2014.

[11] N. Zhang, L. Yinghua, C. Qiang, W. Yiying, Investigation of unintentional video emanations from a VGA connector in the desktop Computers, IEEE Transactions on Electromagnetic Compatibility, Vol.59, No 6, Dec. 2017.

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

[13] HDMI Specification Ver.1.3a, https://www.hdmi.org/manufacturer/specification.aspx.

[14] I. Kubiak, The Influence of the Structure of Useful Signal on the Efficacy of Sensitive Emission of Laser Printers, Measurement, Vol.119, 2018, DOI: 10.1016/j.measurement.2018.01.055.

[15] I. Kubiak, TEMPEST font counteracting a non-invasive acquisition of text data, Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 26, No. 1/2018, DOI: 10.3906/elk-1704-9.

[16] A. Kobayashi, DisplayPort Ver.1.2 Overview, http://www.vesa.org/wp-content/uploads/2010/12/DisplayPort-DevCon-Presentation-DP-1.2-Dec-2010-rev-2b.pdf.

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

[18] K. Grzesiak, I. Kubiak, S. Musiał, A. Przybsz, Generator rastra w procesie infiltracji elektromagnetycznej. Publishing House: Military University of Technology, Warsaw, 2012, ISBN 978-83-62954-28-5.

[19] MIL-STD-461G, Requirements for the control of electromagnetic interference characteristics of subsystems and equipment.