A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels

Pieterjan De Meulemeester, Bart Scheers, and Guy A.E. Vandenbosch, *Fellow, IEEE*

***Abstract*—This paper proposes a method that reconstructs the original video data signal from leaking electromagnetic emanations of multiple video signal sources using a software-defined radio (SDR). The results of the method give valuable insights into the potential risk of this threat of obtaining sensitive information in an everyday situation. The leaking emanations of co-located identical high definition liquid crystal displays are analyzed for possible data reconstruction using a SDR of a small form factor. It is proven that the leaked emanations of multiple identical active video display units (VDUs) can be separated from each other and that their separate video images can be reconstructed individually from one data acquisition. Moreover, this is done by recovering the synchronization frequencies and the image resolution by exploiting multiple leakage channels without having any foreknowledge of the VDU's properties. A multitude of leakage channels is investigated and analyzed for their radiation pattern and their signal-to-noise ratio, and is exploited to increase the quality of the reconstructed images employing multiple-input multiple-output based techniques. As far as we can see, our results and new insights in the nature and mechanisms of multiple compromising emanations are crucial for improving video data security.**

***Index Terms*—Compromising emanations, digital video interface (DVI), high-definition multimedia interface (HDMI), information emission security, liquid crystal display (LCD), multiple-input multiple-output (MIMO), quantitative analysis, radiation pattern, side-channel attacks, signal-to-noise ratio (SNR), TEMPEST.**

I. Introduction

Video display units (VDUs) make an inherent part of today's digital processing systems, much of the digital processed information is in some way displayed on the VDU. Processed video data is not encrypted rendering the information security of the VDU vulnerable for side-channel attacks [1]. To keep data secure, much research is invested in side-channel attacks to mitigate threats that can potentially breach data integrity [2]. Like all electronic systems, a VDU inevitably leaks electromagnetic (EM) energy into the far-field resulting in electromagnetic compatibility (EMC) and electromagnetic interference (EMI) problems. By capturing these leaking emanations, different research works [3]–[8] have revealed that it is possible to recover the original video signal even if the emanations do not exceed the emission standard limits, such as the CISPR standards [9]. Today, this type of side-channel attack still poses a serious threat to data security. Mostly because it is still not quantitatively well understood and documented.

This specific threat has caught the attention of the research community in the last 35 years. However, the threat has been studied before by defense institutions that established different emission standards, such as emission security (EMSEC) and TEMPEST [10]. Their works have not been made public due to the confidentiality and the sensitivity of this information. It is not until 1985, when Van Eck published his work about compromising emanations of cathode ray tube (CRT) screens [3], in which Van Eck succeeded in reconstructing the image displayed on a CRT screen by using an antenna, amplitude demodulation (AM) receiver and a signal generator. This sparked the interest of other researchers, such as P. Smulders who published his work [11] on RS-232 cables and Kuhn [4] who extended the research to flat panel displays. Kuhn discovered that not only emanations originating from analog video signals could be reconstructed, but also from digital video signals more specifically from the low-voltage differential signaling (LVDS) cable or the front panel display link. This implied that not only analog data based systems, such as video graphics array (VGA) cables and CRT screens suffer from the eavesdropping threat, but also digital data based systems. Kuhn realized his experiment using a super-heterodyne receiver, a waveform generator and a directive antenna. Tanaka *et al.* [5] extended and reproduced Kuhn's work on liquid crystal displays (LCDs) using more or less the same instrumentation. They investigated the near- and far-field of the LCD emanations and also the coupling effect of the LCD onto the power cables. Tanaka *et al.* were able to reconstruct the display from the leaked emanations in the far-field up to a distance of 6 m. A couple of years later, Sekiguchi and Seto [6] made a more quantitative analysis of the emanations originating from a VDU using the same methods and instrumentation as

Manuscript received January 30, 2019; revised May 7, 2019; accepted May 31, 2019. This work was supported by the Belgian Ministry of Defence. *(Corresponding author: Pieterjan De Meulemeester.)*

P. De Meulemeester is with the Department of Communication, Information, Systems and Sensors, the Royal Military Academy, Brussels 1000, Belgium and also with the Department ESAT–Telecommunications and Microwaves, the Katholieke Universiteit Leuven, Leuven 3000, Belgium (e-mail: pieterjandemeulemeester@gmail.com).

B. Scheers is with the Department of Communication, Information, Systems and Sensors, the Royal Military Academy, Brussels 1000, Belgium (e-mail: bart.scheers@rma.ac.be).

G. A. Vandenbosch is with the Department ESAT–Telecommunications and Microwaves, the Katholieke Universiteit Leuven, Leuven 3000, Belgium (e-mail: guy.vandenbosch@kuleuven.be).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEMC.2019.2923026

previous works on this topic, however, the type of VDU was not mentioned. More recently, Lee *et al.* [7] proposed a method that recovers leaked video information from a distance of 10 m and includes a synchronization detection method. Independently from our work, they have also decided to use a software-defined radio (SDR) for data acquisition and signal processing.

In previous mentioned works, the tested VDUs are relatively outdated compared to today's VDU standards and some phenomenon or occurrences, such as multiple path signal distortion or the characterization of the multiple emanations sources are not sufficiently addressed or accentuated. The former observation regards the fact that the VDUs used today are more advanced in the sense that the resolution of the displays, or in other words the data bandwidth, has increased considerably. Furthermore, all VDUs now strictly apply the EMC standards. Many new video technologies have come to the forefront, such as LED TVs, 4K video resolution displays and DP/eDP (display port/embedded display port) cables [12]. In terms of information security, it is of utmost importance to determine each data leak. The ability to acquire and analyze the emanations of all leakage sources forms an effective tool to determine the level of data security in the terms of compromising emanations and EMC/EMI. Some of the different video processing stages inside a VDU utilize different synchronization frequencies that do not interfere in the far-field [13], [14] when leaked. This in turn increases the risk of video data transmissions being compromised. The ability to detect various leakage sources opens up the possibility to employ multiple-input multiple-output (MIMO) techniques that can exploit different leakage channels to reconstruct the target image.

This research paper proposes a method that captures and reconstructs the original video data from leaking emanations of multiple co-located identical VDUs that are displaying different video images while having no *a-priori* knowledge of the VDU's synchronization frequency and image's pixel resolution. The latter implies that the proposed method does not focus on synchronization standards, such as the VESA standards [15], but that it instead scans the frequency spectrum to detect carrier frequencies containing leaked processed video information and then extracts the synchronization information from one data capture tuned to one of these carrier frequencies. It also investigates the use of MIMO methods by deploying two directive antennas to increase the detected signal-to-noise ratio (SNR) and the quality of the reconstructed image. An SDR showed to be an effective tool to realize this, according to our previous research work [13] and the work of Lee *et al.* [7], whereby SDRs are used to reconstruct the original video data from leaking emanations. However, the proposed method in this paper significantly improves the SNR of the reconstructed images and effectively exploits the various leakage channels originating from a multitude of identical VDUs. In addition to that the feasibility and the scalability is inspected of a low-cost measurement system of a small form factor. The tested VDU type is a high definition format thin-film-transistor (TFT) LCD display, which is prominently present in most offices and households. The tests are done in a semi-anechoic chamber to emphasize the leakage response of multiple VDUs.

Section II describes the method of video leakage channel detection and video image reconstruction exploiting multiple leakage channels. Section III discusses and examines the results obtained by the proposed method for the different experimental setups. This section is structured as follows: Image reconstruction of one VDU is given in Section III-A. Additional technique exploiting the various leakage channels to increase image reconstruction quality has been elaborated in Section III-B. Image reconstruction of three identical active VDUs has been detailed in Section III-C. The consequences and implications of the results given in Section III-D and Section IV concludes the paper.

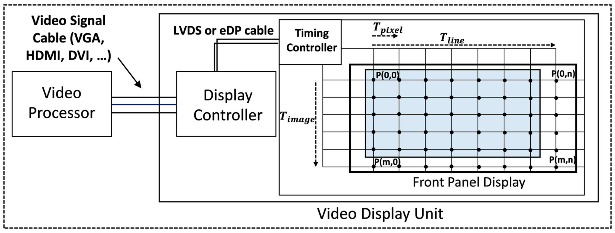


Fig. 1. Simplified architecture of the VDU system. The black dots located on the video raster of the front panel display represent all the pixels. The dots located inside the blue box are the visible pixels, the other located outside are the blanked pixels.

II. Method of Video Leakage Channel Detection and Video Image Reconstruction

A. Compromising Emanations of a VDU

To fully understand this emanations phenomenon of leaked video data, a general picture needs to be conceptualized of the possible leakage sources and the nature of the leaking emissions. The processed video signal is transmitted through many signaling interfaces before being displayed on the display itself as depicted in Fig. 1. These different transmission stages need to be considered when analyzing the leakage characteristics of the VDU because each stage has the potential to leak into the far-field and will have its own leakage characteristics [13], [14]. The video signal contains processed video data and video synchronization signals. This applies for all types of video signaling technologies ranging from analog VGA cables to digital Display Port cables [15], [16]. The video synchronization signals consist out of the time period of one image, one video line, and one video pixel, which will be represented in this paper as the image frequency, line frequency, and pixel frequency, respectively. Fig. 1 depicts a simplified VDU architecture containing the different video signal cables, signaling interfaces, and the timing periods of the video display. It should be noted that the video data signal consist out of visible and blanked pixels. These blanked pixels are not displayed on the front panel display, but contain zero-valued pixel information to introduce a time interval to refresh the data buffers.

The video data are transmitted serially over the video signal cable except for the data of the pixels color and the synchronization that are transmitted in parallel resulting in interference when leaked in the EM spectrum. The synchronization signals, especially the pixel frequency, play a significant role in understanding the data leakage mechanisms. The pixel frequency corresponds to the frequency of the clock signal inside the VDU that contains many high-frequency harmonics due to

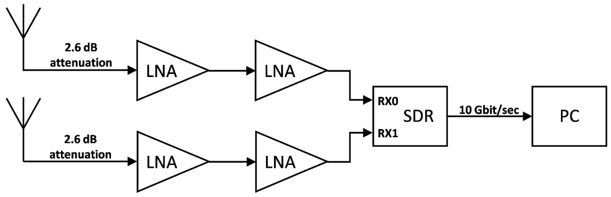


Fig. 2. Measurement signal chain.

the employed square wave signaling. The higher frequencies are more susceptible to leaking into the far-field and will act as a carrier frequency for processed data leaks [4], [13], [17], [18]. The processed video signal is induced on a multitude of carrier frequencies all correlated to the harmonics of clock/pixel frequency. The fortuitous emitters dimension will determine the emission efficiency of the compromising emanations. Accounting for the different signaling interfaces/stages [8], [14], [17] as displayed in Fig. 1, the fortuitous emitters dimension will change with respect to that. This will result in an EM frequency spectrum containing multiple compromising carrier frequencies determined by the harmonics of the pixel/clock frequency and the dimensions of the emitter. The leakage sources include the signal output port of the graphics processing unit (GPU), the video transmission cables (VGA, HDMI, digital video interface (DVI), Display port, etc) and the internal cables of the display (LVDS and embedded displayport (eDP)) [4], [6], [8], [16], [17], [19].

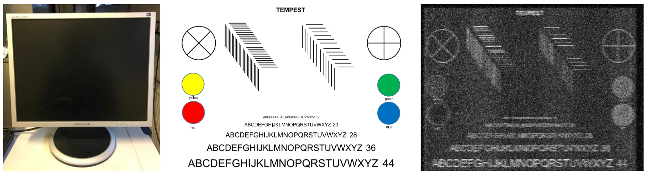
B. Measurement Setups

The goal of this research paper is to have both a quantitative understanding of this threat and a risk analysis of this method becoming conventional for data theft. To address the latter, the instrumentation consists out of two log-periodic dipole array antennas (LPDAs), low-noise amplifiers (LNAs) and an SDR linked to a personal computer. Opting for an SDR makes the measurement setup significantly more practical and feasible for eavesdropping, due to its small form factor and the image processing capabilities of a digital environment, compared to the used measurement setups in other research works concerning this side-channel attack [3]–[6], [20].

The LPDA antennas both cover a broad frequency range from 380 MHz to 8 GHz and have a directive gain of 45 dBi for frequencies up to 1 GHz. Each antenna is connected to an individual signal chain that consists out of two LNAs and a radio frequency (RF) front-end of the SDR as depicted in Fig. 2. The signal is sent to a an Ettus USRP ×310 that has two integrated RF front-ends covering a frequency range of direct current (DC) to 6 GHz, it has an RF bandwidth of 160 MHz and is able to sample the signal at 200 MSps. The SDR processes the signal and feeds the IQ samples into a computer using a high-speed Ethernet cable of 10 Gb/s. More specifications of the instrumentation are stated in Table I.

TABLE I
SPECIFICATIONS OF INSTRUMENTATION

Device	Product model	Specifications
LPDA	Aaronia Hyper-Log 3080x	• Frequency range: 380 MHz-8 GHz • Directive gain: 45 dBi (DC-1 GHz)
LNA	ZX60-P103LN+ (Mini-Circuits)	• Gain: 18 dB • Noise Figure: 0.5 dB
SDR	Ettus USRP x310	• 2 RX channels • RF front end range: DC to 6 GHz • RF front-end bandwidth: 160 MHz • Max. sampling rate: 200 Msps • Form factor: 27.7 cm x 21.8 cm x 3.9 cm


TEMPEST
ABCDEFGHIJKLMNOPQRSTUVWXYZ 20
ABCDEFGHIJKLMNOPQRSTUVWXYZ 28
ABCDEFGHIJKLMNOPQRSTUVWXYZ 36
ABCDEFGHIJKLMNOPQRSTUVWXYZ 44

(a) (b) (c)

Fig. 3. (a) VDU under test in previous work [13]. (b) Test image. (c) Image reconstruction of the leaking emanations originating from the VDU at a distance of 5 m.

In the measurement setups, a single type of VDU is used, which relies on TFT LCD technology and displays a high-definition image with a 1680×1050 pixel resolution. The video signal is generated by a Raspberry Pi model B rev. 2, which transmits it through a HDMI-to-DVI conversion cable and a DVI cable to the LCD display. Both the HDMI and the DVI cable have a ferrite bead in place that suppresses high-frequency noise to prevent EMI. In this paper, the measurement setups are deployed in a semi-anechoic chamber to emphasize the leakage response of the VDU. It has been confirmed in our previous and other works [7], [13], [21] that leaked emissions of electronic devices in realistic environments can be captured and compromise processed information. In our previous work [13], three different types of VDUs were placed in an uncontrolled environment with other electronic equipment present and were examined for their leakage response. Fig. 3 depicts the results of the image reconstruction method applied on one of the tested VDUs. The VDU displayed a test image with a pixel resolution of 800×600 and employed a VGA cable for video signaling. Regarding the influence of other emitting electronic devices on the captured emanations, it could be concluded that the emissions of electronic devices always occupied a specific band of the frequency spectrum. In contrast with leaking VDUs, which cover a very broad spectrum from 100 MHz to 1 GHz. Consequently, the probability that leaked emanations are situated in a relative quiet frequency band is significant. It should also be noted that the leaked emanations located at a frequency band occupied by a telecommunication systems become almost undetectable. Nevertheless, the occupation of these bands depends on the region where the measurements are conducted. Based on these conclusions, we opted to do the measurements inside an anechoic chamber making them independent from their environment, and thus enabling us to capture the full leakage response of the VDUs. This helps us to gain new insights in the video leaking phenomenon in a more quantitative manner.

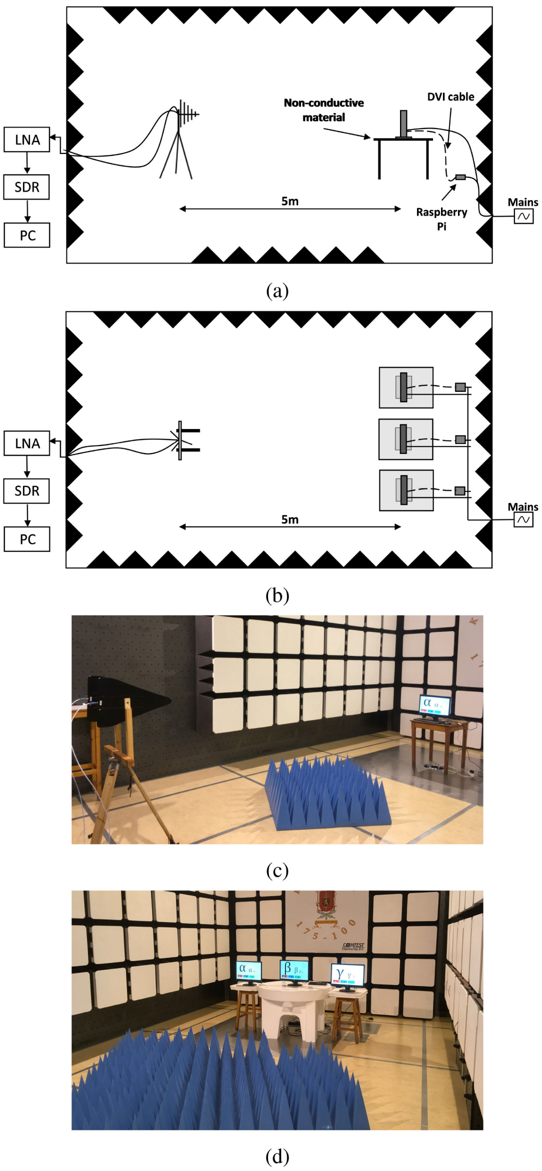


Fig. 4. (a) Side view of the first measurement setup of one VDU in the anechoic chamber. (b) Birdseye view of the second measurement setup examining three VDUs. (c) Picture of the first measurement setup. (d) Picture of second measurement setup.

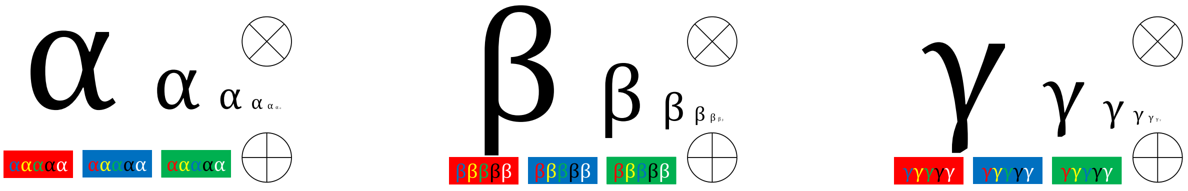
In Fig. 4 the first setup is depicted in which two vertically polarized antennas are placed 5 m from the target VDU on which a test image is displayed. The test image is shown in Fig. 5(a). Subsequently, the proposed image reconstruction method is applied to different detected video leakage channels originating from the VDU. The reconstructed images are thoroughly analyzed and discussed further in Section III. In addition to the image reconstruction, the radiation pattern and SNR are analyzed for each video leakage channel. The second setup is displayed in Fig. 4(b) in which the environment is kept constant aside from the placement of three identical target VDUs. The test images used are depicted in Fig. 5. This setup investigates the impact of the interference originating from the VDUs upon the reconstructed image's SNR. Hence, it examines the possibility to differentiate the leakage channels of one VDU from the other and its interference impact on the SNR of the detected leaking video signal. By displaying a different image on each VDU, it simultaneously helps confirming that the reconstructed image originates from one specific VDU and represents a realistic office situation. It has to be emphasized that this extension to multiple screens is of huge practical importance, since this is the situation widely seen in daily life. Also, this setup represents the worst-case scenario for an eavesdropper due to the fact that each VDU will emanates through the same leakage channels and will operate at the same synchronization frequencies, making it harder to differentiate the leaking emanations from each other due to the interference in the far-field.

C. *Method of Image Reconstruction*

First, the EM spectrum is acquired ranging from DC to 1 GHz by the SDR. Due to the periodic nature of the leaked video signal, averaging and correlation techniques become strong tools to determine which carrier frequency comprise leaked the video data. Therefore, multiple acquisitions are made to average out the received spectrum. The technique used to detect a carrier frequency containing the leaked video information exploits the fact that the image frequency or the refresh rate is a very distinctive frequency. Thus, if the synchronization retrieval method applied upon a specific carrier frequency results in an image frequency of 60 Hz, the probability is very high that it contains leaked video information. This video detection technique is applied to every detected peak in the frequency spectrum. It should be noted that the frequency, the intensity, and the bandwidth of the compromising data carrier is strongly influenced by the leaking mechanism as discussed previously. When selecting a carrier frequency containing potentially leaked video data, the bandwidth of the SDR needs to be carefully considered. Having a too low of a bandwidth, the quality of the reconstructed image will be significantly reduced. A too high of a bandwidth can result in a high intake of noise due to frequency overlap of other occupied frequency bands. The bandwidth is limited by the RF front-end and the sample rate of the analog-to-digital converter (ADC).

When the detected carrier frequency and a well-considered bandwidth is selected, one data acquisition is made for every leakage channel. The acquired sampled data are AM-demodulated before video synchronization methods are applied. The demodulation is based on a digital envelope detection. The video leakage mechanisms inside the VDU are determined by the sharp rises and falls of the differential changes in the transmitted video signal [4], [17], [19]. These sharp rises and falls contain many high frequencies and are intensely emitted into the far-field. Hence, the detected leaked video emissions contain the information of the change in amplitude of the video signal. Therefore, the leaked signal will have amplitude modulated properties. The analysis of the exact mechanisms is out of scope for this research paper and will be investigated in future research. It should be noted that the leaking emanations of some signaling cables have been examined in more details in the works of Kuhn [4], [8], Song *et al.* [19], and Zhang *et al.* [17].

The envelope detection is a crucial step in demodulating the leaked video signal, therefore, several digital envelope



(a) (b) (c)

Fig. 5. Video test images. (a) Test image for the setup of one VDU. (a), (b), and (c) Test images used for the setup with three VDUs.

detection techniques were investigated, i.e. synchronous and asynchronous detection, full-wave and half-wave detection, and real and complex detection [22]. Due to inevitable distorted clock oscillation of the leaked signal synchronous detection would to be difficult to apply, hence asynchronous detection proved to be more stable and more feasible. Real and half-wave detection could be opted for if computational resources are strained and if performance is not crucial. Different tests showed that an asynchronous complex square-law envelope detection had the best performance and that by omitting the low-pass filter the computation resources could be kept at a reasonable level.

Video synchronization retrieval methods are applied after the envelope detection. The synchronization depends on three frequencies, more specifically the image, the line, and the pixel frequency. To reconstruct the video image, these frequencies need to be exactly determined in accordance with the leaked video signal. A VDU can emanate many leaked video signals and each leaked channel will have its own specific synchronization frequencies [13]. The synchronization frequencies are obtained using autocorrelation techniques that are based upon the Wiener–Khintchine theorem [23]. The theorem can only be applied if a wide-sense stationary signal can be assumed, which is the case due to the periodic nature of the leaked emanations. Due to the signal sampling of the SDR, the autocorrelation equation is applied in the discrete time domain.

To filter out each specific synchronization frequency, the autocorrelation method is applied to specific frequency scopes corresponding to the synchronization needed. For instance, the pixel frequency is in the order of megahertz, the line frequency in the order of kilohertz and the image frequency in the order of hertz. Due to the periodic nature of the video signal, the output of the autocorrelation is averaged out to obtain a higher SNR. The pixel frequency can be extracted from the carrier frequency as discussed in Section II-A or it can be deduced from the line frequency as explained next. Consequently, the line and image frequency do need to be extracted precisely. The synchronization frequencies or the synchronization time periods (e.g. $T_{\text{line}} = {}^{1}/_{f_{\text{line}}}$) have the following relationship with the number of horizontal $n_{\text{horizontal}}$ and vertical n_{vertical} pixels:

$$T_{\text{line}} = T_{\text{pixel}} \cdot n_{\text{horizontal}} \tag{1}$$

$$T_{\text{image}} = T_{\text{line}} \cdot n_{\text{vertical}}. \tag{2}$$

The frequencies are presented in terms of time periods, because it states more clearly that the line and image time period govern the synchronization of the image. The other parameters can be arbitrarily chosen if the above relations hold true. In practice, the T_{image} and T_{line} are determined by the synchronization retrieval method and $n_{\text{horizontal}}$ is set to 2000. Consequently, T_{pixel} and n_{vertical} can be deduced.

In the final processing stage, the data stream is resampled to the retrieved pixel frequency. The resampling stage forms a crucial step in the reconstruction method because it needs high precision and flexibility. The resampling algorithm applied enables precision of one-tenth of hertz and has a fast response time. In practice, the former is definitely needed to prevent frame drift. The resulting data stream after resampling is then displayed using the determined $n_{\text{horizontal}}$ and n_{vertical}. However, due to the arbitrary chosen $n_{\text{horizontal}}$, the aspect ratio of the reconstructed image will slightly differ from the original. To effectively improve the SNR of the reconstructed image, moving average techniques are applied. If memory resources are constrained, a single pole infinite impulse response filter can be applied, which alleviates memory constraints due to the fact that only one image needs to be buffered. The length of the moving average (MA) corresponds to the number of images. When averaging, a compromise needs to be made between the time resolution of the image and the SNR of the image. In practice, the effective MA length ranges from 25 to 200. Most of the VDUs operate at an image frequency or refresh rate of 60 Hz, therefore, having a MA length of 200 will result in an update time of ca. 3 s. If the MA length is short, the image can be reconstructed in real-time, otherwise it needs to be processed offline.

The SNR can also be improved by adding a second antenna to the measurement setup as described in Section II-C. In theory, an additional antenna will provide a 3 dB SNR improvement. This increase in SNR is also confirmed in the measurements. However, adding antennas to the measurement system introduces some more complexity, such as synchronizing the two signal channels. Nonetheless, the advantages outweigh the disadvantages. The antennas are deployed as a phased-array, whereby the distance between the antennas is 25 cm. A phased-array makes beamforming possible and also allows for usage of a technique based on spatial multiplexing. It addresses the fact that each antenna can acquire separate data leakage channels carried on different frequencies. This method is tested and discussed further in Section III-B.

III. Results

In this section, the results of the different setups are discussed. First the compromising emanations of one VDU are thoroughly

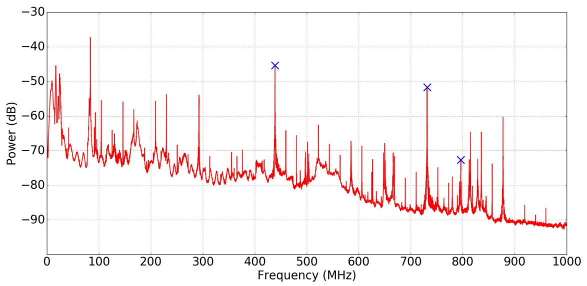


Fig. 6. RF spectrum covering 0–1 GHz of one VDU placed in a noiseless environment. Cross marks indicate the leakage channels with the highest SNR containing compromised video data.

TABLE II
SNR OF THE DETECTED LEAKAGE CHANNELS ORIGINATING FROM ONE VDU

Center frequency	One amplification stage	Two amplification stages
440 MHz	0.2 dB	22.2 dB
730 MHz	5.5 dB	24.4 dB
795 MHz	0 dB	10.5 dB

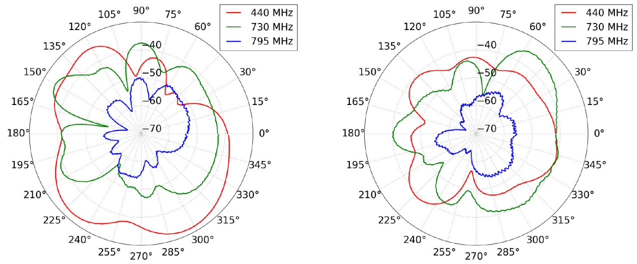
examined as depicted in Fig. 4(a) and analyzed by applying the proposed image reconstruction method and by determining the radiation pattern and the SNR of the detected signal. An additional technique is proposed to increase the image reconstruction quality by exploiting the various leakage channels of the VDU. The second setup in Fig. 4(b) examines the effect of three co-located active identical VDUs on the leakage spectrum. The proposed reconstruction method is again tested to see whether each VDU's leakage channel can be individually detected and its video data content can be reconstructed. Also, the effect of the multiple active VDUs on the SNR of the detected signal is examined.

A. Image Reconstruction of One VDU

The measurement system, discussed in Section II-C, is deployed to apply the video leakage detection and reconstruction methods on the test setup depicted in Fig. 4(a). The result of EM spectrum acquisition from DC to 1 GHz is displayed in Fig. 6. The spectrum acquisition contained three leakage channels at 440, 730, and 795 MHz and is plotted in Fig. 6. It should be taken into account that the acquisition contains some non-linear amplification due to the double amplification that results in some distorted frequency bands and in an increase of noise. The SNRs of the detected leakage channels for the acquisitions are stated in Table II. The SNRs are calculated with a bandwidth resolution of 5 MHz and by averaging the detected signal and noise. The bandwidth resolution of 5 MHz is the absolute minimal bandwidth needed to determine if the carrier frequency holds any leaked video data.

The radiation pattern of the VDU, relative to the above mentioned leakage channels, is investigated for a horizontal and vertical polarization. The antennas are placed 5 m from the VDU, one vertically polarized and the other horizontally. The averaged radiation pattern is acquired for a 360° angle at a center frequency of 440, 730, and 795 MHz with a bandwidth resolution of 5 MHz. The radiation pattern is displayed in Fig. 7 for both polarizations. The vertically and horizontally polarized radiation have overall the same radiation strength, but the vertically polarized radiation results in a more omnidirectional pattern. It is decided to polarize the antennas vertically for all the tests throughout this paper because of the more omnidirectional radiation pattern and for practical reasons.

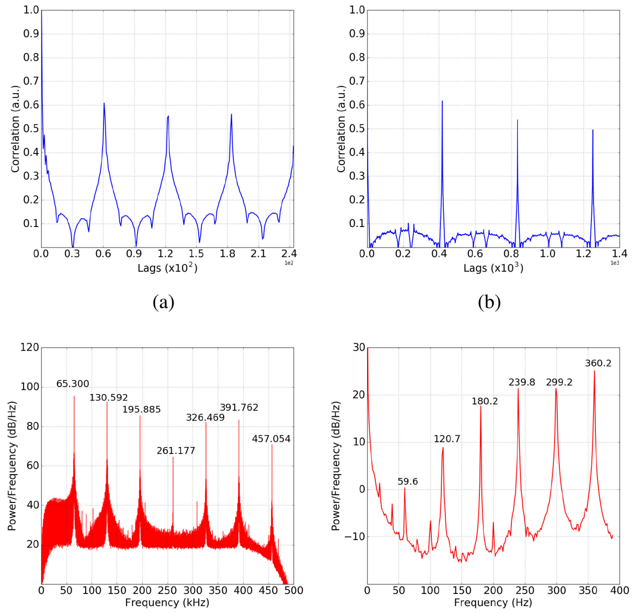
After the video leakage channels are determined by the previous leakage channel detection step. One acquisition is made for each leakage channel. The synchronization retrieval method is applied on each leakage channel of center frequencies 440, 730, and 795 MHz. The results of the synchronization retrieval method for the line frequencies and image frequencies for the carrier frequency 730 MHz are depicted in Fig. 8 as correlograms



(a)

(b)

Fig. 7. Averaged radiation pattern of one VDU as a function of magnitude [dB] at carrier frequencies 440, 730, and 795 MHz. (a) Horizontal polarization. (b) Vertical polarization.

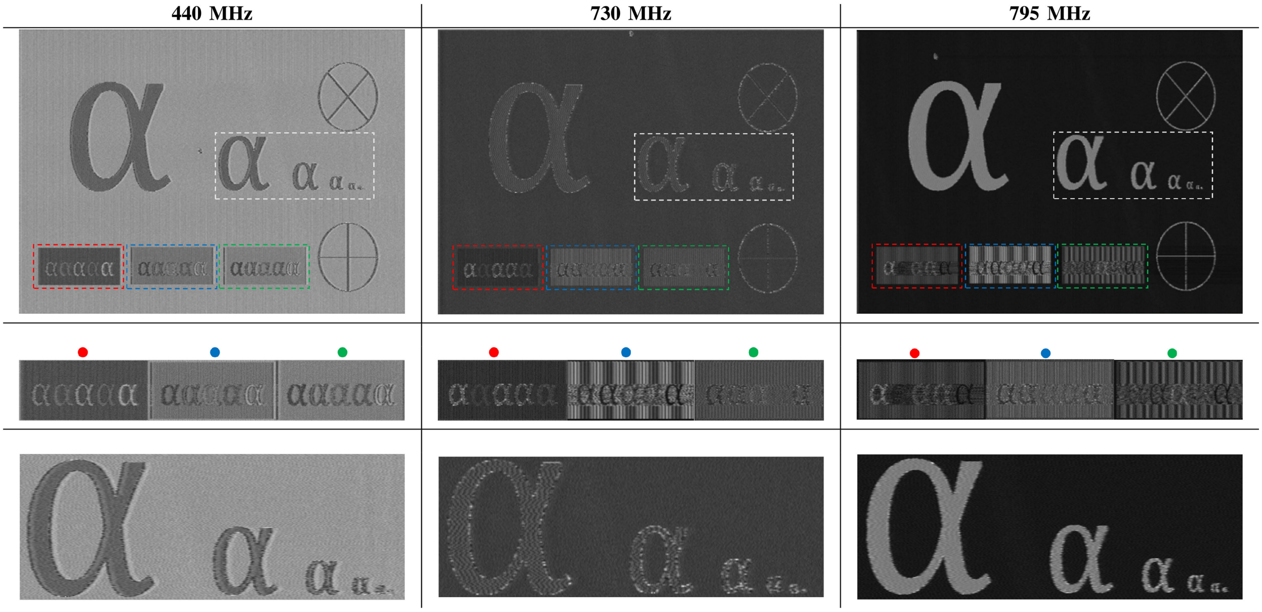


(c)

(d)

Fig. 8. PSD plots and correlograms of the emanations from one VDU tuned to the center frequency of 730 MHz. (a) Correlogram of the line frequency at a sample rate of 4 Msps. (b) Correlogram of the image frequency at a sample rate of 25 kSps. (c) PSD plot of the line frequency. (d) PSD plot of the image frequency.

TABLE III
IMAGES RECONSTRUCTED AT CARRIER FREQUENCIES 440, 730, AND 795 MHZ



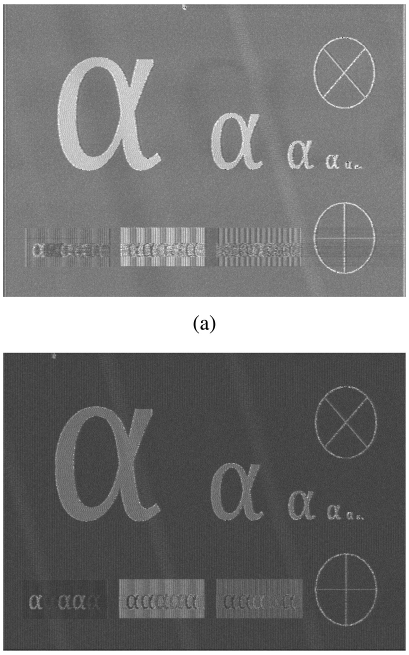
The first row displays the full reconstructed images. The second and third row depict enlarged parts of the reconstructed images. More specifically the areas defined by the dashed rectangles with the corresponding colors of the original backgrounds. Moving average lengths of 50, 25, and 25 are applied, respectively, to the images reconstructed from the three carrier frequencies.

and power spectral density plots. The line and image frequency are clearly represented in the plots and have a distinctive pattern, such as the harmonics at specific frequencies that facilitate the detection of a leaking video data channels. The pixel frequency is indirectly determined as explained in Section II-C by using (1) and (2). After determining the synchronization frequencies and the image's resolution according to the synchronization relations, the image is reconstructed after resampling the data stream corresponding to the recovered pixel frequency and setting the correct number of pixels in the horizontal and vertical direction of the image. Subsequently when perfect synchronization is achieved, moving average techniques are applied to increase the SNR of the reconstructed image. The same method is analogously applied for the other two leakage channels and their resulting reconstructed image are displayed in Table III.

The first observation when analyzing the reconstructed images is that the leaked data induced on each carrier frequency do not result in identical images. For instance, the color information that is translated into grayscale values during the emanation process is notably different between the leakage channels. Enlarged parts of the reconstructed images in Table III help to give a clearer visualization of the differences and similarities. The grayscale values of the reconstructed image obtained from the 795 MHz channel seem to be inverted compared to the image obtained from the 440 MHz channel. The 795 MHz channel's image also suffers more from pixel "trailing" than the 440 MHz channel's image. This is clearly seen in the enlarged images of the small alphas with their corresponding colored background indicated by the dot. Furthermore, the colored backgrounds of the 730 and 795 MHz channels also have a considerable ripple in their grayscale value. This effect is less pronounced for the 440 MHz channel. However, the image reconstructed from the 795 MHz channel has the highest SNR, and therefore, the sharpest images compared to the others. These indications reveal that each leakage channel is probably generated by a different source or leakage mechanisms.

B. Additional Technique Exploiting the Various Leakage Channels to Increase Image Reconstruction Quality

Due to the multiple video data leakage channels, a MIMO technique involving spatial multiplexing can be employed to improve the quality of the reconstructed image. According to previous observations, each video data leakage channel results in its own distinctive reconstructed image. Therefore, it would be interesting to combine these channels to optimize the reconstructed image. For instance, the leaked data induced on the 440 MHz carrier frequency suffers less from pixel "trailing" as discussed previously than the leaked data induced on the 795 MHz carrier frequency. However, the reconstructed images based on the 795 MHz channel are noticeably sharper in detail. By capturing a different leakage channel for each antenna and applying the image reconstruction for each channel individually and combining them at the end, the quality of the reconstructed image can be improved due to a higher leaked information throughput. This technique is closely related to MIMO techniques involving spatial multiplexing, but in this case the channels are carried on different carrier frequencies instead of one [24]. In Fig. 9 the image is reconstructed combining the induced leaked data on carrier frequencies 440 and 795 MHz and for the carrier frequencies 730 and 795 MHz. The same image reconstruction method is applied as in previous sections. Fig. 9(a) shows that by combining the channels of 440 and 795 MHz the color properties specifically have changed in respect to the



(a)

(b)

Fig. 9. Reconstructed images using a spatial multiplexing technique. For both images a moving average length of 25 is applied. (a) Frequency channels 440 MHz and 795 MHz. (b) Frequency channels 730 MHz and 795 MHz.

reconstructed images in Table III. However, the ripple effect inherent to the 795 MHz leakage channel is still very present. This is not the case for the resulting image when combining the channels of 730 and 795 MHz Fig. 9(b). The combination of these two channels does show an improvement with respect to the individual channels. The smaller alpha letters are more distinguishable from each other and the "trailing" and ripple effect discussed in previous results is mitigated.

C. Image Reconstruction of Three Identical Active VDUs

The next test investigates whether the video images can still be reconstructed if other identical VDUs are active in the near vicinity. The exact setup is depicted in Fig. 4(b), whereby each VDU displays a different test image as depicted in Fig. 5. The RF spectrum is again scanned for compromising emanations at specific carrier frequencies. As expected, the same carrier frequencies containing leaking video data are detected. Tuning to the center frequency of 795 MHz, the image reconstruction results in Fig. 10. It is seen that the VDUs clearly interfere with each other's leakage channels. However, it is discovered that each VDU has a small offset Δf_{pixel} in pixel frequency. This offset ranges from 1 to 100 Hz. By averaging out the reconstructed image to its exact f_{pixel}, each individual VDU can be separated from each other as seen in Fig. 11. This shows that even though the received leaked signal contains many other RF signals on approximately the same carrier frequency, one can lock onto one channel by exploiting the periodicity of the video signal. For the other leakage channels the same method can be applied to obtain the same results aside from the different color pattern and image distortion inherent to the leakage channel as discussed in Section III-A.

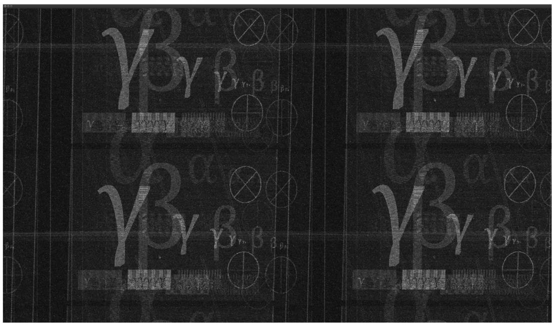


Fig. 10. Image reconstruction of the leakage channel at 795 MHz.

TABLE IV
SNR MEASUREMENTS OF THE DETECTED COMPROMISING VIDEO EMANATIONS ORIGINATING FOR TESTED SETUPS OF ONE VDU AND THREE VDUS

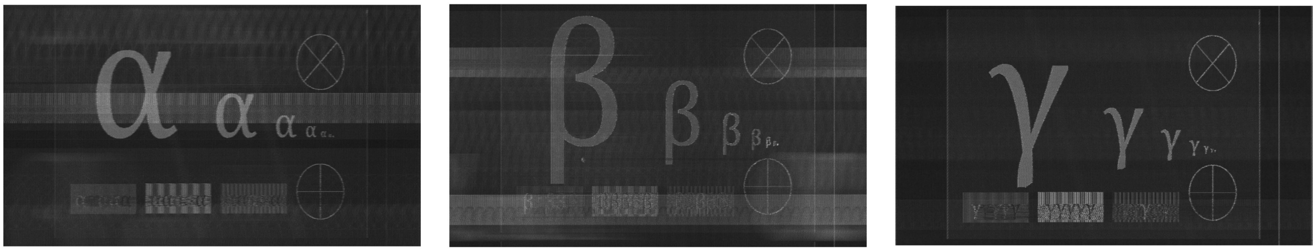
Center Frequency	One VDU Setup	Three VDU Setup
440 MHz	22.2 dB	18.0 dB
730 MHz	24.4 dB	21.9 dB
795 MHz	10.5 dB	10.0 dB

For both measurement, the two LNA stages are used.

The cause of this frequency offset is the small variation in the quartz crystal oscillation that generates the clock frequency. The crystal is susceptible to small temperature differences and small physical property differences compared to other crystals [25]. Also during the tests, it is revealed that these oscillations change in time due to the increasing temperature of the turned ON VDUs. Therefore, the synchronization frequencies need to be constantly updated. The SNR measurements are done for this setup and are compared with the SNR measurements for one VDU as shown in Table IV. The SNR measurements are performed with a resolution bandwidth of 5 MHz and with two amplification stages. The measurements indicate that the global SNR for the three VDU setup has decreased. In general, one can conclude that constructive and destructive interference of the various emanations originating from the VDUs have a relative small effect on the SNR.

D. Consequences and Implications of the Results

The results of the different examined setups reveal that the video eavesdropping risk of modern day video equipment is existent. Due to the small form factor of the used instrumentation, the relative low-cost and the effectiveness, the proposed system can be deployed in many different environments. This can act as an opportunistic incentive to deploy such a system for people who are interested in data theft. Also, it has to be taken into account that the effective SNR of the reconstructed image can be improved by employing more than two antennas in a phased-array constellation with beamforming or spatial multiplexing capabilities. Besides improvement on hardware level, various signal processing techniques can also realize improvements in the reconstruction quality. For instance, letter recognitions



(a) (b) (c)

Fig. 11. Image reconstructed using the leakage channel at 795 MHz and with an applied moving average length of 50. (a) Image reconstruction of the test display α by locking onto its exact pixel frequency of 65 292 283 Hz. (b) Image reconstruction of the test display β with a pixel frequency of 65 292 283 Hz + Δf_{pixel}. (c) Image reconstruction of the test display γ with a pixel frequency of 65 292 283 Hz + Δf_{pixel}.

algorithms as proposed in [26] can be applied to enhance the reconstruction of leaked video signals containing text.

Other works that investigate methods to reduce the eavesdropping risk propose active jamming techniques. The method proposed in [27] is based on jamming the leaked video emanations by generating a strong RF signal that is synchronized to the leaked video signal. It proofs to be effective against averaging techniques, however, it should take into account multiple signal processing stages that might employ other synchronization frequencies [13], [14] to be fully effective.

IV. Conclusion

The proposed image reconstruction method demonstrated that even for weak emanating high definition VDUs, the video leakage channels can be detected and the original video data can be reconstructed resulting into a readable video image. The proposed method was able to obtain the exact synchronization frequencies and the image resolution of the leaked video data without any foreknowledge of the system. The addition of a second LPDA antenna results in an increase of the SNR and enables a new method based on a MIMO technique that exploits the different leakage channels. Subsequently, the image reconstruction method was tested in an environment having multiple active identical VDUs, which revealed that it is possible to reconstruct the leaked video data of each VDU individually. For all tests, SNR measurements were performed to act as reference to other leaking VDUs and the radiation patterns of the VDU are determined. The feasibility and the practicality aspects of the measurement technique are fully taken into account. The measurement system has a small form factor and low-cost that is made possible by the utilization of an SDR and two directive antennas.

Acknowledgment

The authors would like to thank Luc Bontemps for making this research possible and for his good advice.

References

[1] P. Rohatgi, "Side-channel attacks side-channel attacks," in *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*, vol. 3, Hoboken, NJ, USA: Wiley, 2006, p. 241.

[2] R. Frankland and A. Offences, "Side channels, compromising emanations and surveillance: Current and future technologies," *Dept. Math., Roy. Holloway, Univ. London, Egham*, U.K., Tech. Rep. RHUL-MA-2011-07, 2011.

[3] W. van Eck, "Electromagnetic Radiation from video display units: An eavesdropping risk?" *Comput. Security*, vol. 4, no. 4, pp. 269–286, Dec. 1985. [Online]. Available: http://dx.doi.org/10.1016/0167-4048(85)90046-X

[4] M. G. Kuhn, "Compromising emanations: Eavesdropping risks of computer displays," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep. 577, 2003.

[5] H. Tanaka, O. Takizawa, and A. Yamamura, "A trial of the interception of display image using emanation of electromagnetic wave," *J. Nat. Inst. Inf. Commun. Technol.*, vol. 52, no. 1/2, pp. 213–223, 2005.

[6] H. Sekiguchi and S. Seto, "Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer," in *Proc. IEEE Instrum. Meas. Technol. Conf.*, 2008, pp. 1859–1863.

[7] H. S. Lee, D. H. Choi, K. Sim, and J. Yook, "Information recovery using electromagnetic emanations from display devices under realistic environment," *IEEE Trans. Electromagn. Compat.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8423652

[8] M. G. Kuhn, "Compromising emanations of LCD TV sets," *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 3, pp. 564–570, Jun. 2013.

[9] I. S. C. O. R. Interference, *Electromagnetic Compatibility of Multimedia Equipment–Emission Requirements*, CISPR 32:2015, 2015.

[10] "NACSIM 5000 TEMPEST fundamentals," National Security Agency, Fort Meade, MD, USA, 1982.

[11] P. Smulders, "The threat of information theft by reception of electromagnetic radiation from RS-232 cables," *Comput. Security*, vol. 9, no. 1, pp. 53–58, Feb. 1990. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/016740489090157O

[12] VESA, "VESA publishes embedded displayport (eDP) standard version 1.4a," 2015. [Online]. Available: https://www.vesa.org/news/vesa-publishes-embedded-displayport-edp-standard-version-1-4a/

[13] P. De Meulemeester, L. Bontemps, B. Scheers, and G. A. Vandenbosch, "Synchronization retrieval and image reconstruction of a video display unit exploiting its compromising emanations," in *Proc. IEEE Int. Conf. Mil. Commun. Inf. Syst.*, 2018, pp. 1–7.

[14] J. Shi, A. Yongacoglu, D. Sun, M. Zhang, and D. Wei, "Computer LCD recognition based on the compromising emanations in cyclic frequency domain," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 2016, pp. 164–169.

[15] Video Electronics Standards Association (VESA), "VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1, Revision 11," Video Electron. Standards Assoc., Milpitas, CA, USA, Tech. Rep., 2007.

[16] VESA, "VESA Issues Updated Embedded DisplayPort (eDP) Standard Version 1.3," 2011. [Online]. Available: https://www.vesa.org/news/vesa-issues-updated-embedded-displayport-edp- standard-version-1-3/

[17] N. Zhang, Y. Lu, Q. Cui, and Y. Wang, "Investigation of unintentional video emanations from a VGA connector in the desktop computers," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 6, pp. 1826–1834, Dec. 2017.

[18] M. Prvulovic, A. Zajic, R. L. Callan, and C. J. Wang, "A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 1, pp. 34–42, Feb. 2017.

[19] T. Song, Y. Jeong, and J. Yook, "Modeling of leaked digital video signal and information recovery rate as a function of SNR," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 2, pp. 164–172, Apr. 2015.

[20] C. Ula, U. Ak, and C. Karadeniz, "Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines," *Comput. Security*, vol. 58, pp. 250–267, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300049

[21] P. Juyal, S. Adibelli, N. Sehatbakhsh, and A. Zajic, "A directive antenna based on conducting disks for detecting unintentional em emissions at large distances," *IEEE Trans. Antennas Propag.*, vol. 66, no. 12, pp. 6751–6761, Dec. 2018.

[22] S. A. Tretter, *Communication System Design Using DSP Algorithms: With Laboratory Experiments for the TMS320C6713TM DSK*. Berlin, Germany: Springer, 2008.

[23] N. Wiener, "Generalized harmonic analysis," *Acta Math.*, vol. 55, pp. 117–258, 1930. [Online]. Available: https://doi.org/10.1007/BF02546511

[24] T. Paulraj and A. Kailath, "Increasing capacity in wireless broadcast systems using distributed transmission/directional reception (DTDR)," U.S. Patent 5 345 599, 1993.

[25] J. R. Vig, *Introduction to Quartz Frequency Standards*. Electron. Power Sources Directorate, Army Res. Lab., Fort Monmouth, NJ, USA, 1992. [Online]. Available: http://www.oscilent.com/esupport/TechSupport/ReviewPapers/Intro Quartz/vigtoc.htm

[26] Z. Hongxin, H. Yuewang, W. Jianxin, L. Yinghua, and Z. Jinling, "Recognition of electro-magnetic leakage information from computer radiation with SVM," *Comput. Security*, vol. 28, no. 1, pp. 72–76, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740480800093X

[27] Y. Suzuki and Y. Akiyama, "Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 2010, vol. 768, pp. 132–137.

Pieterjan De Meulemeester received the B.S. degree in electrical and electronic engineering sciences from the Katholieke Universiteit Leuven, Leuven, Belgium in 2014 and the M.S. degree in Nanoscience, Nanotechnology and Nanoengineering from the Katholieke Universiteit Leuven, Leuven, Belgium in 2016. He has done the M.S. thesis in close collaboration with Interuniversitair Micro-Elektronica Centrum, Leuven, Belgium, in 2016. He is currently working toward the Ph.D. degree in electrical and electronic engineering with the Royal Military Academy, Belgium and the Katholieke Universiteit Leuven.

His main interests include EMI/EMC phenomena, TEMPEST, information emission security, and computational electromagnetics.

Bart Scheers was born in Rumst, Belgium, in November 1966. He received the M.S. degree in engineering, with a specialisation in communication from the Royal Military Academy, Brussels, Belgium in 1991 and a joint Ph.D. degree in 2001 from the Université catholique de Louvain, Ottignies-Louvain-la-Neuve, Belgium/Royal Military Academy, where he presented his Ph.D. dissertation on the use of ground penetrating radars in the field of humanitarian demining.

After his studies, he was an Officer in a territorial signal unit of the Belgian Army. In 1994, he was an Assistant in the field of signal processing with the Royal Military Academy, where since 2003, he has been a Military Professor with the Communications Information Systems and Sensors (CISS) department, and is also the Director of the research unit on radio networks. His current domains of interest are mobile ad hoc networks (layers 2 and 3), cognitive radio, and internet of things.

Guy A. E. Vandenbosch (M'92–SM'08–F'13) received the M.S. and Ph.D. degrees in electrical engineering in 1985 and 1991, respectively, from the Katholieke Universiteit Leuven, Leuven, Belgium, where he held as a postdoctoral researcher, from 1991 to 1993.

Since 1993, he has been a Lecturer, and since 2005, a full Professor with the Katholieke Universiteit Leuven. He teaches courses on electromagnetic waves, antennas, electromagnetic compatibility, electrical engineering, electronics, and electrical energy, and digital steer- and measuring techniques in physics. From September to December 2014, he was a Visiting Professor with Tsinghua University, Beijing, China. His research interests include electromagnetic theory, computational electromagnetics, planar antennas and circuits, nano-electromagnetics, EM radiation, EMC, and bio-electromagnetics. He has authored/ co-authored in more than 310 papers in international journals and has led to ca. 375 papers at international conferences.

Dr. Guy Vandenbosch has been a member of the management committees of the Consecutive European COST Actions on Antennas since 1993. Within the ACE Network of Excellence of the EU (2004–2007), he was a member of the Executive Board and coordinated the activity on the creation of a European antenna software platform. He currently leads the EuRAAP Working Group on Software and represents this group within the EuRAAP Delegate Assembly. From 2001 to 2007, he was the President of Systems International TELemarketing, the Belgian Society of Engineers in Telecommunication and Electronics. From 2008 to 2014, he was a member of the board of the Federation des Ingenieurs des Telecommunications de la Communaute Europeenne, Belgium, the Belgian branch of the Federation of Telecommunications Engineers of the European Union. During 1999–2004, he was a Vice-Chairman, during 2005–2009 was a secretary, and from 2010 to 2017 was the Chairman of the IEEE Benelux Chapter on Antennas en Propagation. During 2002–2004 he was the Secretary of the IEEE Benelux Chapter on EMC. From 2012–2014, he was the Secretary of the Belgian National Committee for Radio-electricity (URSI), where he is also in charge of commission E.