Reconstruction of Video Information Through Leakaged Electromagnetic Waves from Two VDUs Using a Narrow Band-Pass Filter

DONG-HOON CHOI1, (Student Member, IEEE), EUIBUM LEE1, (Student Member, IEEE), AND JONG-GWAN YOOK.1, (Senior Member, IEEE)

1Dept. Electrical and Electronic Engineering, Yonsei University, Seoul, Republic of Korea (e-mail: cdhemail@yonsei.ac.kr)

Corresponding author: Jong-Gwan Yook (e-mail: jgyook@yonsei.ac.kr).

ABSTRACT This paper proposes a method to reconstruct an original video display from electromagnetic leakage by using the characteristics of digital video interfaces (e.g., digital visual interface (DVI) and high-definition multimedia interface (HDMI)). Moreover, it is proven that the analysis is applicable through a very narrow multiband pass filter when multiple video display units (VDUs) with identical video properties (resolution, refresh rate, etc.) are placed together and emanate simultaneously. The proposed method is verified with our reconstruction system and is expected to contribute to improving the security of video display signals by raising awareness regarding information leakage risks.

INDEX TERMS TEMPEST, LCD monitor, information leakage, electromagnetic interference (EMI), compromising emanations

I. INTRODUCTION

Modern electronic information devices employ high-speed circuits and systems for rapid signal processing. Such development inevitably results in electromagnetic interference (EMI) and electromagnetic compatibility (EMC) problems, causing issues related to information leakage via compromising emanations [1]. A video display unit (VDU), which is convenient and irreplaceable, is also affected by this vulnerability, and visual information may no longer be the most secure data presentation method. Research on information leakage via compromising emanations, such as Van Eck’s phreaking, has been carried out steadily since the 1980s to the present when most electronic devices use a liquid crystal display (LCD) VDU presenting visual information [2]. However, numerous previous reports have only described the process of acquiring compromising emanations and the reconstruction method, while the signal characteristics of the DUT source operating as an EMI source have not yet been analyzed.

Therefore, this paper presents the acquisition process of compromising emanations from the target LCD VDUs and reconstruction of the information. In addition, the signal characteristics of the compromising emanation are analyzed, and the information reconstruction algorithm used in the measurement system is described in detail.

The compromising emanation sources that generate an EMI field in an LCD VDU can be classified into two types. One is the low-voltage differential signal lines inside the VDU that includes signal flow from the A/D converter and timing controller. The other is an external interconnection between the VDU and video graphic arrays (VGA). Among the two source types, the external interconnection is electrically more extensive, and thus more prone to emitting electromagnetic waves that carry display information. Furthermore, there are distinct advantages in using the digital clock because it is more consistent than other signals, such as the Video Electronics Standards Association (VESA) standard.

Typical video interfaces constituting external interconnections include a VGA connector using an analog modulation method, digital visual interface (DVI), as well as high-definition multimedia interface (HDMI) using digital modulation methods. Recently, as the resolution of VDUs has been developed to high definition or higher, it requires a significant amount of data, and the digital modulation method is more applicable. Furthermore, among the various video interfaces adopting the digital modulation method, the HDMI
interface is the most popular because of its higher stability, lower power consumption, and higher electromagnetic compatibility compared to the DVI.

Therefore, developing a technique to acquire compromising emanations from the HDMI signal is more realistic and useful. Specifically, there are several studies related to compromising emanations from the HDMI cable applied to various targets, such as the TEMPEST to computer VDUs [3-7], keyboards [8,9], embedded displays on printers [10,11], and beam projectors [12]. Most previous studies assume an isolated target VDU, meaning that there is only one such device in space.

However, in a realistic environment, there are likely to be multiple VDUs in the same place, simultaneously emitting their respective display information. This causes severe problems in the autocorrelation procedure, which is the most essential process in the frame-averaging method used to enhance the signal-to-noise ratio (SNR) of the compromising emanations. As a result, accurate and precise pixel-rate extraction for the frame average becomes impossible.

In view of these bottlenecks under realistic situations, a quantitative analysis of multiple VDUs is presented in this paper for multiple VDU environments. A previous study attempted to distinguish a certain VDU among three targets placed in the same space displaying the respective information [13]. However, the study does not present any quantitative analysis for obtaining a pixel rate for accurate frame averaging and only mentions the possibility of distinction.

Therefore, this paper introduces a novel method to distinguish the target VDU quantitatively based on the heuristic analysis of video interfaces that are coercively operated on compromising emanation sources. The two fundamental ideas in our method involve distinguishing the number of displays using their respective characteristics, and the design of an adequate filter to extract the pixel rate of a target display from its display information.

For verification, a TEMPEST system was implemented with an RF front-end that covers the L-band (390 MHz – 1.55 GHz) with a software-defined radio (USRP-2940R). The experiments were conducted on two identical LCD VDUs that simultaneously display different types of information, such as still as well as moving picture frames. This paper is organized as follows: Section II analyzes the VDU to understand how the electronic signal is generated as a pixel. Hence, in this subsection, we decompose the TMDS encoding algorithm used in HDMI to analyze how the electronic signal is generated as a pixel value. The pixel consists of three color elements: red, green, and blue (RGB) values, which are processed and transmitted to the VDU in parallel through the HDMI. The different bitstream combinations depend on the RGB values of each pixel, but this study only considers the generation of a digital bitstream of white and black pixels that are commonly used in a document. Accordingly, it can be assumed that each color value was the same in this analysis. Most display interfaces express each color element in an 8-bit format with a range of 0-255. However, in general, for efficient color space usage, a limited range of color elements from 16 to 235 in the decimal is utilized [13,14,15]: accordingly, the black digital bitstream value is 16, while the value of the white pixel is 235 in decimal. In TMDS encoding, bit conversion is performed to minimize the transition in the bitstream using XNOR (exclusive, not OR gate) or XOR (exclusive OR gate) operations. Furthermore, two additional parity bits were added for error correction. The entire process is shown in Fig. 1, and is also described in [16,17,18].

For example, the TMDS encoding outputs 011110000 for black pixels, 001110011, 001110011, and 1000001100 for white pixels, and 1011001100 for invisible pixels. The pixel having multiple bitstream cases sequentially transmits the bitstreams, and the electronic signal of each bitstream is shown in Fig. 2. Fig. 2 illustrates the electronic signal of the respective pixel presented four times per pixel period. As mentioned earlier, the white pixel has three bitstream types, and they are
repeated sequentially such that the electronic signal has a length that is three times the period of the black pixel. Note that the invisible pixel has the same period as the black pixel. Consequently, each pixel value has a different period and signal waveform, and accordingly, the spectrum of each pixel is very different when Fourier decomposition is applied, as shown in Fig. 3.

As clearly shown in Fig. 3, each pixel signal consists of a different proportion of spectral components. The frequency interval between the components of each pixel can be determined as follows:

\[ \Delta f_{\text{Black}} = (2n - 1)f_p \quad (n = 1, 2, ..., N) \]  
\[ \Delta f_{\text{White}} = \frac{n}{3}f_p \quad (n = 1, 2, ..., N) \]  
\[ \Delta f_{\text{Invisible}} = nf_p \quad (n = 1, 2, ..., N) \]

where \( f_p \) is the pixel update frequency, which is a display configuration parameter. Consequently, because the spectral signal composition constituting each byte of pixel information is different, the collected pixel information varies depending on the selected frequency band. Thus, development of an efficient demodulation method is necessary.

**B. DISPLAY CONFIGURATION OF THE HDMI**

The display configuration, which is essential in determining the baseband signal, is shown in Fig. 4.

In Fig. 4, there are two regions: The visible space that presents a visible pixel, and the invisible space incorporated for VDU repose. In addition, there are four terms that determine the VDU resolution: Number of horizontal visible pixels (\( x_v \)), number of vertical visible pixels (\( y_v \)), total...
number of horizontal pixels \((x_t)\), and total number of vertical pixels \((y_t)\). As described in the previous section, the white and black pixels are shown in the visible space, whereas the invisible pixels are shown in the invisible space. Note that every pixel is converted to an electronic signal, and it is repeated from top left to bottom right sequentially and passes over to the next display information frame, as illustrated in Fig. 5.

These repetitions inevitably generate several periodic features, such as the horizontal update \((f_h)\), vertical update \((f_v)\), and pixel frequencies \((f_p)\). These terms are summarized in Table 1 as the primary display characteristics.

| Parameter | Value                        |
|-----------|------------------------------|
| \(x_t\)   | # of the total horizontal pixel |
| \(x_v\)   | # of the horizontal visible pixel |
| \(y_t\)   | # of the total vertical pixel |
| \(y_v\)   | # of the horizontal visible pixel |
| \(f_h\)   | Horizontal update frequency |
| \(f_v\)   | Vertical update frequency |
| \(f_p\)   | Pixel update frequency |

Most VDUs that adopt HDMI as their video interface conform to the VESA standard. It provides the number of horizontal and vertical pixels for each resolution, and the appropriate \(f_p\), \(f_h\), and \(f_v\) values are determined according to the user-defined monitor refresh rate. As a result, a single HDMI video interface signal frame can be modeled as an analog or phase-modulated baseband signal, where the horizontal update frequency constitutes the carrier frequency envelope with an interval of \(f_p/3\) because of the white pixels, as shown in Fig. 3.

### III. VERIFICATION OF THE ANALYSIS WITH SINGLE VDU

#### A. MEASUREMENT SET UP

A receiver system is set up with an RF front-end, antenna, bandpass filter, low-noise amplifier (LNA), and 1-channel software-defined radio to acquire the compromised emanation signal. The apparatus specifications and a schematic diagram are shown in Fig. 6.

As described in the previous section, if the resolution of a target VDU is given and its interface is HDMI, the main leakage band can be predicted. However, common-mode emissions may have various sources, such as process errors in differential lines, clock signal errors, and reflection owing to impedance mismatches. As a result, the presence of a signal component in a specific frequency band does not unconditionally guarantee leakage emanations. Furthermore, the signal strength of the compromising emanation is weak, and it is affected by the surrounding frequency environment. Hence, careful selection of a frequency band that satisfies all the mentioned conditions is a necessary first step.

#### B. MEASUREMENT IN ANECHOIC CHAMBER AND IMAGE RECONSTRUCTION WITH FRAME-AVERAGING TECHNIQUE

First, to determine the frequency band in which the compromising emanation from the target DUT occurs, the measurement setup is placed inside an anechoic chamber to exclude undesirable environmental conditions. The antenna used for this experiment was a log-periodic antenna (LPDA), and the configuration of the DUT and measurement is shown in Fig. 7. The distance between the VDU and measurement system was 7 m. The specific USRP operating conditions are as follows: sampling rate at 148.5 MHz, bandwidth of 20 MHz, window length of 16.67 ms, and repeated 200 times.

### TABLE 2: Parameter of target VDU

| Parameter | Quantity |
|-----------|----------|
| \(x_t\)   | 2200     |
| \(y_t\)   | 1125     |
| \(f_h\) (kHz) | 67.5  |
| \(f_v\)=Framepersec.\((Hz)\) | 60     |
As shown in Table 2, as the target display information consists of black, white, and invisible pixels, the spectrum shown in Fig. 3 provides good benchmarks for the demodulation method. Specifically, when there is a significant magnitude difference between the white and black pixels in a certain frequency band, the AM demodulation method is applicable; in contrast, when the magnitude of the two pixels is the same, the PM demodulation method is suitable. Then, the display configuration parameters, horizontal ($f_h$), vertical ($f_v$), and pixel frequencies ($f_p$), were recovered in advance to check whether the information regarding the received signal was from the target VDU. For $f_h$ and $f_v$, this is obtained by applying an autocorrelation to the received signal, as described in (2).

$$R(k) = \lim_{T \to T_{\text{meas}}} \int_{T}^{-T} y^*(t)y(t + \frac{k}{f_s})dt \quad (2)$$

To be specific to (2), $k$ is the integer of the time lag, $T_{\text{meas}}$ is the received signal time, $y(t)$ is the leakage signal, $y^*(t)$ is the conjugate of $y(t)$ and $f_s$ is the sampling rate. The autocorrelation process result of the leakage electromagnetic waves at 643 MHz is shown in Fig. 8, and it is conducted on a windowed signal with a two frame acquisition time.

The number of samples in 1-frame is $2.475 \times 10^6$, and Fig.8 shows that the peak values of auto-correlation are also present at the same position. The interval between peaks represents the horizontal synchronization, which is 1125, the same as the number of the total horizontal pixels. A display image can be reconstructed using the estimated components of the display configuration. Nonetheless, the reconstructed image is usually not likely to provide meaningful information because of the extremely low signal strength of the compromising emanation. Thus, a special scheme to improve the SNR is necessary, and the frame-averaging technique is an excellent candidate. However, it requires advanced frame synchronization, and to satisfy such a requirement, an accurate $f_p$ of the display information should be retrieved. $f_p$ is obtained by using the cross-correlation method, as described in (3), and the result of the cross-correlation between a reference frame
and an arbitrary frame is shown in Fig. 9.

\[
G(k) = \lim_{T \to T_{meas}} \int_{T}^{T} y^*(t)x(t + \frac{k}{f_s})dt
\]  

(3)

With the estimated value of \(k\) in (3), the time lag caused by the difference between \(f_s\) and \(f_p\) is obtained, and eventually, each frame may be synchronized using time compensation. The estimated \(k\) from the maximum \(G(k)\) of successive frames is shown in Fig. 9(d), and an averaged reconstructed image is shown in Fig. 9(a), (b), and (c). The frequency bands used for measurement were 594, 643, and 693 MHz, which correspond to the frequency bands of the white and invisible pixels. White pixels were selected as the target because leakage electromagnetic waves occur in various frequency bands. Conversely, the frequency band components of invisible pixels were selected because the leakage electromagnetic waves are relatively large compared to other signals. As shown in Fig. 3, invisible pixel components are highlighted at 594 MHz, and white pixel components are highlighted at 643 and 693 MHz. As clearly shown in the figures, the letters and diagrams become much clearer with the frame-averaging technique.

IV. ANALYSIS OF THE MULTIPLE VDUS

In the previous section, the feasibility of reconstructing the display information was demonstrated based on a display configuration parameter analysis. As a next step, a method to distinguish display information from multiple-compromising emanation signals (MCES) from identical multiple VDUs is presented in this section. For experimental verification, an additional DUT set displaying an upside-down image used in Section 3 was utilized, and the measurement was conducted in an anechoic chamber. The two images displayed are shown in Fig. 10, and the spectrum of the acquired MCES is shown in Fig. 12. The distance between the VDUs and the measurement system is 7 m. The specific operating conditions of the USRP are as follows: sampling rate of 148.5 MHz, bandwidth of 20 MHz, window length of 16.67 ms, and repeated 200 times. Fig. 11 shows the reconstruction results for the two monitors. The restoration process is the same as before; however, the synchronization between each frame indicates that it is different and not constant, and as a result, the restored screen information with an averaged signal indicates degraded performance.

A. ANALYSIS OF THE SPECTRUM

As described earlier, the bitstream array that represents the display information pixel values is continuously generated according to the predetermined pixel frequency, which is determined by the independent clock signal of each VGA. However, although the VGA that transmits the bitstream signal to the connected VDU is identical to the others, the clock signal inevitably exhibits asynchronous behavior owing to
the independent hardware devices. This results in frequency differences between the pixel rate of the respective display information and becomes more pronounced when the pixel frequency spectral harmonics order is increased.

\[ S_2(t) = S_{\text{base}, 2}(t) \cdot e^{j2\pi(f_0 + \Delta f)t} \]  

In (4) and (5), \( S_1(t) \) and \( S_2(t) \) are the baseband signals that include various crucial components distributed within an interval of \( f_h \). The exponential terms can be considered as the carrier frequencies of each baseband signal and include the frequency difference \( \Delta f \). The MCES from the two VDUs is modeled as the summation of \( S_1(t) \) and \( S_2(t) \), and it is evident that a direct MCES demodulation, which eliminates the baseband frequency, generates a shuffling of the baseband signals. Consequently, the conventional correlation method is no longer valid because of incorrect pixel-frequency estimation. Accordingly, an additional pretreatment for selective display information is required.

**B. NARROW BAND FILTERING PROCESS**

To perform selective display information reconstruction based on the MCES characteristics, the baseband signal components, dispersed with an interval of \( f_h \), but carried on a different carrier frequency, should be selectively utilized. Accordingly, an appropriate filter is proposed, and the RCFT is described below.

\[
H(f) = \begin{cases} 
1, & |f| \leq \frac{1-\beta}{2\pi T} \\
\frac{1}{2} [1 + \cos(\frac{\pi f}{\beta} |f| - \frac{1-\beta}{2\pi})], & \frac{1-\beta}{2\pi T} < |f| \leq \frac{1+\beta}{2\pi T} \\
0, & \text{otherwise} 
\end{cases}
\]

\[ H_{\text{train}}(f) = \sum_{n=0}^{n} H(f) \cdot e^{\pm j\pi n T} \]  

The transfer function in (6) is the raised cosine filter [19] that has a sharp cut off, and (7) is the RCFT with an interval of the prominent components, \( f_h \). The roll-off factor \( \beta \) of the proposed RSTF is 0.1, the bandwidth \( T \) is 1 kHz, and the number of trains \( n \) is 20. The selection of \( f_0 \) in (7) determines the baseband signal that is to be extracted from the MCES spectrum, and the result is shown in Fig. 12.

**C. RESULT OF RECONSTRUCTED INFORMATION**

The designed RCFT renders the MCES with only the selected display information characteristics. However, it is extremely narrow and generates an inevitable signal distortion when it is demodulated, as shown in Fig. 13. Clear information features do not exist, but the figure’s blurry shapes and background position appear.

Because the information location exists, the filtered MCES signal is still applicable for the correlation, which quantitatively allows the individual pixel rate to be adjusted. Eventually, an accurate pixel rate of the respective display information is achievable, and the frame-average results conducted using the extracted pixel rates are shown in Fig. 14 and Fig. 15, revealing excellent performance. An average of 200 frames was used in these experiments. In the case of Fig. 14, because it is the result of reconstructing the leakage electromagnetic waves for the system used in the first experiment, the \( k \) of the Max \( G(k) \) value is the same as in the first experiment, as shown in Fig. 9(d). Alternatively, in the
case of Fig. 15, it is the result of reconstructing the second system's information. It has a $k$ of $\text{Max} \ G(k)$ value with a different slope than the first system, which indicates that there is a difference in the clock between the two systems. The two results demonstrate that the proposed method can distinguish between the information of the two VDUs. However, the frequency of the invisible pixels produces a component that strongly interferes with the recovered information. Interference appears very strong at 594 MHz because the contrast of the invisible pixels is higher than that of the white pixels that represent information. Therefore, the proposed method to distinguish video information consisting of white, black, and invisible pixels in multiple systems must reconstruct the information, excluding the invisible pixel frequency.

Selective information recovery is possible even for identical display devices with identical refresh rates in space. We hope that this analysis raises awareness among users and the possibility of security breaches related to eavesdropping in the future.
V. CONCLUSION
This study presents a procedure for information reconstruction using electromagnetic wave leakage originating from two identical video systems. The conventional synchronization methodology, which does not include any discriminator for information from different displays, is severely affected by the interference of the other, eventually offering incorrect adjustment parameters. Conversely, the proposed scheme first discriminates the display information on the spectrum using RCFT, making it possible to extract the accurately adjusted parameter for the respective displays using cross-correlation. In addition, on the frame average, we verified that the recommended frequency bands for effective reconstruction of the information are where $\Delta f_{\text{white}}$ and $\Delta f_{\text{Invisible}}$ are not the same because of the afterimage generated by the high invisible pixel intensity after the process. Finally, we demonstrated that leakage electromagnetic waves from two VDUs in the exact location are acquirable for the respective information at a distance of 7 m. Furthermore, additional research can effectively attenuate or eliminate the afterimage effects by utilizing the disadvantageous frequency bands.

REFERENCES
[1] D. Gollmann. “Computer Security, 2nd edition.” John Wiley and Sons, Inc., Jan. 2006.
[2] W. van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?”, Comput. Secur., vol. 4, no. 4, pp. 269–286, Dec. 1985.
[3] M. G. Kuhn, “Compromising emanations of LCD TV sets”, IEEE Transactions on Electromagnetic Compatibility, IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 564–570, 2013.
[4] H. S. Lee, D. H. Choi, K. Sim and J. Yook, “Information recovery using electromagnetic emanations from display devices under realistic environment”, IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1098–1106, Aug. 2019.
[5] H. S. Lee, K. H. Sim and J. G. Yook, “Analysis of the Electromagnetic Leakage from Liquid Crystal Display Monitors”, J. Korea Electromagn. Eng. Soc., vol. 27, pp. 844–853, 2016.
[6] Y. I. Hayashi, N. Homma, T. Watanabe, W. O. Price, and W. A. Radasky, “Introduction to the special section on electromagnetic information security,” IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 539–546, Jun. 2013.
[7] D. J. Sim, H. S. Lee, and J. G. Yook, “Measurement and Analysis of Electromagnetic Emanations from USB Keyboard,” International Journal of Advanced Research in Computer Engineering and Technology, vol. 4, no. 4, pp. 1576–1579, Apr. 2015.
[8] A. Boitan, I. Kubiak, and R. Bărtusică, “Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process,” Symmetry, Nov. 2020.
[9] P. De Meulmeester, B. Scheers and G. A. E. Vandenbosch, “A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels,” IEEE Transactions on Electromagnetic Compatibility, vol. 62, no. 3, pp. 663–672, Jun. 2020.
DONG-HOON CHOI received the B.S. degree in electronic communication engineering from Chonnam National University, Yeosu, South Korea, in 2016, where he is currently working toward the Ph.D. degree in electrical and electronic engineering at Yonsei University, Seoul, Korea. His research interests include the TEMPEST, information recovery, and EMI/EMC.

EUIBUM LEE received his B.E and M.S degree in Electronic Engineering from Konkuk University, Seoul, Korea in 2018 and 2020 respectively. He is currently working toward his Ph.D degree in electrical and electronic engineering at Yonsei University, Seoul, Korea. His current research interests include RF circuit design, EMI, EMC, TEMPEST and information security.

JONG-GWAN YOOK (S’89–M’97–SM’12) received the B.S. and M.S. degrees in electronics engineering from Yonsei University, Seoul, Korea, and the Ph.D. degree in electrical engineering and computer science from the University of Michigan, Ann Arbor, MI, USA, in 1987, 1989, and 1996, respectively. He is currently a Professor with the School of Electrical and Electronic Engineering, Yonsei University. His research interests include theoretical/numerical EM modeling and characterization of microwave/millimeter-wave circuits and components and design, analysis, and optimization of high-frequency high-speed interconnects, including signal/power integrity (EMI/EMC), based on frequency-domain as well as time-domain full-wave methods. Dr. Yook was the recipient of the Excellent Teaching and Research Activity Award from Yonsei University several times. From 2009 to 2012, he was the Chair of the Korean EMC Society. From 2012 to 2013, he was a Distinguished Lecturer for the IEEE EMC Society. He was also the Chair of the Technical Program Committee of Asia Pacific International Symposium on Electromagnetic Compatibility Conference 2017.

* * *

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/