A Quantitative Analysis of Compromising Emanation from TMDS Interface and Possibility of Sensitive Information Leakage

Euibum Lee, Dong-hoon Choi, Taesik Nam and Jong-gwan Yook, (Senior Member, IEEE)

Department of Electrical and Electronic Engineering, Yonsei University, Seoul, 03722 Korea, Republic of (e-mail: ikanow@yonsei.ac.kr)
Corresponding author: Jong-gwan Yook (e-mail: jgyook@yonsei.ac.kr).

ABSTRACT This paper investigates the electromagnetic interference characteristics of the transition-minimized differential signaling (TMDS) scheme, a well-known technology for rapid serial data transmission, from a radio communication perspective. Such scrutiny regarding the leaking phenomenon inspires a pseudo model of the compromising signal model, which can simultaneously consider behavioral features of the software-defined radio with a simple RF front-end measuring the leakage. In this work, a conceptual explanation with mathematical formulations in implementing the pseudo model has been presented. Subsequently, by merging the model with various extra noises being in nature, the model can be utilized to facilitate and quantify the possibility of information extraction from the defected electromagnetic signatures. Furthermore, it is interesting to note that there are asynchronous problems due to inevitable timing errors in video display devices, even with a sophisticated acquisition system, turning out to be fatal for the frame-averaging scheme conducted before the signal demodulation. In view of these challenges, we have formulated a synchronizing scheme and verified validity by utilizing the pseudo model with the extra noise to take into account the asynchronous problem. Moreover, the structural similarity (SSIM), a function of the signal-to-noise ratio, can provide the number of frames for the frame-averaging process and eventually give the minimum acquisition time to earn meaningful information from the compromising emanation. Finally, after the appropriate post-processing, the extracted information from the actual measurements is compared with the reconstruction from the pseudo-model results revealing excellent agreements.

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

I. INTRODUCTION

Nowadays, information, treated as a priority asset, constitutes an irreplaceable part of daily human life. Accordingly, related software-security technology is of utmost importance to most users in preventing exposure to extortion threats [1]. However, different types of risks also have been reported that could bypass such protection by utilizing radiated emission, which is a physical phenomenon inherent in the hardware of electronic devices [2]. The technique based on this physical phenomenon is called a side-channel attack, and its purpose is to recover specific information such as cryptographic keys [3], display information [4], or other types of sensitive information. This study intends to focus on the recent technological progress on the possibility of the information reconstruction from the electromagnetic leakage (EM leakage) from the standardized display interface (SDI) cables, and the related historical background is briefly described. W. van Eck was the first to report the presence of display information in EM leakage in 1985. Moreover, he demonstrated that cathode ray tube devices were susceptible to such leakage [5]. Later, Kuhn stated that the EM leakage from digital display systems also contains meaningful information; furthermore, he verified the possibility of reconstruction [6]. Subsequently, Plukovic reported that the information radiated by digital devices is either amplitude- or frequency-modulated within the leakage [7]. Thus, it is reasonable to infer that the information can be partially reconstructed through appropriate sampling and demodulation after raw signal acquisition.
A video system usually comprises three parts. The first is a video graphic card (VGC) responsible for consistently generating and transmitting hundreds of frames of display information, the second is a SDI cable for video signal transmission, and the third is a video display unit (VDU) that receives the signal and visualizes the information. For better comprehension, a simplified configuration of a video display system is shown in Fig. 1.

Note that each component has various paths for the electronic signals of display information, and accordingly, it is inevitable that the signal flows on transmission lines with discontinuities entailing EM-leakage bearing some form of repetitive information. In addition, the SDI and VDU are more likely to experience EM leakage than the VGC, which is typically placed inside the grounded conductor housing. For these reasons, many reports have assumed these two exposed objects as the primary sources of EM leakage and have attempted to acquire meaningful information from them [8].

### FIGURE 1: Generalized video display system configuration

The VGC generates display information according to the standard preset defined by the ‘Video Electronics Standards Association (VESA)’ [14]. The preset includes two specific divisions: the display region and blank region. So, for example, given the display in a VDU of the alphabet ‘A’ as shown in Fig. 2-(a), the signals in the HDMI cable include the pixel information of the display region as well as the pixels in the blank region (PBR). Such an empty area defined by the VESA is similar to most SDIs.

As shown in Fig. 2-(a), $x_t$ and $y_t$ are the total numbers of pixels in the horizontal and vertical directions, respectively, and $x_d$ and $y_d$ denote the partial ranges where visible pixels exist. Therefore, if each pixel constituting the display information of Fig. 2-(a) is assumed as a personal space described in Fig. 2-(b), the transmission of information can be represented by filling the respective area with a specific symbol indicating the value of the pixel. The transition minimized differential signaling (TMDS) fills each space with the value that consists of a 10-bit sequence during a time interval of 10ns.

The TMDS is one of the most popular standard display interfaces. It comprises multiple pin ports and primarily utilizes six pins to transmit the display information: red $+$, red $-$, green $+$, green $-$, blue $+$, and blue $-$ in differential signaling. It is known that the leading cause of EM leakage in differential circuits is common-mode noise caused by fabrication errors or timing mismatches [4], [10]. Thus, the signal characteristics of EM leakage are highly relevant to the signaling in HDMI, and its investigation gives excellent insight into the leakage of sensitive information.

The VGC generates display information according to the standard preset defined by the ‘Video Electronics Standards Association (VESA)’ [14]. The preset includes two specific divisions: the display region and blank region. So, for example, given the display in a VDU of the alphabet ‘A’ as shown in Fig. 2-(a), the signals in the HDMI cable include the pixel information of the display region as well as the pixels in the blank region (PBR). Such an empty area defined by the VESA is similar to most SDIs.

As shown in Fig. 2-(a), $x_t$ and $y_t$ are the total numbers of pixels in the horizontal and vertical directions, respectively, and $x_d$ and $y_d$ denote the partial ranges where visible pixels exist. Therefore, if each pixel constituting the display information of Fig. 2-(a) is assumed as a personal space described in Fig. 2-(b), the transmission of information can be represented by filling the respective area with a specific symbol indicating the value of the pixel. The transition minimized differential signaling (TMDS) fills each space with the value that consists of a 10-bit sequence during a time interval of 10ns.

The TMDS is one of the most popular standard display interfaces. It comprises multiple pin ports and primarily utilizes six pins to transmit the display information: red $+$, red $-$, green $+$, green $-$, blue $+$, and blue $-$ in differential signaling. It is known that the leading cause of EM leakage in differential circuits is common-mode noise caused by fabrication errors or timing mismatches [4], [10]. Thus, the signal characteristics of EM leakage are highly relevant to the signaling in HDMI, and its investigation gives excellent insight into the leakage of sensitive information.

The VGC generates display information according to the standard preset defined by the ‘Video Electronics Standards Association (VESA)’ [14]. The preset includes two specific divisions: the display region and blank region. So, for example, given the display in a VDU of the alphabet ‘A’ as shown in Fig. 2-(a), the signals in the HDMI cable include the pixel information of the display region as well as the pixels in the blank region (PBR). Such an empty area defined by the VESA is similar to most SDIs.

As shown in Fig. 2-(a), $x_t$ and $y_t$ are the total numbers of pixels in the horizontal and vertical directions, respectively, and $x_d$ and $y_d$ denote the partial ranges where visible pixels exist. Therefore, if each pixel constituting the display information of Fig. 2-(a) is assumed as a personal space described in Fig. 2-(b), the transmission of information can be represented by filling the respective area with a specific symbol indicating the value of the pixel. The transition minimized differential signaling (TMDS) fills each space with the value that consists of a 10-bit sequence during a time interval of 10ns.

The TMDS is one of the most popular standard display interfaces. It comprises multiple pin ports and primarily utilizes six pins to transmit the display information: red $+$, red $-$, green $+$, green $-$, blue $+$, and blue $-$ in differential signaling. It is known that the leading cause of EM leakage in differential circuits is common-mode noise caused by fabrication errors or timing mismatches [4], [10]. Thus, the signal characteristics of EM leakage are highly relevant to the signaling in HDMI, and its investigation gives excellent insight into the leakage of sensitive information.
For better understanding, take the 5th row of display information shown in Fig. 2-(a) as an example; it consists of a consecutively alternating sequence: a white bit sequence lasting for $6T_p$, a black bit sequence lasting for $6T_p$, another white bit sequence lasting for $3T_p$, and finally, the bit sequence representing the PBR lasting for $3T_p$. Therefore, if we reveal the bit sequence of the respective R, G, and B values in each space, the frequency characteristic of the current signal flow is available when the pixel’s color is given. The specific TMDS bit sequence generation principle is well described in [4]; in this study, the bit sequences of the black and white pixels are described in addition to the PBR in Fig. 3 as an example. These are the most elementary pixel compositions constituting a document. As shown in Fig. 3-(a), it is evident that the constant bit sequence repeats at $T_p$ intervals for black pixels. In the case of white pixels, there are two types of bit sequences repeating twice and once during a total of $3T_p$ intervals, as shown in Fig. 3-(b). Regarding the PBR, there exist four types of bit sequences in reality [4], but for the sake of convenience, this study focuses on a specific bit sequence that generally occupies more than 90% of its pixel space. As such, because the bit sequence representing the pixel of a particular color continuously changes with time, it is evident that the signal characteristics of EM leakage emitted from TMDS interface also change instantaneously. Therefore, in a specific duration where the same bit sequence continuously appears, the EM leakage can be considered a Fourier series. This series can be assumed to be composed of harmonic components associated with $f_p$, which is the reciprocal of $T_p$. Interestingly, the white pixel, the bit sequences of which are consecutively repeated every $3T_p$, presents a harmonic component with $f_p/3$ separation. For better comprehension, a spectrogram of the 5th row of Fig. 2-(a) is illustrated in Fig. 4.

Figure 4 shows that the inherent $f_p$-related harmonic components for three different pixels are distinctly visible during their time period. Moreover, it is clear that such analytical approaches can be applied similarly to all other colors rep-
represented by pixel values. In addition, because the HDMI repeatedly transmits the number of pixels constituting a frame \((x_t, y_t)\) through serial communication following the direction of progress, as illustrated in Fig. 2-(b), the spectrum shown in Fig. 5 can be obtained. Note that the length of one frame, \(T_{fr}\), is given as \(x_t \cdot y_t \cdot T_p\).

\[
T_{fr} = x_t \cdot y_t \cdot T_p
\]

**FIGURE 5:** Frequency spectrum during \(T_{fr}\)

It is noteworthy that by stretching a specific harmonic band, the center frequency of which \(f_c\) is associated with \(f_p\), various distinct frequency components are observed, as shown in the circle of Fig. 5. These are observed at an interval of the horizontal synchronization frequency, \(f_h\), which is the reciprocal of the horizontal sync periodicity \((T_h = x_t \cdot T_p)\). This phenomenon occurs because the pixels are arranged with a vertically identical color as well as the PBR in the range of \(y_t\) rows. Interestingly, such spectral characteristics are similar to those of the baseband signal modulated at multiple carrier frequencies. Because the radiation of the EM leakage starts with a rapid transition of current flow in the circuit, the spectral characteristics of the HDMI signal are extremely useful in analyzing the corresponding EM leakage.

**III. MODELING AND QUANTIFICATION**

The previous section concluded that the display configuration along the pixel arrangement determines the baseband characteristics. Moreover, the shape and combination of the TMDS bit sequence assigned to each pixel determines the carrier frequency, which modulates the baseband signal. This section proposes a PCE model through a joint analysis of the operational characteristics of a real-time software-defined radio (SDR) used for signal acquisition. The model offers a quantitative analysis of the frame-averaging technique used for display information reconstruction.

**A. MODELING OF THE PSEUDO-CE AND SYNCHRONIZING FORMULATION**

Most display devices express the values of each pixel with respective 8-bits for red, green, and blue. In addition, in the case of the HDMI, R, G, and B values are converted into TMDS codes and transmitted in parallel. Unfortunately, because of the excessive number of cases (16,777,216 for 24-bit), when every color of the pixel is examined, this study assumes only five achromatic colors in which the R, G, and B values of the pixels in the display region are identical to each other. The five colors that were selected are: black \(\{0_R, 0_G, 0_B\}\), dark gray \(\{63_R, 63_G, 63_B\}\), gray \(\{127_R, 127_G, 127_B\}\), light gray \(\{191_R, 191_G, 191_B\}\), and white \(\{255_R, 255_G, 255_B\}\). First, to analyze the radiation emission caused by the signal flow in the HDMI (one of the TMDS interface) operating as Full-HD (1920x1080, 60 Hz), a near-field H-field probe and a high-speed digital oscilloscope were utilized, as illustrated in Fig. 6.

**FIGURE 6:** Measurement of EM-leakage according to the color

The acquisition time of the leakage was more than \(100T_p\). Fig. 7 presents the spectrum and corresponding waveforms of the six types of pixels (five achromatic colors + PBR), checking their harmonic configuration according to the TMDS bit sequences assigned to each pixel.

As is clearly shown in Fig. 7, the dark gray pixel manifests an alternatively repeating EM leakage waveform with a \(3T_p\) period and \(f_p/3\) interval in its harmonic spectrum, similar to the white pixels. In addition, in the case of the gray pixel, the total period of which is \(5T_p\), also presents an \(f_p/5\) interval.

**FIGURE 7:** Spectrum and the corresponding waveforms of the pixels

Consequently, the harmonic configuration of the respective color pixel is defined as (1). In (1), A is a positive integer,

\[
A\{a_1, a_2, a_3\} = \begin{cases} 
1 & \text{for black} \\
2 & \text{for dark gray} \\
3 & \text{for gray} \\
4 & \text{for light gray} \\
5 & \text{for white}
\end{cases}
\]
and $s_{color}$ are the noise-free time-domain signals, as shown in Fig. 7, according to its subscript $color$. The EM leakage appears in a broad frequency band; thus, if a particular band, including a specific harmonic component of the respective
color pixel, is collected among the multiple configurations, it is possible to distinguish the difference in the pixel values using various demodulation methods [15]. Here, a real-time SDR comprising down-conversion, filters, and a continuous signal sampler can be utilized for the band-limited signal collection, as shown in Fig. 8, [15], [16].

In the SDR, there exists a trade-off between the SNR and the bandwidth of the acquired signal. Hence, it is crucial to select an appropriate bandwidth, and this study sets the bandwidth of the radio frequency (RF) front-end as approximately 5% of the fractional bandwidth (FBW) at a specific center frequency \( f_c \). In addition, the bandwidth is limited not to exceed \( f_p/3 \). For a more detailed instance, this study deals with generating PCE after collecting a specific band, the center frequency of which is \( (3 + 2/3)f_p \), using the SDR under the previous bandwidth assumption. Note that the selected frequency is the middle frequency among the effective frequency ranges of our acquisition system. Assuming that the operation frequency of the down-conversion mixer in the SDR \( f_{LO} \) shifts the selected band, the center of which is \( f_c \), to the origin, as shown in (2), the spectrum of the resultant pixel is presented in Fig. 9.

\[
s_{\text{color, filt}}(f) = S_{\text{color}} \cdot H_{BPF,a} 5\% \cdot \delta(f - f_{LO}) \quad (2)
\]

In (2), \( S_{\text{color}}(f) \) is a spectrum of \( s_{\text{color}}(t) \) in (1). As shown in Fig. 9, there are three types of pixels, dark gray, gray, and white that exist on the selected band. In addition, the relative magnitude can be derived using Parseval’s theorem, as in (3).

\[
V_{\text{color}} = \sqrt{\int_{-\infty}^{\infty} S_{\text{color, filt}}^2(f) df} \quad (3)
\]

Note that the values were normalized within an 8-bit expression. To utilize the \( V_{\text{color}} \) results in the configuration of the baseband, two types of display information containing only the five types of achromatic color pixels are adopted and subsequently transformed into the pixel magnitude configuration according to Table I, as shown in Fig. 10.

| Table 1: \( V_{\text{color}} \) on \((3+2/3)f_p \). |
|---|---|---|
| \( V_{\text{Black}} \) | \( V_{\text{D.gray}} \) | \( V_{\text{Gray}} \) |
| 0 | 255 | 180 |
| \( V_{\text{L.gray}} \) | \( V_{\text{White}} \) | \( V_{\text{PBR}} \) |
| 0 | 110 | 0 |
Now, the baseband configuration for the PCE can be achieved by allocating the converted pixel information into the Display region, as shown in Fig. 2-(a), and subsequently filling the remaining blank region with the PBR magnitude derived in the previously selected \((3 + 2/3) f_p\) band. Furthermore, as shown in Fig. 9, the gray pixel, which includes \((1/15) f_p\) of the frequency offset from the origin, should be in consideration. For this reason, instead of using the constant value of 180, it utilizes a complex value of \(180 \cdot e^{j(2\pi 1/15 n + \phi_s)}\). Here, \(n\) is the order of samples in a discrete signal, while \(\phi_s\) is a term used to initialize the phase when a bundle of consecutive gray pixels re-emerges. Given that the complete configuration of the baseband signal is arranged in a serial format according to the direction of progress described in Fig. 2-(b), a discrete signal of \(S_{base}[n]\) comprises \(x_t \cdot y_t\) number of samples, constituting one frame. In addition, VDS continuously repeats the baseband signal as follows:

\[
S_{base}[n] = S_{base}[n - x_t y_t].
\]  

(4)

Then, the re-sampling of (4) with \(T_p\) can be written as presented in (5):

\[
S_{base}(t) = \sum_{n=-\infty}^{\infty} S_{base}(nT_p) \cdot \text{sinc}(\frac{t - nT_p}{T_p}),
\]  

(5)

where, \(S_{base}(t)\) is the original signal at the center frequency of \(f_c\), and the down-conversion frequency, \(f_{LO}\), is used in SDR. Now, the received signal right after the RF front-end can be modeled as:

\[
S_{received}(t) = S_{base}(t) \cdot e^{j2\pi (f_c - f_{LO}) t}.
\]  

(6)

Figure 11 shows a comparison between the spectrum of the pseudo-\(S_{received}\) and the actual-\(S_{received}\) observed using the oscilloscope. The time length of the Fourier transform is defined as \(T_{fr}\). The spectral characteristics of the pseudo-signal and the actual signal from \((3+2/3) f_p\) are quite similar. Taking this into consideration, we now discuss the behavioral properties of the sampling and windowing process for the real-time SDR using the implemented pseudo-signal. It must be noted that a tiny tolerable range exists for every electronic device; consequently, the VDS cannot update the display information while perfectly following \(T_{fr}\), defined by VESA. This is illustrated in equation (7), in which the correlation between the accurate sampling rate of SDR \((f_s)\) and \(f_p\), including some errors, is expressed using \(\Delta\). In addition, the natural number \(P\) ensures at least one sample collection for one-pixel information.

\[
P \cdot f_p = \Delta \cdot f_s \quad (P \in \mathbb{N})
\]  

(7)

The required sampling time for an approximate single frame \(T_{window}\), as many as the number of pixels \((x_t \cdot y_t)\), can be expressed as:

\[
T_{window} = \frac{P}{f_s} \cdot x_t \cdot y_t.
\]  

(8)

Here, by considering (7) and (8) simultaneously, a time difference can be observed between \(T_{window}\) and \(T_{fr}\) owing to...
to $\Delta$ as;

$$T_{\text{window}} = \Delta \cdot T_{fr}. \quad (9)$$

Additionally, because of the unknown error parameter, $\Delta$, the previously defined $f_{LO}$ can be expressed as;

$$f_{LO} = \Delta \cdot f_c. \quad (10)$$

This error prevents the down-conversion from cancelling out the exponential term in (6), eventually causing a carrier frequency offset. Finally, by considering the sampling characteristics of the ADC in the real-time SDR, a pseudo-CE with a length of $T_{\text{window}}$ can be obtained as;

$$S_{fr,k}(t) = \sum_{n=0}^{N-1} s_{\text{base}}(t - \tau_k) \cdot e^{j2\pi(f_c-f_{LO})(t-\tau_k)} \cdot w(t) \cdot \delta(t - \tau_k - \frac{n}{f_s}). \quad (11)$$

(but, $k = 0, 1, 2, ..., K-1, N = x_t, y_t$)

Here, $\tau_k$ is $k \cdot T_{\text{window}}$ and $w(t)$ is a window function whose time length is $T_{\text{window}}$ from the origin. $S_{fr,k}$ shows that the VDS clock error ($\Delta$) and carrier frequency offset error ($f_{\text{carr}} - f_{LO}$) are accumulated in proportion to the windowing index ($k$). Therefore, in order for the sampled signal $s_{fr,k}[n]$ to satisfy the coherency for every $k$, time error correction as much as $\tau_k$ and phase error correction as much as $\tau_k(f_{\text{carr}} - f_{LO})$ must be conducted. The compensation reflecting these can be expressed as;

$$S_{\text{adj},k}[n] = S_{fr,k}[n] \ast \delta[n + k\Delta] \cdot e^{-j2\pi k\Delta(f_c-f_{LO})} \quad (12)$$

To obtain the parameters $k\Delta$ and ($f_{\text{carr}} - f_{LO}$), auto-correlation [11] and carrier frequency offset estimation can be utilized [13].

### B. Quantitative Analysis of Information Reconstruction Possibility

This section describes the possibility of sensitive information reconstruction utilizing the implemented PCE model. The sensitive information adheres in the CE with various modulated forms, and several preceding studies have described that the most effective demodulation technique is amplitude demodulation, as presented in (13) [4], [5], [8], [11], [17], [18];

$$u_{AM}[n] = \sqrt{S_{fr,k}[n] \cdot S_{fr,k}^*[n]}. \quad (13)$$

After the demodulation of the windowed PCE ($S_{fr,k}$), the reconfiguration of the display information is available by reshaping the demodulated PCE in accordance with the display configuration shown in Fig. 2-(a). However, the CE does not exist in a pure state but is combined with extra noise in a realistic environment. Hence, ($N_{AWGN}$) of which distribution follows the Gaussian is applied to the PCE, and eventually, $S_{\text{noisy}}$ that comprises $S_{fr}$, and $N_{AWGN}$ as in (14) is utilized. Also, the SNR is defined as in (15).

$$S_{\text{noisy},1} = S_{fr} + N_{AWGN} \quad (14)$$

$$SNR_{1,2} [\text{dB}] = 20 \cdot \log_{10}\frac{S_{fr,2}(\text{RMS})}{N_{AWGN}(\text{RMS})}. \quad (15)$$

Here, there are two kinds of $S_{\text{noisy}}$ as an instance; one of which, $S_{\text{noisy},1}$, includes the conditions; $P = 1, f_c = (3+2/3) \cdot f_p, \Delta = 100.00001\% (f_c-f_{LO})/f_{LO} = 0.000091\%$, $SNR = -6.01$ dB and Fig. 9-(a) is its $S_{base}$, while the other, $S_{\text{noisy},2}$, has the conditions; $P = 1, f_c = (3 + 2/3) \cdot f_p, \Delta = 99.99989\%, (f_c - f_{LO})/f_{LO} = 0.00009\%$, $SNR = -5.99$ dB and Fig. 9-(b) is its $S_{base}$. Because $P$ is 1 for both cases, the number of samples for a single $k$ is approximately $x_t \cdot y_t$. Accordingly, the reconfiguration can be achieved by arranging $u_{AM}[S_{\text{noisy}}]$ in a two-dimensional format, as shown in Fig. 2-(a), and the results for different windowing index ($k$) are illustrated in Fig. 12.

As shown in Fig. 12, most of the sensitive information from the pseudo-CE is not achievable at all only with a single $k$ of $S_{fr}$ owing to the considerable amount of additive noise. Therefore, to define the possibility of the sensitive information acquisition from such a noisy PCE, we utilized a different index called structural similarity (SSIM), which is defined as an objective method to quantify the visual difference between a distorted and reference image [19];

$$SSIM_{S_1,S_2} = \frac{(2\mu_{S_1}\mu_{S_2} + c_1)(2\sigma_{S_1S_2} + c_2)}{(\mu_{S_1}^2 + \mu_{S_2}^2 + c_1)(\sigma_{S_1}^2 + \sigma_{S_2}^2 + c_2)}. \quad (16)$$
In (16), $\mu_{S_1}, \mu_{S_2},$ and $\sigma_{S_1}, \sigma_{S_2}$ are the average and variance of $S_1$ and $S_2$, respectively, and $\sigma_{S_1S_2}$ is the covariance between $S_1$ and $S_2$. In addition, $c_1$ is set as $(0.01 \cdot 255)^2$ and $c_2$ is set as $(0.03 \cdot 255)^2$ in this work. Given that $S_1$ is $u_{AM}[S_{fr,k}]$ as the reference signal and $S_2$ is $u_{AM}[S_{noisy,k}]$ as the distorted signal, the SSIM variation as a function of SNR is obtained, as shown in Fig. 13.

$$S_{fa\text{ or }2}[n, K] = \frac{1}{K} \sum_{k=0}^{K-1} (S_{adj\text{ or }2,k} + N_{AWGN})$$

$$= S_{fr\text{ or }2,0} + \frac{N_{AWGN}}{K}$$

In (17), Given that the coherency of every $S_{fr,k}$ is established based on $k = 0$, it is manifest that the every $S_{fr,k}$ is similar to $S_{fr,0}$ and additive noise decreases according to the averaging divider ($K$). Furthermore, the SNR variation according to the number of averaged frames can be derived as (18), and a related improvement graph is presented in Fig. 14.

$$SNR_{fa\text{ or }2}[K][dB] = 20 \cdot \{log_{10}(\frac{S_{fr\text{ or }2,0}}{N_{AWGN}}) + log_{10}\sqrt{K}\}$$

Considering the minimum value of SSIM to obtain meaningful information from the noisy PCE is 95%, the corresponding SNR value for each of $S_{noisy1}$ and $S_{noisy2}$ is respectively 12.12 dB and 15.35 dB, according to the graph presented in Fig. 13. Therefore, to improve the results shown in Fig. 12, having an SNR of approximately -6 dB, the required amount of frames are estimated as 65 and 137, respectively, as shown in Fig. 14. Subsequently, the reconstructions after conducting the frame-averaging are presented in Fig. 15.
In (20), the parameters that use the subscript 1 are regarded as the $S_{\text{base}}$, as shown in Fig. 10-(a) and 2 for Fig. 10-(b). In addition, $P$, $f_c$, and the joint error parameters related to $\Delta$ and $(f_c - f_{LO}) / f_{LO}$ of $S_{fr1}$ and $S_{fr2}$ are the same as the previous assumption, and their scalars $\alpha$ and $\beta$ are 0.682 and 1, respectively, with $N_{\text{AWGN}}$. Under such conditions, the reconstructed information $u_{AM} [S_{\text{mult}}]$ at different $k$ values is shown in Fig. 16, and both $SNR_1$ and $SNR_2$ are set to -10 dB.

Since the required minimum SNR to achieve meaningful information is 12.12 dB and 15.35 dB, as discussed in the previous part, the frame average for $S_{\text{mult}}$ is conducted after the adjustment in (12), and the formulations of the frame-averaging are expressed as in (21).

Given the frame-averaging is conducted for respective information using their own parameters [20], the objective $S_{fr}$ among the two kinds may satisfy the coherency and remain during the process. While the other $S_{fr}$ is eliminated by destructive interference by incoherency and averaging divider $K$, as described in (21). Eventually, it improves the SNR of the Pseudo-CE even if the acquired signal is adjoined with complex noise. Moreover, we expresses the SNR variation as a function of the number of averaged frames ($K$) in (22).

\[
SNR_1[K][dB] = 20 \cdot \log_{10} \left( \frac{\alpha \cdot S_{fr1}(RMS)}{(\beta \cdot S_{fr2} + N_{\text{AWGN}})(RMS)} \right) \quad (22a)
\]

\[
SNR_2[K][dB] = 20 \cdot \log_{10} \left( \frac{\beta \cdot S_{fr2}(RMS)}{(\alpha \cdot S_{fr1} + N_{\text{AWGN}})(RMS)} \right) \quad (22b)
\]

In addition, Fig. 17 presents the minimum required number of the frames are 154 and 354 in this instance,
and the reconstructed image of $u_{AM}\{S_{fa1}[n, 154]\}$ and $u_{AM}\{S_{fa2}[n, 354]\}$ are subsequently presented in Fig. 18. As presented in Fig. 18, in contrast to the reconstruction from $S_{noisy}$, which includes only single sensitive information, the reconstruction from $S_{mult}$ includes a wavy afterimage. This phenomenon is because the unwanted PCE component is not perfectly eliminated, subsequently inducing a non-ideal effect by the demodulation process. The most simple method of removing the afterimage is increasing the averaging number ($K$); advanced signal-processing techniques can also effectively remove such noise [21].

Furthermore, an SNR-and SSIM-based analysis can be applied to counter the effects of poor electromagnetic propagation environments such as concrete or wooden walls existing in the line of sight between the target device under test (DUT) and antenna aperture. It can determine the duration of acquisition required to achieve a given SNR, provided that the electromagnetic characteristics are modeled, and the path loss of the obstacles is estimated [22], [23].

In this section, we described the methodology for generating the PCE and adhered to the quantitative analysis of the possibility of information reconstruction based on the implemented PCE. Although this study handles a specific frequency band of 5% FBW centered at $(3+2/3)f_p$, the proposed methodology is also applicable to implement the PCE in other frequency bands as well. Moreover, it is noteworthy that the potential of the proposed analysis is not limited to environments with AWGN. It can be easily extended to environments containing various other types of noise, such as other communications as well as other types of EMI interference.

**IV. VERIFICATION**

This section describes the reconstruction of the display information from the actual CE of the HDMI to validate the effectiveness of the proposed methodology. It provides comparisons between reconstructions from the implemented PCE, single frame (or single $k$), and multiple frames to be averaged from the actual CE. To acquire the actual CE from the HDMI, an experiment was conducted in the EMC chamber, as shown in Fig. 19. The experiments are conducted toward
band \((f_c)\) is set as \((3 + 2/3)f_p\). 544.5 MHz, as with the previous sections. Also, it utilizes an RF front-end consists of a log-periodic dipole antenna, a tunable bandpass filter (FBW = 5%), a low-noise amplifier, and a software-defined radio (NI-USRP 2940). Also, there is an auxiliary signal processor to conduct reconstruction from the acquired leakage.

### A. RECONSTRUCTION FROM SINGLE-VDU

Figure 20 presents the reconstructed results of the modeled PCE, actual CE of single and 84 frames-averaged respectively regarding the display information introduced in Fig. 10-(a). The SNR of the received actual CE is estimated as -4.8 dB; frame-averaging improves the SNR to approximately 19.2 dB, which provides a considerably higher amount of information.

![Figure 20](image)

**FIGURE 20:** Result from (a) PCE, (b) single and (c) 84-frame averaged actual CE in accordance with Fig. 10-(a)

Figure 21 presents the reconstructed results of the modeled PCE, actual CE of single and 84 frames-averaged respectively regarding the display information introduced in Fig. 10-(b). The SNR of the received actual CE is estimated as -5.6 dB; frame-averaging improves the SNR by approximately 21.5 dB, providing a considerably higher amount of information.

![Figure 21](image)

**FIGURE 21:** Result from (a) PCE, (b) single and (c) 140-frame averaged actual CE in accordance with Fig. 10-(b)

### B. RECONSTRUCTION FROM DUAL-VDU

This section discusses the case in which two separate VDUs are placed at the same time and place. Figure 22 respectively shows the reconstruction for a single \(k\), targeting the information in Fig. 10-(a) with 88 averaged frames, as well as Fig. 10-(b) with 158 averaged frames.

![Figure 22](image)

**FIGURE 22:** Result from (a) single frame, (b) 84 of averaged frames for Fig. 10-(a) and (c) 158 of averaged frames for Fig. 10-(b)
In the case of Fig 22-(b), the signal strength of Fig. 10-(a) is higher than that of the other (Fig. 10-(b)); hence its reconstruction result is similar to the experiment conducted with a single VDU. On the other hand, as presented in Fig. 22-(c), the weaker signal can be significantly affected in the demodulation process and provides afterimages even though the frame-averaging is conducted. Overall, the experimental results validate the effectiveness of our proposed analysis.

V. CONCLUSION

This paper proposes a quantitative analysis method on the possibility of information reconstruction by modeling EM leakage from the TMDS interface among various SDIs currently used in public. First, to analyze the EM leakage characteristics of the TMDS interface, the signal flow in the HDMI cable is analyzed, and it is revealed that the baseband characteristics of the TMDS interface; the signal flow in the currently used in public. First, to analyze the EM leakage possibility of information reconstruction by modeling EM demodulation process and provides afterimages even though the frame-averaging is conducted. Overall, the experimental results validate the effectiveness of our proposed analysis.

ACKNOWLEDGMENTS

This work was supported by support for standardization and certification of new energy technologies of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Trade, Industry and Energy. (No. 20217301010050)

REFERENCES

[1] G. McGraw, "Software security," in IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83, March-April 2004
[2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in Proc. Cryptographic Hardware Embedded Syst., 2001, pp. 251–261
[3] Y. Hayashi et al., "Evaluation of information leakage from cryptographic hardware via common-mode current", IEICE Trans. Electron., vol. E95-C, no. 6, pp. 1089-1097, 2012
[4] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in Proc. Privacy Enhancing Technologies, pp. 88-107, May 2005.
[5] W. Van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk?", Computers & Security, vol. 4, pp. 269-286, 1985
[6] M.G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays", Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, Dec. 2003.
[7] 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,” in IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 1, pp. 34–42, Feb. 2017
[8] P. De Meulemeester, B. Scheers and G. A. E. Vandenbosch, “A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels,” in IEEE Transactions on Electromagnetic Compatibility, vol. 62, no. 3, pp. 663-672, June 2020
[9] L. Nowosieki, R. Przesmycki and M. Nowosiecki, “Compromising Emanations from VGA and DVI Interface,” in Proc. 2016 Progress in Electromagnetic Research Symposium (PIERS), 2016, pp. 1024-1028
[10] T. Song, Y. Jeong and J. Yook, “Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR,” in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 2 pp. 164-172, April 2015
[11] H. S. Lee, D. H. Choi, K. Sim and J. Yook, “Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment,” in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1098-1106, Aug. 2019
[12] L. J. Cutiona, E. N. Leith, L. J. Porcello and W. E. Vivian, “On the application of coherent optical processing techniques to synthetic-aperture radar,” in Proceedings of the IEEE, vol. 54, no. 8, pp. 1026-1032, Aug. 1966
[13] Jian Li, Guoqing Liu and G. B. Giannakis, “Carrier frequency offset estimation for OFDM-based WLANs,” in IEEE Signal Processing Letters, vol. 8, no. 3, pp. 80-82, March 2001
[14] Video Electronics Standards Association (2013), VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT), Feb, 2013, https://glenwing.github.io/docs/VESA-DMT-1.13.pdf
[15] P. De Meulemeester, B. Scheers and G. A. E. Vandenbosch, “Differential Signaling Compromises Video Information Security Through AM and FM Leakage Emissions,” in IEEE Transactions on Electromagnetic Compatibility, vol. 62, no. 6, pp. 2376-2385, Dec. 2020
[16] F. Eltibol, U. Sarac and I. Erer, “Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system,” in Proc. 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), 2012, pp. 1767-1771
[17] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, “A threat for tablet PCS in public space: Remote visualization of screen images using EM emanation,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2014, pp. 954–965.
[18] 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. Comput., 2010, vol. 768, pp. 132–137.
[19] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004.

FIGURE 22: result from (a) single frame, (b) 84 of averaged frames for Fig. 10-(a) and (c) 158 of averaged frames for Fig. 10-(b) (Cont.)
[20] D. H. Choi, E. Lee and J.-G. Yook, “Reconstruction of Video Information Through Leaked Electromagnetic Waves From Two VDUs Using a Narrow Band-Pass Filter,” in IEEE Access, vol. 10, pp. 40307-40315, 2022.

[21] X. Liu, S. Wang, S. Fu, L. Yuliang, S. Liu and W. Zhou, “An Efficient Collaborative Filtering Method for Image Noise and Artifact Removal,” in IEEE Access, vol. 8, pp. 124158-124171, 2020.

[22] G. Daian, A. Taube, A. Birnboim, et al., “Modeling the dielectric properties of wood”, Wood Sci Technol 40, pp. 237-246, 2006

[23] K. Cho, S. Jo, Y. H. Noh, N. Lee, S Kim and J Yook, “Complex Permittivity Measurements of Steel Fiber-Reinforced Cementitious Composites Using a Free-Space Reflection Method with a Focused Beam Lens Horn Antenna”, Sensors. 2021, 21(23):7789.

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.

DONG-HOON CHOI received the B.S degree in electronic communication engineering from Chonnam National University, Yeosu, South Korea, in 2016. 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.

TAESIK NAM received the B.S degree in electronic communication engineering from Hanbat National University, Daegwon, South Korea, in 2020. He is currently working toward the Ph.D degree in electrical and electronic engineering at Yonsei University, Seoul, Korea. His research interests include the Machine Learning, information recovery, signal processing, wireless communication and autonomous vehicle.

JONG-GWAN YOOK (’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.

***