# Source Estimation of Electromagnetic Information Leakage from Information Devices

Daiya Nagata[1] Ryota Birukawa[1] Yu-ichi Hayashi[2]
Takaaki Mizuki[3] Hideaki Sone[3]

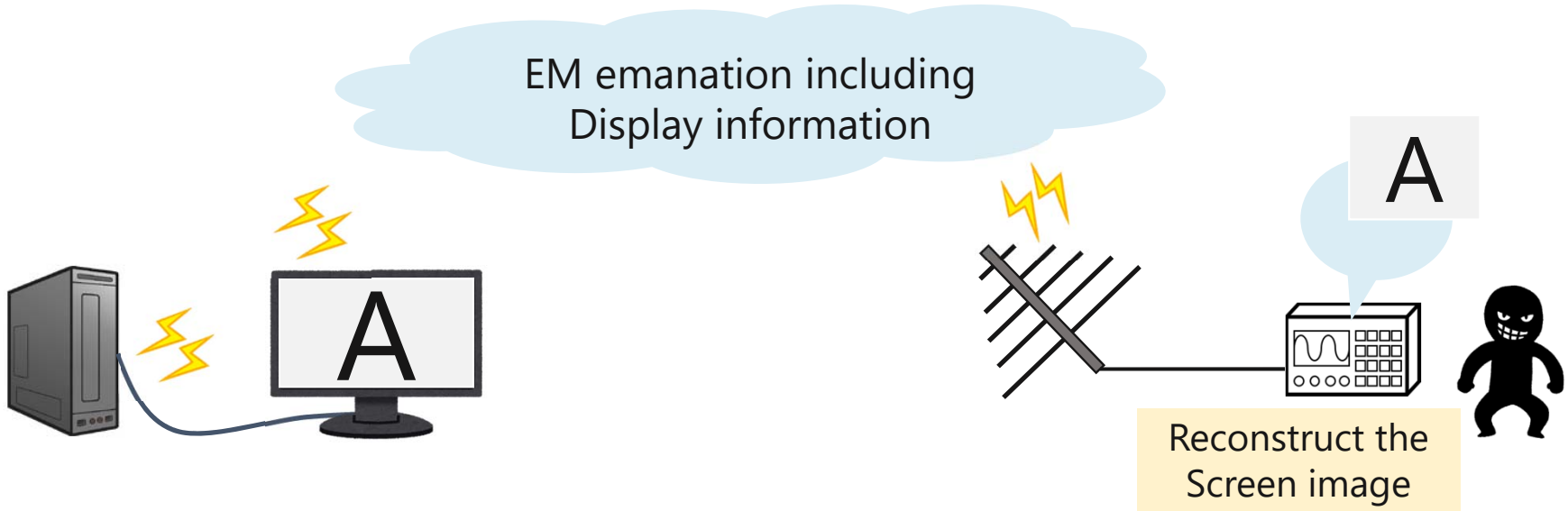
1 Graduate School of Information Sciences, Tohoku University
2 Nara Institute of Science and Technology
3 Cyberscience Center, Tohoku University

# Contents

# Contents

# The threat of EM information leakage from display

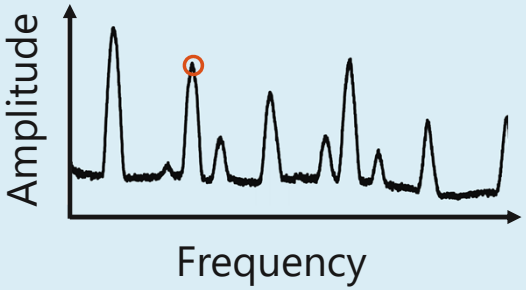
- Achieved by exploiting unintentional electromagnetic (EM) emanation at a specific frequency
- Various information devices have been reported as the targets (desktops, laptops, tablets, etc.)



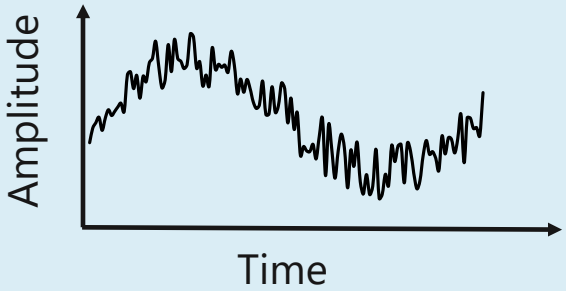
# EM information leakage

1. Observe the EM emanation

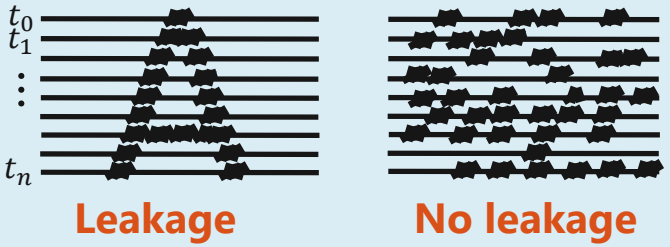
2. Select a frequency




3. Demodulate




4. Reconstruct the screen



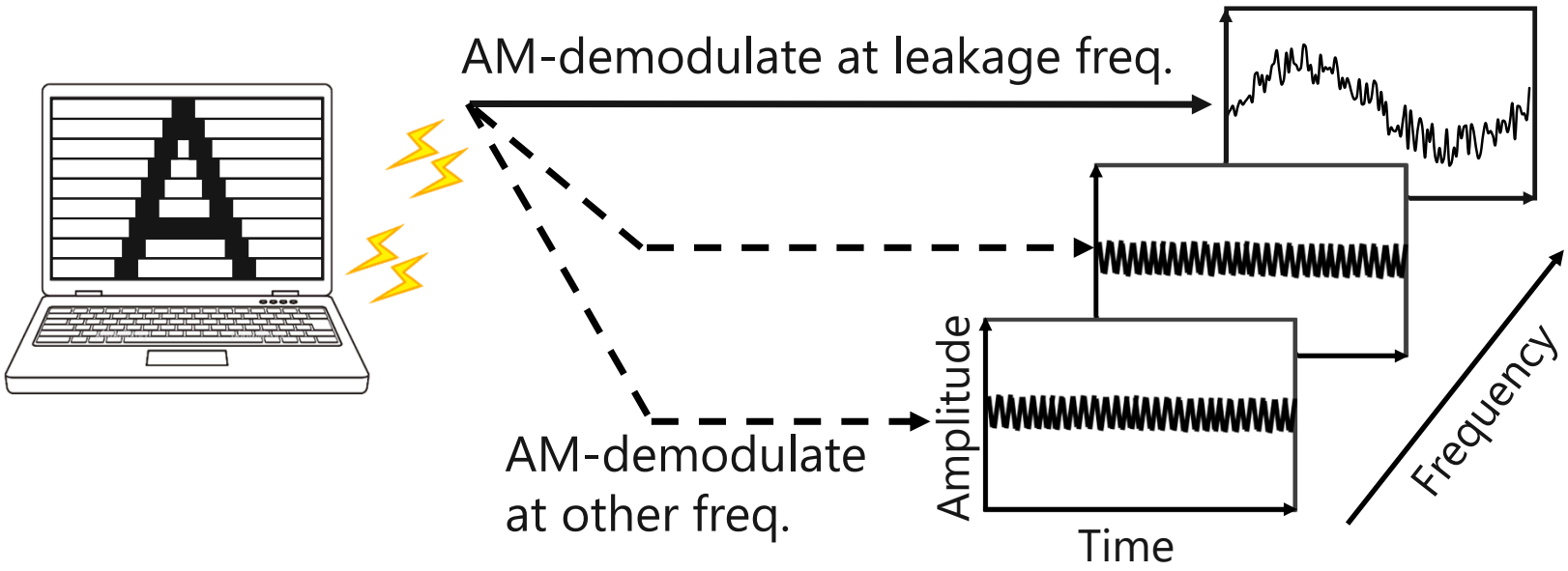
# Purpose

| | |
|---|---|
| **Problems** | Eavesdropping the screen image of a device by exploiting EM emanation<br>EM shielding the device is known as a countermeasure of the EM information leakage<br>→ EM emanation sources should be located to suppress EM emission |
| **Purpose** | Source estimation of EM emanation by measuring the distribution of electromagnetic field at specific frequencies which are determined by estimating leakage frequencies of a tablet and a display monitor |

# Contents

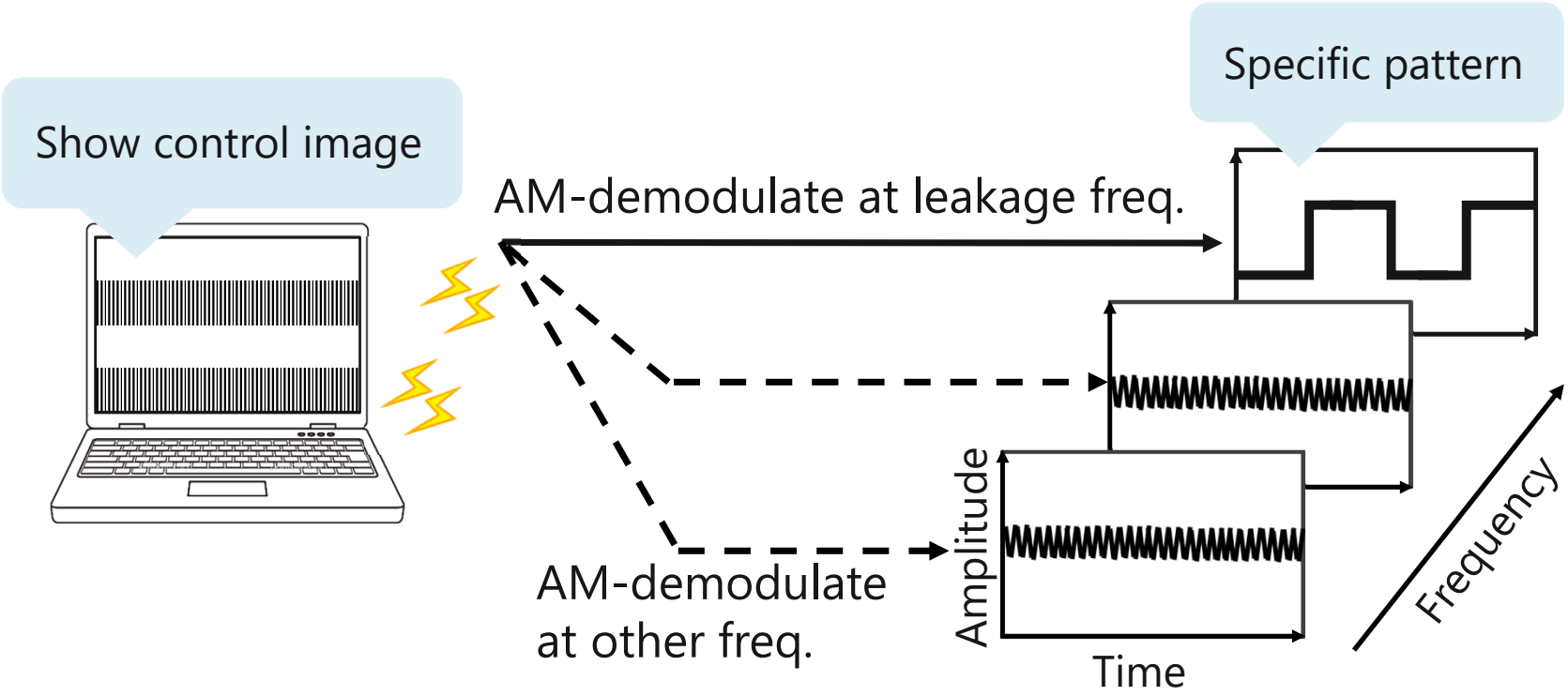
# Previous study | Leakage estimation without screen reconstruction

There is a correlation between the transmission data of the displayed image and the AM-demodulated EM emanation at the leakage freq.



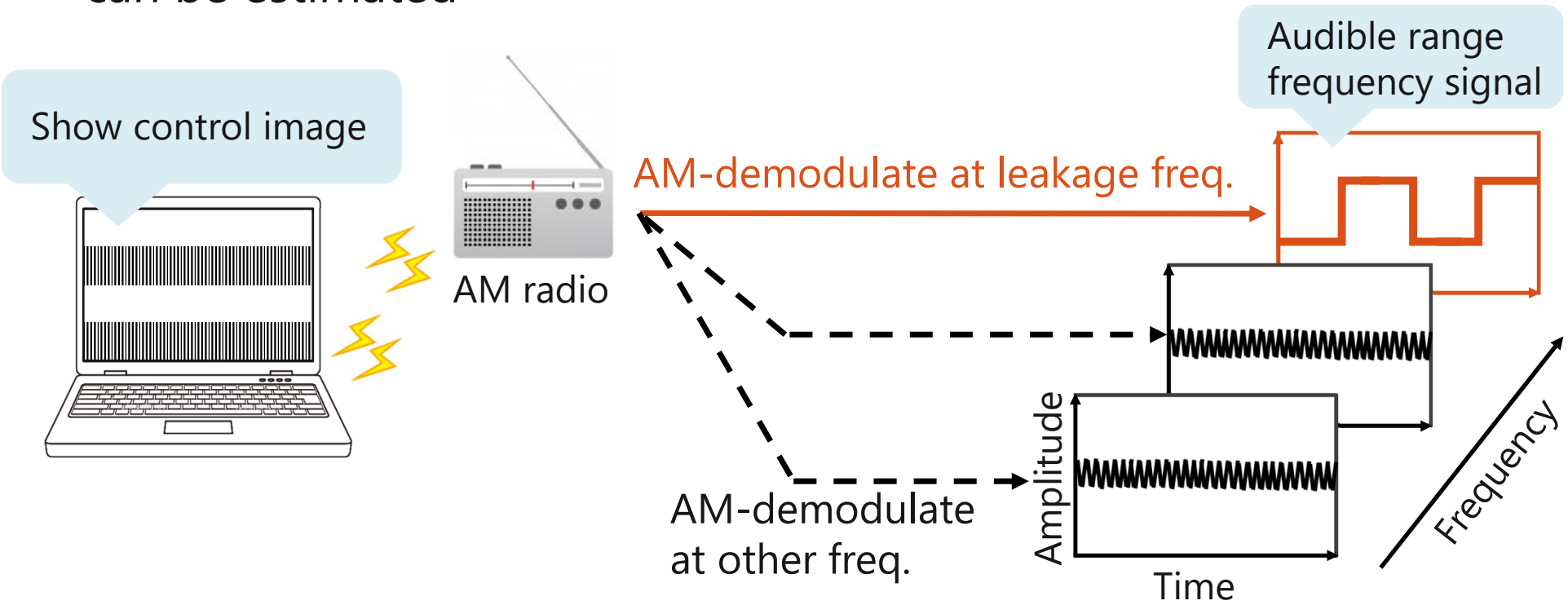
# Previous study | Leakage estimation without screen reconstruction

There is a correlation between the transmission data of the displayed image and the AM-demodulated EM emanation at the leakage freq.



# Previous study | Leakage estimation without screen reconstruction

- The pattern was controlled as an audible frequency range signal
- By detecting this audio with low-cost equipment, the leakage freq. can be estimated



# Mechanism of the EM emanation in digital signal

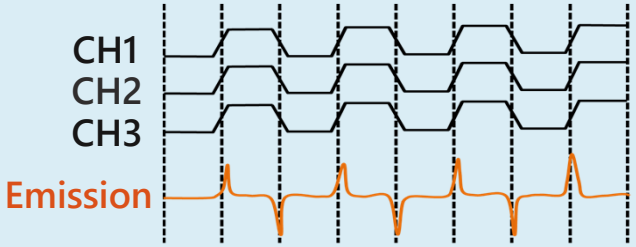
The number of bit inversion affects the EM emanation

The EM emanation depends on the display color

- High emission color

CH1 : 0101010
CH2 : 0101010
CH3 : XXX1010

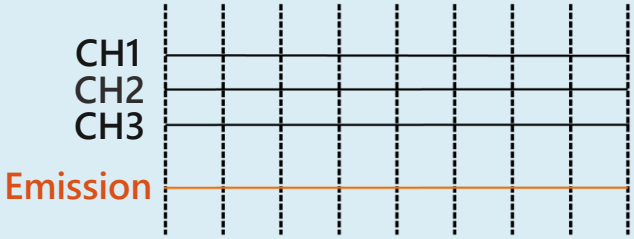
Large emanation occurs by bit inversion




- Low emission color

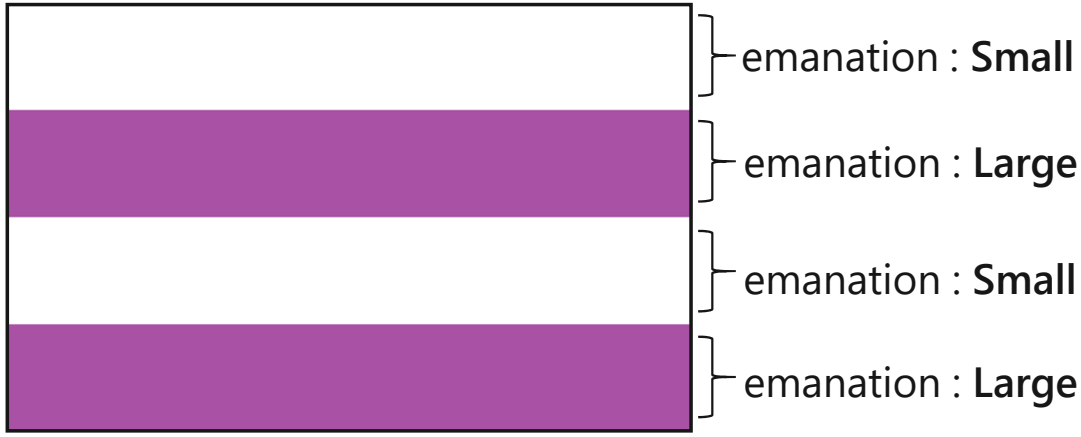
CH1 : 0000000
CH2 : 0000000
CH3 : XXX0000

No emanation occurs




Example of 1 pixel in LVDS

# How the EM emanation be controlled



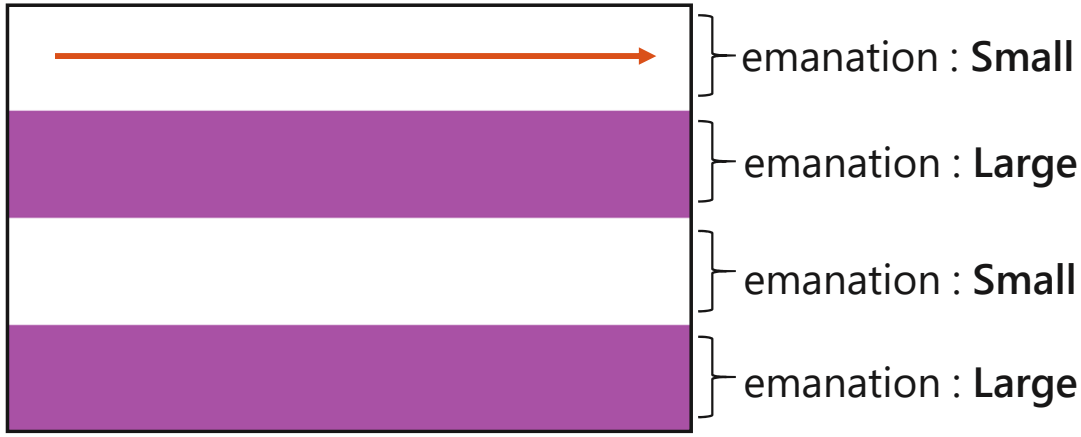

Control image

A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM emanation at leakage freq.


EM emanation

# How the EM emanation be controlled



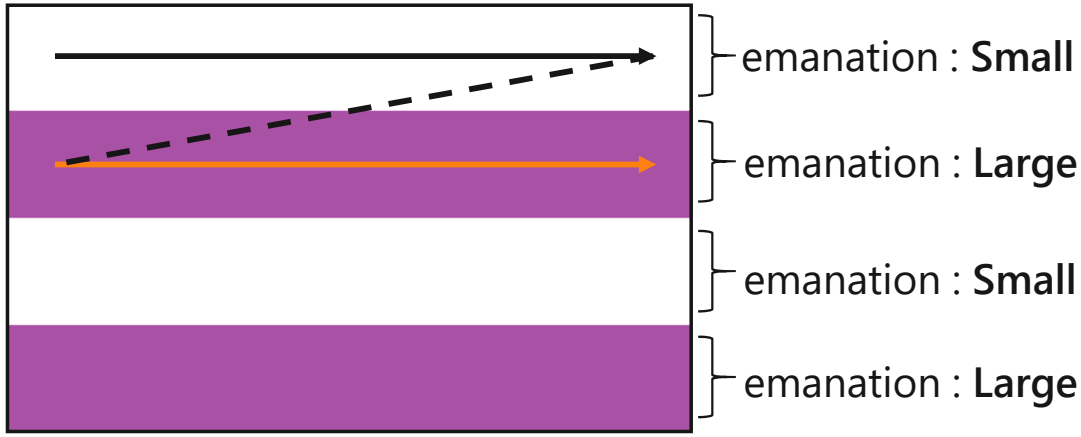

Control image

A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM emanation at leakage freq.


EM emanation

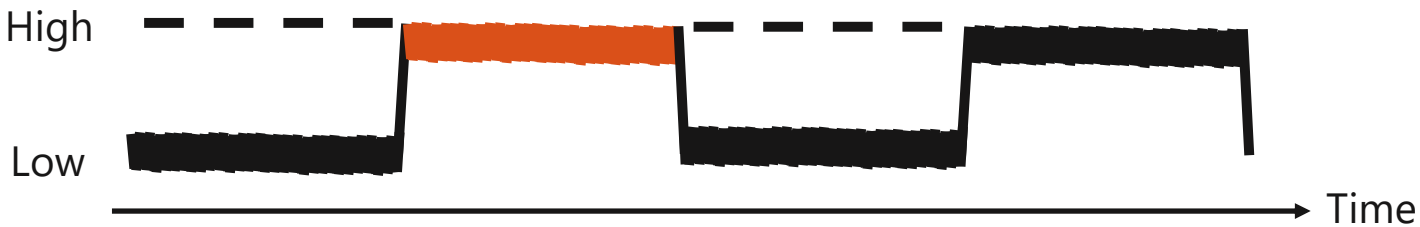
# How the EM emanation be controlled




Control image

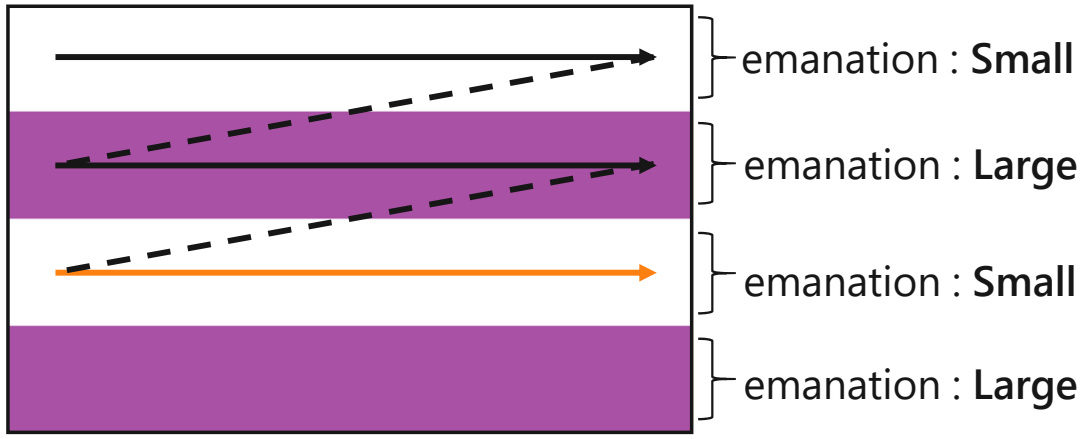
A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM emanation at leakage freq.




EM emanation

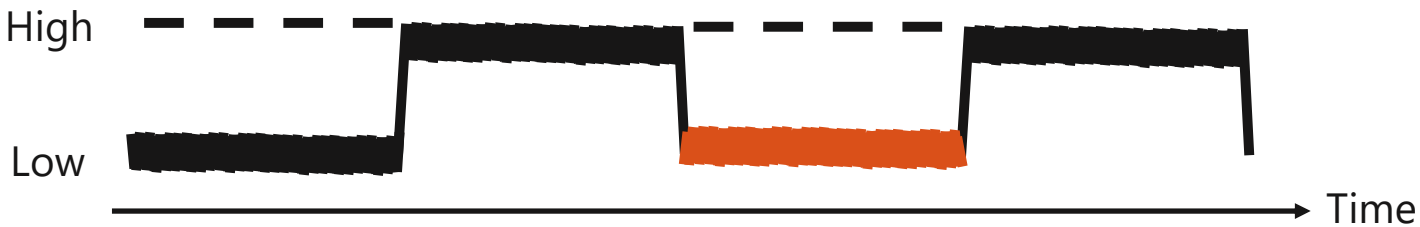
# How the EM emanation be controlled




Control image

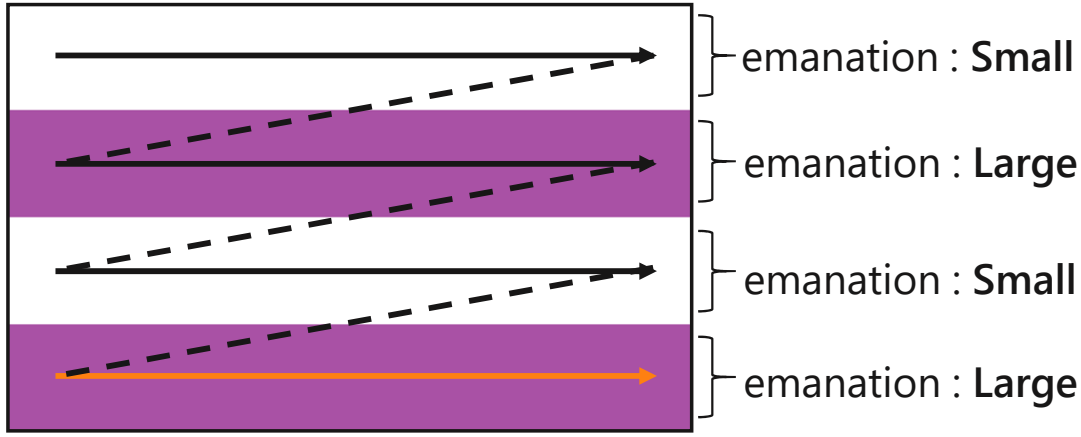
A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM emanation at leakage freq.




EM emanation

# How the EM emanation be controlled



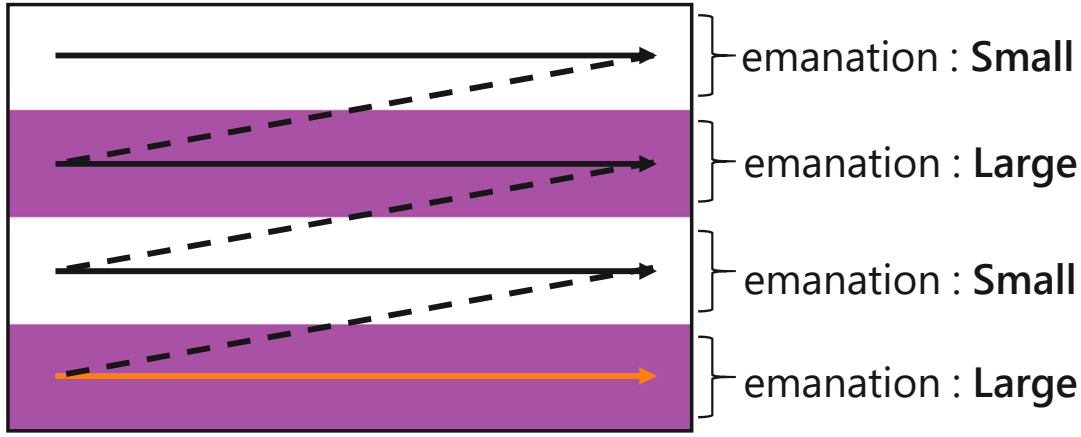

Control image

A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM emanation at leakage freq.


EM emanation

# How the EM emanation be controlled




Control image

A colored section with a large amount of bit inversion is placed below a white section

AM demodulate the EM

$f$ = 2 × Refresh rate

freq.

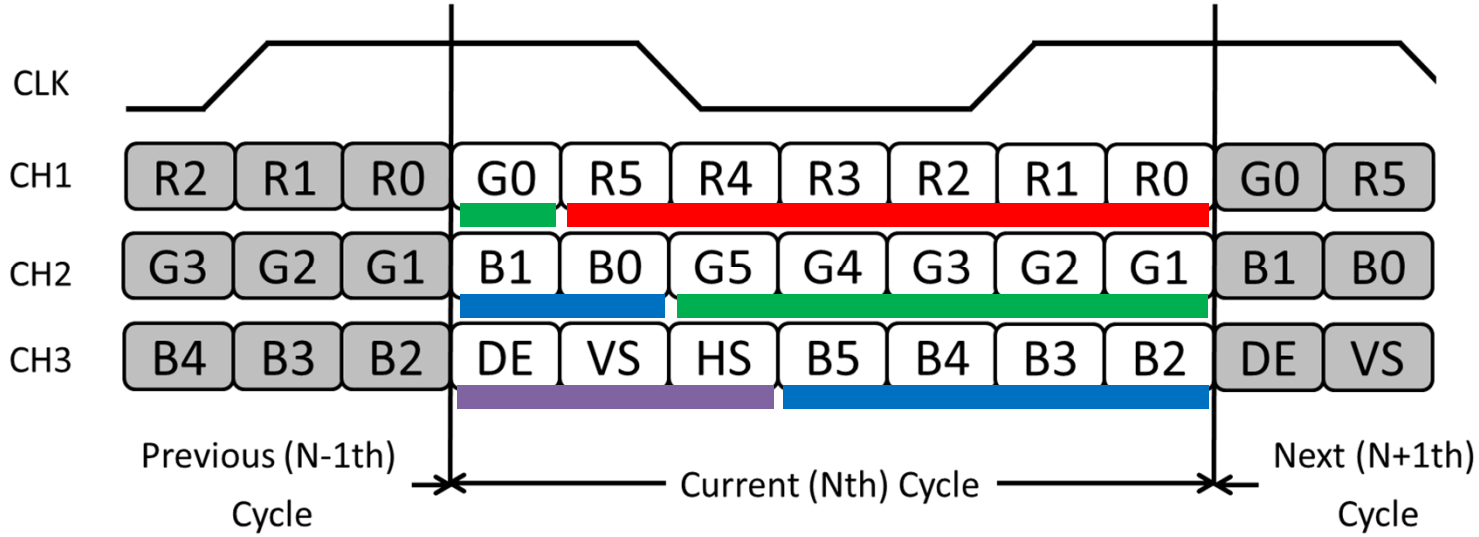

EM emanation

# Contents

# Transmission protocol used in tablets and laptops

## LVDS (Low Voltage Differential Signaling) / FPD-Link

- A physical layer protocol which achieves high-speed data transmission
- RGB pixel data (18bit): Red 6bit, Green 6bit, Blue 6bit
- Synchronization signal (3bit): Data Enable 1bit, Vsync 1bit, Hsync 1bit



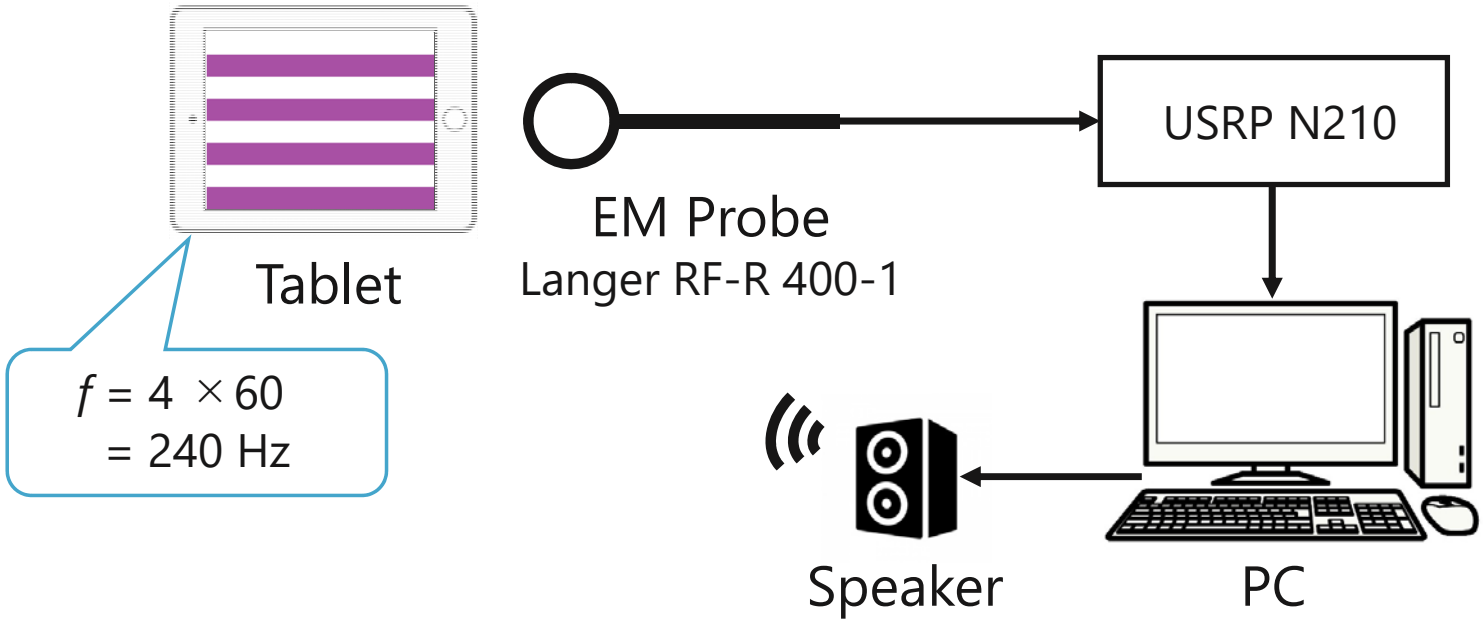

Bit mapping and timing chart of LVDS

# Control image considering the number of bit inversion in LVDS

Control image in LVDS

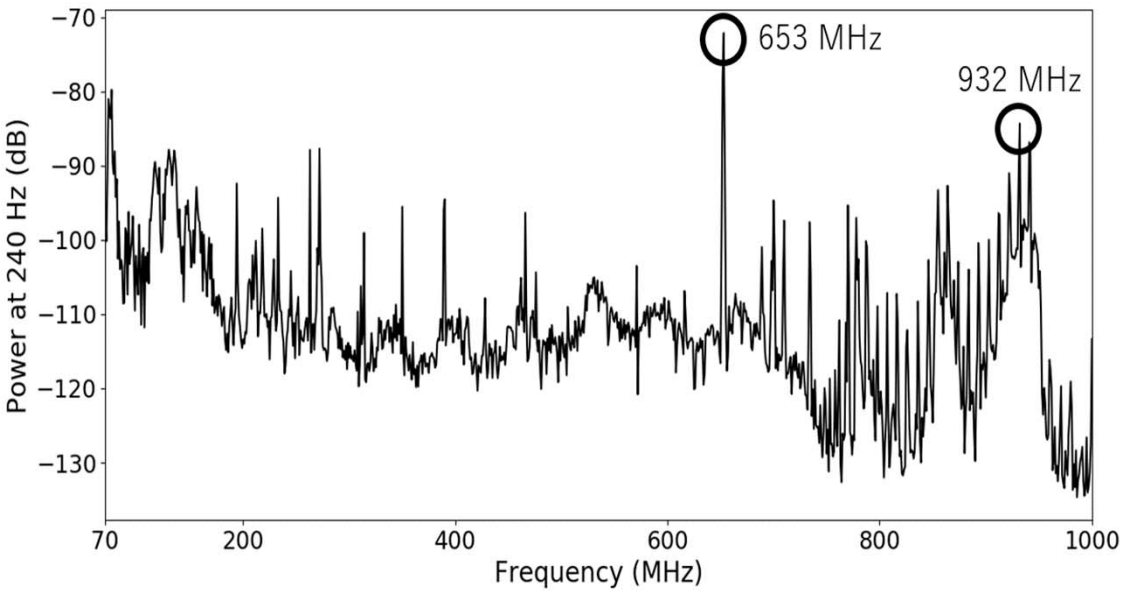
| Displayed color | RGB value | LVDS data | EM emanation |
|---|---|---|---|
| All bits 1 | 255 255 255 | CH1: **1111111**<br>CH2: **1111111**<br>CH3: **XXX1111** | Small |
| Bit inversion for all channels | 168 50 164 | CH1 : **0101010**<br>CH2 : **0101010**<br>CH3 : **XXX1010** | Large |

# Experimental setup




- Control image was displayed on the evaluation target device
- The EM emanation was AM-demodulated from 70 MHz to 1000 MHz
- Amplitude of the power spectrum at 240 Hz of demodulated emanation and audio signal were observed

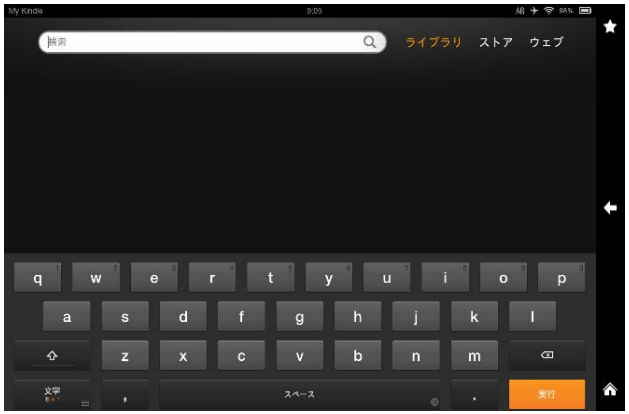
# Measurement results




Power spectrum at 240 Hz of the AM-demodulated EM emanation

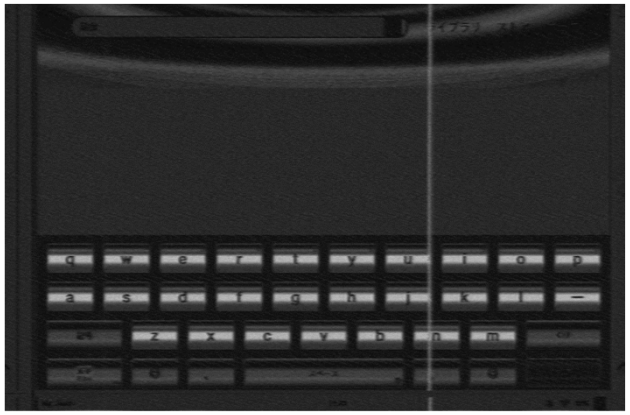
- Information leakage likely occurred at frequencies where high peaks were observed
- 653 MHz and 932 MHz were selected to observe in greater details

# Reconstruction results at each frequency

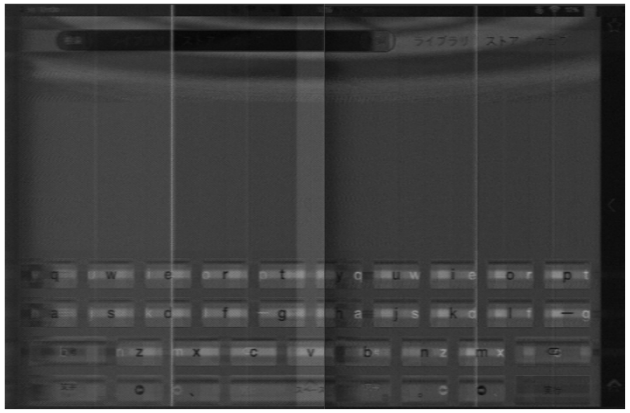



Test image

Both frequencies contain emanated information



653 MHz



932 MHz

# Contents

# TMDS(Transition Minimized Differential Signaling)

- Data transmission protocol used in HDMI/DVI
- 3 channels for R, G and B are converted by 8b/10

**Transmission minimized**

- Translate 8bit to 9bit
- XOR process or XNOR process are applied

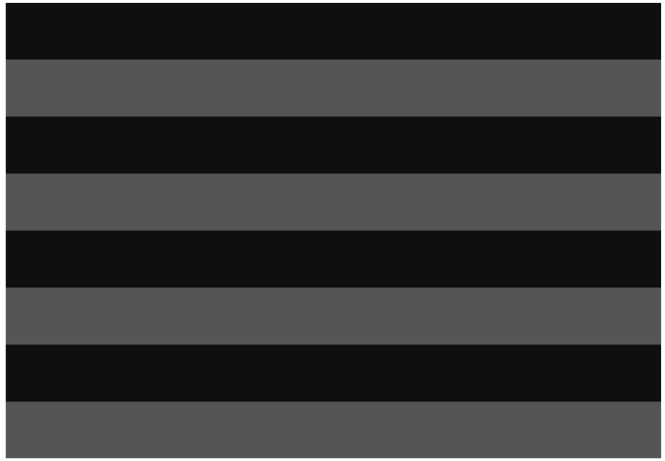
e.g. $55_{16}$: 01010101
→100110011

**DC-Balancing**

- Translate 9bit to 10bit
- Even the same color pixel has different encoding depending on past data
- There are 52 types of conversion that do not depend on past data
- Bit inversion is 2 to 5 times

e.g. 100110011→0100110011

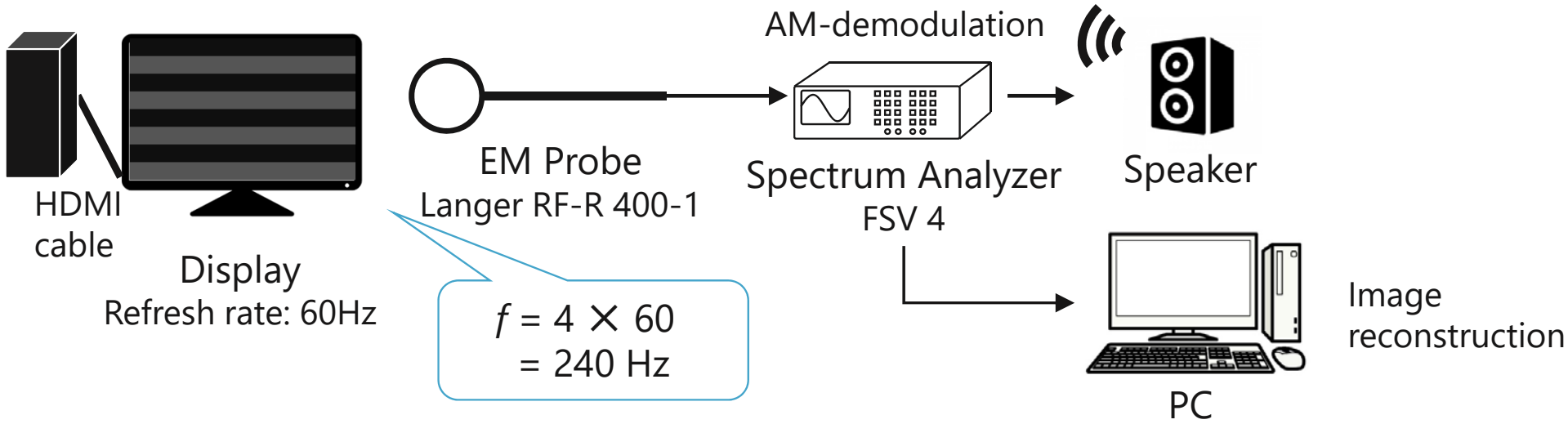
# Control image considering the number of bit inversion in TMDS



Control image in TMDS

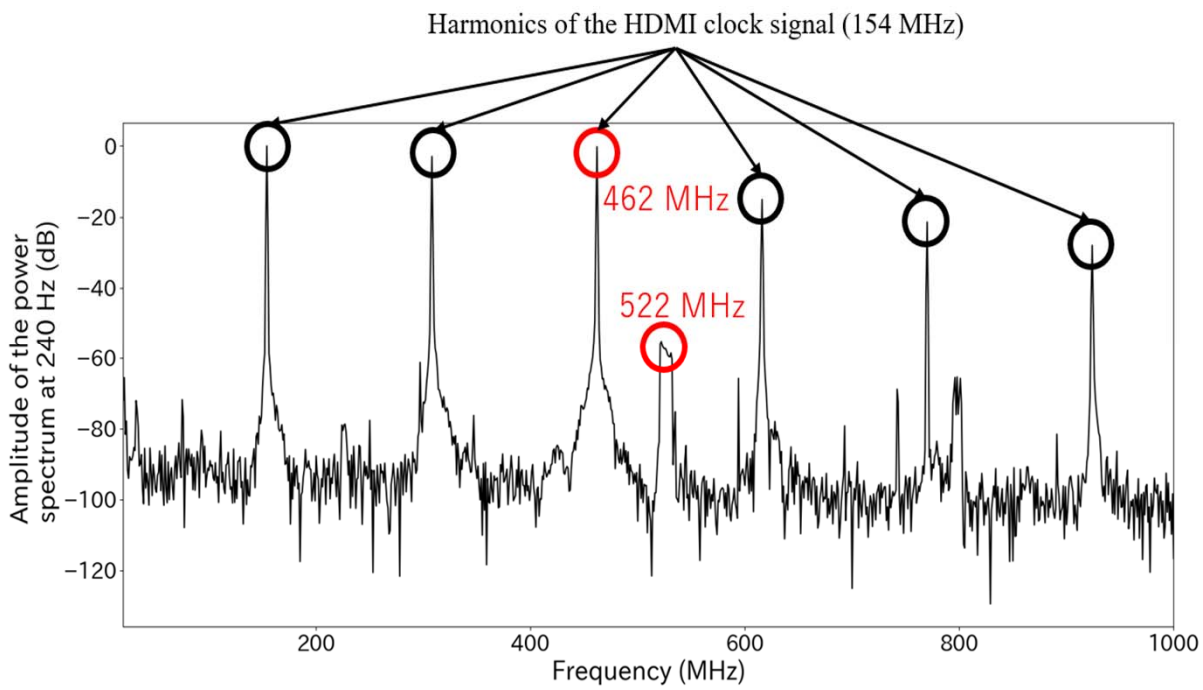
| Displayed color | RGB value | Transmission data | EM emanation |
|---|---|---|---|
| **Bit inversion every 2 bits for all channels** | 16 16 16 | CH1 : **0111110000**<br>CH2 : **0111110000**<br>CH3 : **0111110000** | **Small** |
| **Bit inversion every 5 bits for all channels** | 85 85 85 | CH1 : **0100110011**<br>CH2 : **0100110011**<br>CH3 : **0100110011** | **Large** |

# Experiment Setup




- Control image was displayed on the display monitor connected by HDMI cable
- The EM emanation was AM-demodulated from 20 MHz to 1000 MHz
- Amplitude of the power spectrum at 240 Hz of demodulated emanation and audio signal were observed

# Measurement result




Power spectrum at 240 Hz of the AM-demodulated EM emanation

- Information leakage likely occurred at frequencies with high peaks
- Harmonics of the HDMI clock signal(154 MHz) are high emanation
- 462MHz, 522MHz were selected to observe in greater details

# Reconstruction results at each frequency

The quick brown fox jumps over the lazy dog.

The quick brown fox jumps over the lazy dog.

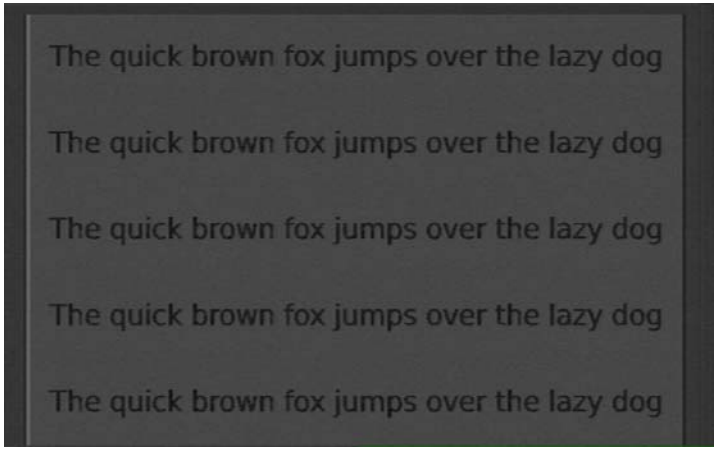
The quick brown fox jumps over the lazy dog.

The quick brown fox jumps over the lazy dog.

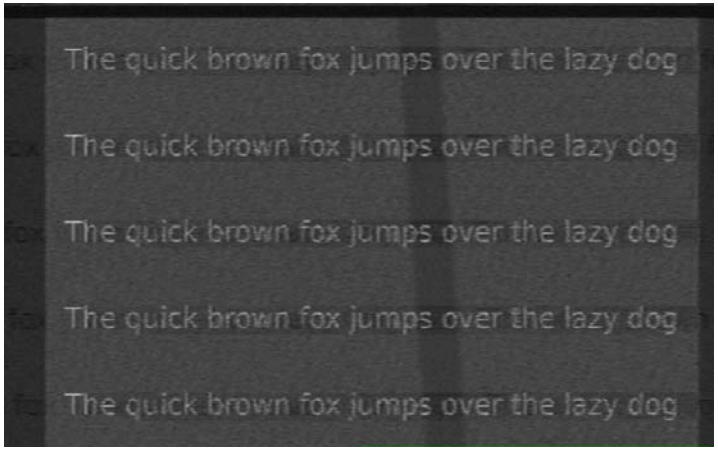
The quick brown fox jumps over the lazy dog.

Test image

Both frequencies contain emanated information



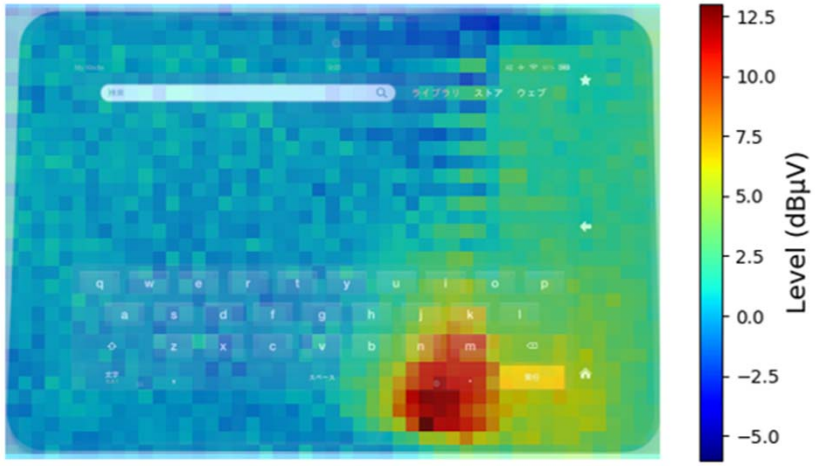

462 MHz



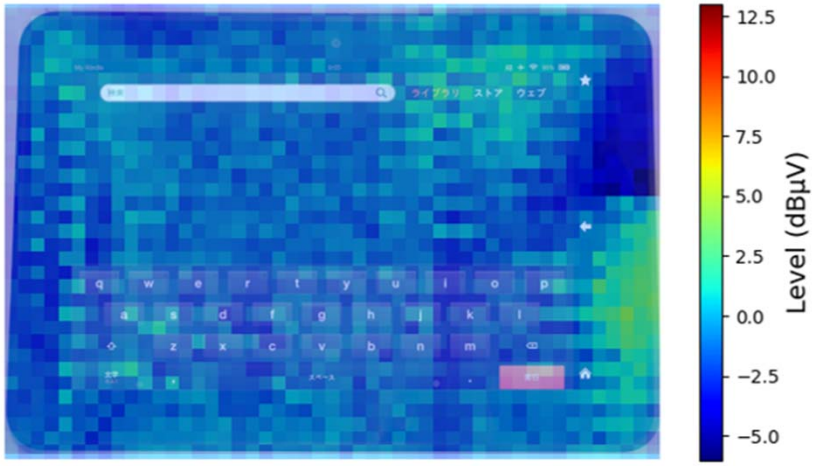

522 MHz

## Contents

# Estimating EM emanation sources of the tablet




Distribution of EM field at 653 MHz

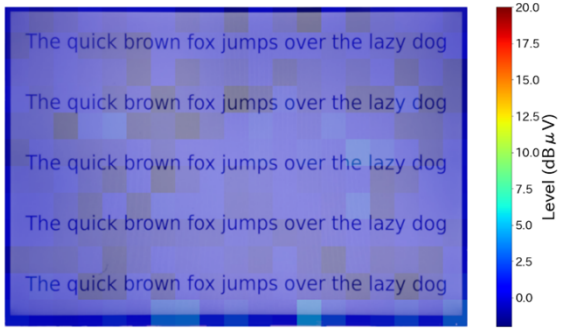



Distribution of EM field at 932 MHz

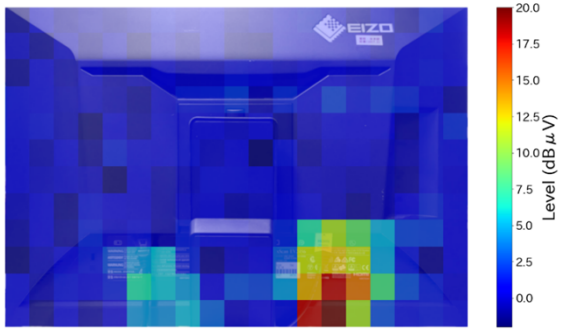
- The EM emanation source of 653MHz is the cable which connects LCD panel to the board of the tablet
- The EM emanation source of 932MHz is the edge of the screen

→ Confirmed multiple EM emanation sources in the tablet

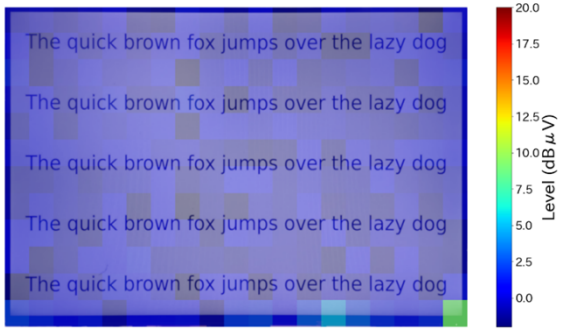
# Estimating EM emanation sources in the display monitor



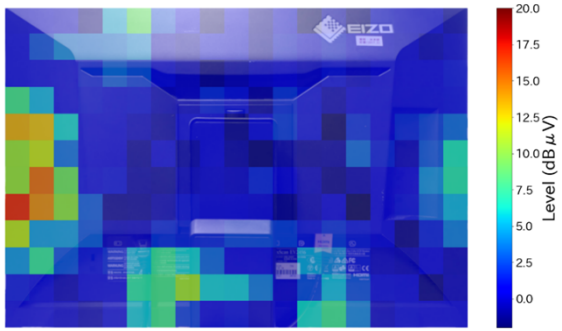

462MHz: Front




462MHz: Back




522 MHz: Front




522MHz: Back

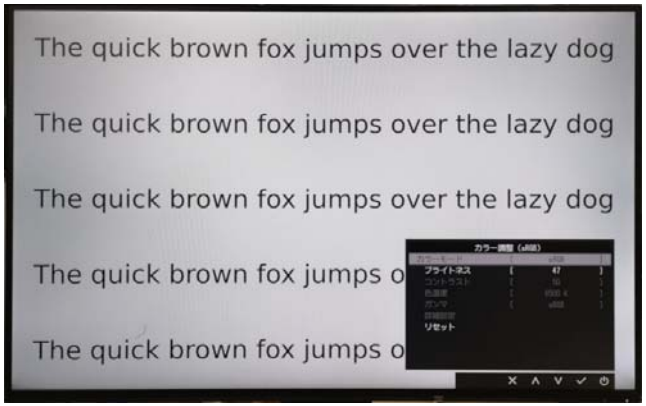
- The EM emanation sources are HDMI cable, power supply wiring at 462 MHz
- The EM emanation sources are the edge of the screen at 522 MHz

→ 462 MHz and 522 MHz have different emanation sources

# Reconstruction results at displaying the display setting screen

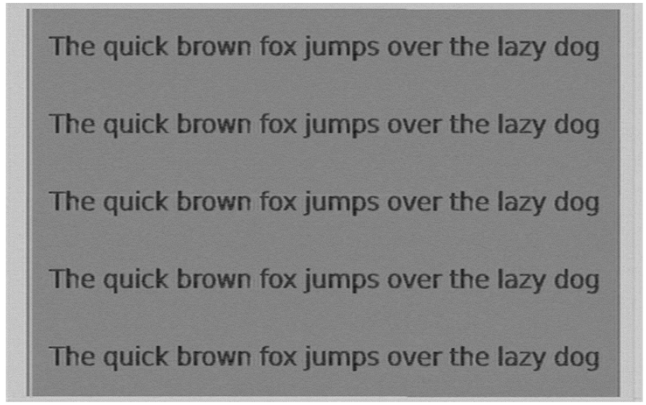
The display setting window image is overwritten on the original screen image signal transmitted in HDMI cable

→ Different reconstruction image means their leakage frequency have different sources which are before and after the setting screen is overwritten

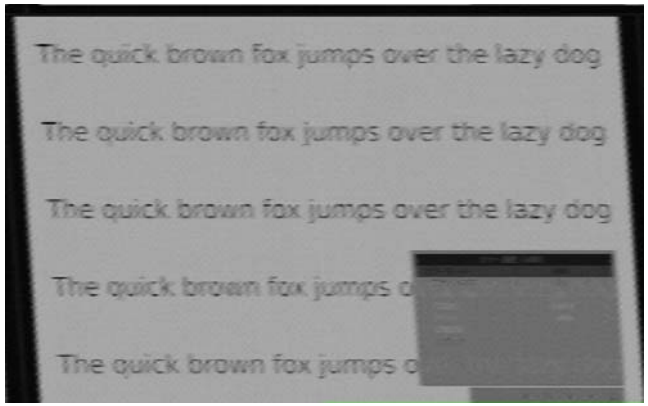



Test image

Reconstructed image




462 MHz




522 MHz

# Contents

# Conclusion

| | |
|---|---|
| **Background** | EM emanation sources should be located to suppress EM emanation |
| **Purpose** | Propose a new method of source estimation of EM emanation by measuring the distribution of electromagnetic field at specific frequencies which are determined by estimating leakage frequencies of a tablet and a display monitor |

| | |
|---|---|
| **Conclusion** | A new method to estimate source of EM emanation is proposed<br><br>Multiple EM emanation sources should be taken into account to prevent EM information leakage from devices |

Supported by JSPS KAKENHI 17H01751