creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

공학박사 학위논문

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATION AND ITS RECONSTRUCTION

누설전자파를 위한 방사 보안 레벨 및 신호 복원

2013년 8월

서울대학교 대학원

Department of Electrical Engineering

Lee Hee-Kyung

공학박사 학위논문

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

누설전자파를 위한 방사 보안 레벨 및 신호 복원

2013년 8월

서울대학교 대학원

Department of Electrical Engineering

Lee Hee-Kyung

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

지도 교수 김 성 철

이 논문을 공학박사 학위논문으로 제출함

2013년 8월

서울대학교 대학원

전기, 컴퓨터공학부

이 희 경

이희경의 박사 학위논문을 인준함

2013년 8월

위 원 장 남 상 욱 (인)

부위원장 김 성 철 (인)

위 원 김 남 수 (인)

위 원 이 종 호 (인)

위 원 김 용 화 (인)

Abstract

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

LEE HEE-KYUNG
Department of Electrical Engineering and Computer Science
The Graduate School
Seoul National University

In this dissertation, reconstruction of electromagnetic emanation security (EMSEC)-channel information for video display units and printer are reconstructed using the averaging technique and proposed adaptive deringing filter. Also, emission security limits are proposed based on the analysis of the indoor EMSEC-channel. An emitted waveform from equipment which manages the important information can be detected and restored intentionally using the sensitive antenna and high performance receiver. These documents related to the EMSEC have classified by high confidentiality so that these are prohibited to publish by military organization. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary.

Firstly, we try to identify the exact a signal characteristics and the frequency components to measure and analyze the spectrum of electromagnetic waves which are contained information on personal computer (PC) and printer. The target devices are the desktop, laptop and laser printer which is generally used in the domestic offices in this study. The printer processed a large amount of information for a short period of time, there may be leaked the information in this process. To verify the leakage of electromagnetic spectrum that contains information, we measure and analyze the whole spectrum from 100 MHz to 1000 MHz.

Secondly, we represent how to build the EMSEC-system and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and video display unit (VDU) of PC. The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, resolution bandwidth (RBW) of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system. Whereas image restoration algorithm for EMSEC system as post-processing is a portion corresponding to the software of EMSEC system.

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective

and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system. But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic compromising emanations need to be considered in order to establish emission security limits. In addition to, we propose the adaptive deringing filter to reconstruct the EMSEC- channel information from PC and printer. We can obtain that the minimum peak signal-to-noise ratio (*PSNR*) enhancement is 2 and maximum *PSNR* enhancement is 10 compared with the original reconstructed image.

Next, we perform the EMSEC-channel measurements in the 100–1000 MHz frequency bands. Second, we analyze the pathloss characteristics of the indoor EMSEC-channel based on these measurements. We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). Also, the pathloss exponent value have a range from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with propagation environments.

Through this EMSEC-channel analysis, we affirm that the TRA, which is one of the key parameters for determining the security limits for compromising emanations, follows the Rician distribution. However, previous work assumed that radio attenuations would have constant values. We found that the TRA does not show significant differences depending on the frequency bands and

has the following range depending on the environment, 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4, and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.

Based on the experimental results of this study, we propose security limits on periodic as well as aperiodic EMSEC-channel information. The proposed security limits on compromising emanations are classified into two levels according to the TRA and the level of required confidentiality. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. And periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 700-1000 MHz, respectively.

Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits. We can then compare our security limits with other security limits and existing civil and military EMC standards.

Future works may include characterization and reconstruction of FAX, smartcard and other electronics. And it is need to EMSEC-channel analysis in more complex environments.

Keywords: Compromising emanation (CE), Electromagnetic Emanation security (EMSEC), Channel analysis, Rician distribution

Student Number: 2006-30856

Contents

List of Tables

List of Figures

Chapter 1. Introduction

The use of information and communication devices has raised over the years as accelerating the information age. Electronic devices has the convenient that can be handled quickly and easily, also has the risk of leakage by electromagnetic radiation which occurs when the data communication at the same time.

Such phenomena are referred to as compromising emanations (CEs) or electromagnetic emanation security (EMSEC) [1]. Information leakage from electronic equipment is achieved through the following path. Electronic equipment includes complex electronic circuitry inside. Within these circuits, electronic components such as central processing unit (CPU), memory, and oscillator component, and each part is built are connected by wires. The exchange of information between the wires, it is shown that the electromagnetic leakage occurs in this process. Leakage of electromagnetic waves that are generated by the baseband signal that is caused by a short rise time and falling time of the transients and harmonic components will have the same frequency components of the original signal. Therefore, electromagnetic waves were collected by a high-sensitivity receiver, which is also able to reconstruct the original signal using a simple signal processing process. In addition, the larger the size of the signal and the far the radiation of the electromagnetic. It is important to prevent equipment that is handling confidential information from emitting such unintentional electromagnetic

radiation.

We assumed that the location between the target information technology (IT) device and the antenna for eavesdropping is a communication channel [2], it is defined by EMSEC-channel. In addition, we regarded that the EMSEC-channel analysis to mean the analysis of the electromagnetic leakage signals from the electronic devices and EMSEC-channel attack is s any attack based on information gained intentionally due to unintentional electromagnetic radiation particularly in equipment that is handling important information. All electronic devices unintentionally radiate information-bearing electromagnetic waves, which is called EMSEC-channel information.

While important documents related to these compromising emanations have been withheld from the public by military organizations, basic information about these emanations has been declassified by the National Security Agency (NSA) [3]. However, information on the actual security limits and the test procedures used to determine those limits have been omitted from published versions, and some declassified documents cited only terminology and the widely known electromagnetic compatibility (EMC) test [4, 5]. In addition, there exist differences in test procedures, the type of detector used, and frequency ranges between the civilian and military EMC standards and security limits for compromising emanations [6]. Therefore, civilian and military EMC standards related to IT devices are unsuitable for emission security purposes [6, 7]. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary.

In order to take countermeasures to prevent information leakage due to electromagnetic information leakage will be preceded by a study about what frequency bands are weak at eavesdropping and some extent the level of information leakage. That is, to raise reasonable countermeasures on the based on the information about the leaked electromagnetic frequency range and the size of the signal leakage. Therefore, we measured and analyzed the electromagnetic spectrum of general IT and communication devices to identify the common characteristics of the leakage radiation leakage.

1.1 Historic background and previous work

Since at least the early 1960s, it has been known to military organizations that computer generate electromagnetic radiation that not only interferes with radio reception, but also leaks information about the data being processed. It has known as compromising emanations or Transient ElectroMagnetic Pluse STandard (TEMPEST) radiation, the unintentional electromagnetic broadcast of data has been a significant concern in sensitive military and diplomatic computer applications. TEMPEST, referred originally to a classified by US government program aimed at such EMSEC problems at developing protection standards. It has since then become a synonym for compromising emanations.

National compromising emanations test standards “NAG1A” and “FS22” is defined firstly by the US government in the 1950s and 1960s [8]. “National Communications Security Information Memorandum 5100: Compromising

Emanations Laboratory Test Standard, Electromagnetics" is revised in 1970 and a later version. "NACSIM 5100A" was defined in 1981. The names of the standards keep changing. "NSTISSAM TEMPEST/1-92" appears to be the current incarnation, of which extracts were declassified in 1999 [3]. However, the released parts reveal mostly only material that can also be found in the open computing, security, and EMC literature while the actual emanation limits, test procedures, and even definitions of some terms remain classified as military secrets. NATO equivalent "AMSG 720B", still classified documents and were therefore not accessible to the author [9, 10].

Electromagnetic radiation as a computer security risk was mentioned in the open literature as early as 1966 [11, 12]. But there is any kind of technical details on specific risks and eavesdropping techniques. The concept was brought to the attention of the broader public by a 1985 paper [12] and a 5-minute TV demonstration on the BBC program, in which van Eck demonstrated that the screen content of a video display unit (VDU) could be recovered at a distance using low cost home built equipment.

The most popular form of portable cryptographic module is the smartcard [13], a credit-card is shaped plastic card with embedded microcontroller. The type interfaces are either five electrical surface contacts for power supply, reset, ground, clock, and a bi-directional serial port or an induction loop. Research interest in compromising emanations from smartcards increased significantly when Kocher, Jaffe, and Jun [14] demonstrated the power analysis of high-frequency current fluctuations with cryptanalytic techniques on block ciphers. In their Differential Power Analysis attack, they

demonstrated the reconstruction of DES sub-key bits merely from access to a number of known plain or cipher texts, the corresponding power-line current curves and knowledge of the cipher algorithm being used. They showed that it is feasible to evaluate power-line information without prior reverse engineering of the low-level design of the executed software and that it is instead sufficient to look for correlations with single bits in intermediate results of the executed algorithm. The correlation process takes care of locating the specific machine instructions that leak the compromising energy. A number of improvements of the attack, attacks on other algorithms and countermeasure methods have been published since then [15, 16], including variants that measure magnetic-field fluctuations above the chip surface [17-20], as well as an attack on an SSL accelerator module inside a closed server from 5 m distance [21].

Several researchers have reported on electromagnetic compromising emanations from video displays [7], computer keyboards [22], and printers [23]. Sun [24] simulated the simple channel transfer function (CTF) of compromising emanations with a commonly used two-ray Rayleigh fading model. However, this model is too simple to reflect a realistically complex environment, and may give rise to some discrepancies between simulation results and real measurements. ITU-T SG5 [1] reported on the test methods and provided a guideline against information leaks through unintentional electromagnetic emissions. Kuhn [7] discussed security limit on video signals as compromising emanation. Although radio attenuation fluctuates according to the environment and distance between the transmitter (TX) and the receiver

(RX), these previous works [1, 7, 24, 25] assumed that the radio attenuations are constant in order to obtain security limit and guide test method.

1.2 Motivation and scope

In our study, we focused on establishing the emission security limits for the compromising emanations in indoor environments. Several researchers have been reported the dominant leakage frequency bands for various electronic devices [2, 7, 22, 23, 25]. Table 1 shows that the leakage frequencies have the range from 105 MHz to 950 MHz for several types of electronic equipment. Accordingly, we selected from 100 MHz to 1000 MHz in all the frequency bands because the compromising frequency bands are different from the confidential signals and the hidden antennas in device.

Table 1. Leaked frequencies of various electronic equipment types

Frequency (MHz)	Equipment	Reference
105–165	PS/2, USB and Wireless Keyboard	[22]
328.3	Laser printer	[23]
285, 324, 350, 648	Toshiba440 laptop	[7]
292, 480, 700, 740	Dell D1025HE monitor	
310–340, 440–475,	SONY VAIO PCG	[2]
775–810, 910–950	personal computer	

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). TRA is defined as the sum of all types of radio attenuations such as free space loss

and additional radiation pathloss in the environment. The expected noise level and attenuation values are random variables that, in the absence of better data, have to be modelled as being normally distributed with some mean and variance determined from the statistical evaluation of a large number of measurements in various indoor environments [7].

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system [2, 7, 25].

But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic-compromising emanations need to be considered in order to establish emission security limits. Based on the experimental results of this study, we propose security limits on periodic as well as aperiodic EMSEC-channel information. The proposed seculity limits on compromising emanations are classified into two levels according to the TRA and the level of required confidentiality. We can then compare our security limits with other security limits and existing civil and military EMC standards.

This dissertation is organized as follows: In Chapter 2, we investigate the characteristics EMSEC-channel information and detecet the EMSEC leaked freuqency band from VDUs and printer. In Chapter 3, detected EMSEC-channel information is reconstructed using the averaging technique and proposed the adpative deringing filter. In Chapter 4, we present the indoor EMSEC-channel measurement for compromising emanation on 100–1000 MHz. Also, we analyze the pathloss characteristics of indoor EMSEC-channel on the basis of experimental data. In Chapter 5, we find the random distribution of TRA and propose periodic and aperiodic emission security limits based on the 90 % TRA confidence level. In brief, we show the comparison between the proposed emission security limits and other security limits and EMC standards. Finally, in Section 6, we present our conclusions.

Chapter 2. Detection of Compromising Emanations

2.1 Introduction

The PC and Printer are the most frequently used IT devices around us. It is well known that the risk of information leakage by the leakage electromagnetic wave emitted from the VDU of PC in many researches. In case of PC, it is urgently needed to countermeasure which is possible for detection and reconstruction of important information from PC a long distance particularly.

We try to identify the exact a signal characteristics and the frequency components to measure and analyze the spectrum of electromagnetic waves which are contained information on PC. The target devices are the desktop and laptop which is generally used in the domestic offices in this study.

The printer processed a large amount of information for a short period of time, there may be leaked the information in this process. To verify the leakage of electromagnetic spectrum that contains information, we measure and analyze the whole spectrum.

In this study, only the first laser printer, to the parallel communication in the most widely used. Printer can be divided by the page printer and line printer depending on the printing method. The page printer refers to a laser printer to print the data you want to print a page-by-page. On the other hand,

line printers are dot matrix printers and inkjet printers to print line-by-line. According how to communicate with a PC, printer can be divided into parallel communication printer and serial communication printer, too. In this paper, the laser printer which are most widely used the parallel communication were included.

2.2 Compromising Emanations from Video Display Units

Firstly, we identify the basic theory of the VDU signal transmission arising from internal and external to infer the characteristics of electromagnetic waves caused by the leakage before measuring the leakage electromagnetic spectrum that occurs on PC.

2.2.1. Property of Video Display Units

A. VDU signal process

Figure 2.1 is shown on the process which VDU signal is generated the display by a PC monitor.

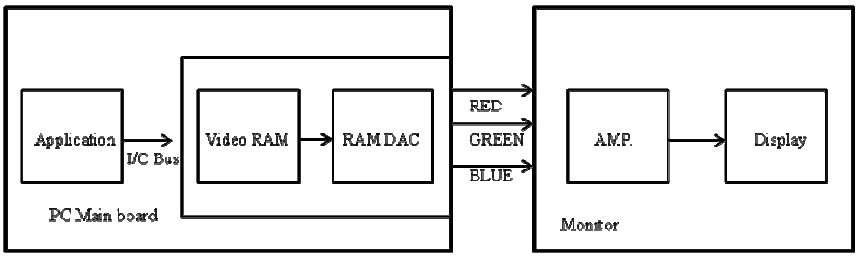


Figure 2.1 VDU Signal Process

(1) Signal process of PC

① The video data is generated by an application program

② Generated video data is converted in the form of video output to the monitor via video card.

③ Red, green, blue color data with the synchronization signal will be sent to the monitor at the same time.

(2) Signal process of monitor

① Received analog signal from the PC is changed adaptively and sent to the cathode ray tube (CRT) via the Main Board.

② Analog data is transmitted to the three electron guns at the rear of the CRT via main Board.

B. Characteristics of transmission signal

It is expected to occur mainly electromagnetic leakage in the process signal amplification to fit inside the CRT and emission part of the PC and the monitor connection.

2.2.2. Leakage path of Video Display Units

A. Signal leakage causes

Leakage electromagnetic waveform occurs in PC clock oscillator, Digital ICs, switching power, and the electromagnetic waves that occur on the inside of the unit flows through the input/output (I/O) cables, power lines, or PCB. Conducted signal is radiated into free space through PCB that acts as an

antenna or power line cable, I/O signal. It mainly takes place radiation where the change in impedance such as the power line or PCB, I / O cable and the junction of the wires or connections.

B. Signal leakage path

Leakage electromagnetic waveform from the PC, monitor and peripheral devices conducted and radiated directly or indirectly external signal lines, ground or power lines, etc.

(1) Desktop

Desktop is connected to longer cable and more many cables comparing Laptop. Whereas liquid crystal display (LCD) uses the characteristics of the electric field along the direction of the change in the molecular arrangement of liquid crystal using low voltage signal, CRT is amplified by the large voltage causing the electron beam from the electron gun emitting a fluorescent screen. Therefore, electromagnetic waves emitted from CRT will appear larger than the LCD monitor.

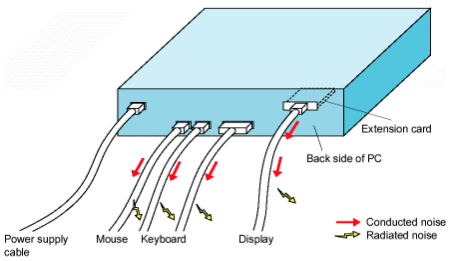


Figure 2.2 Desktop signal leakage paths

(2) Laptop

Electromagnetic waveform from the body of the laptop and the cables is radiated and the cable between the LCD panel and the laptop body are emitted. The laptop operates as a high-speed signal. Because the case is made of plastic, it does not have the shielding effect and is radiated a high level of electromagnetic waveform from the computer generally.

Many cable is connected, so it is occurred the electromagnetic radiation from the cable.

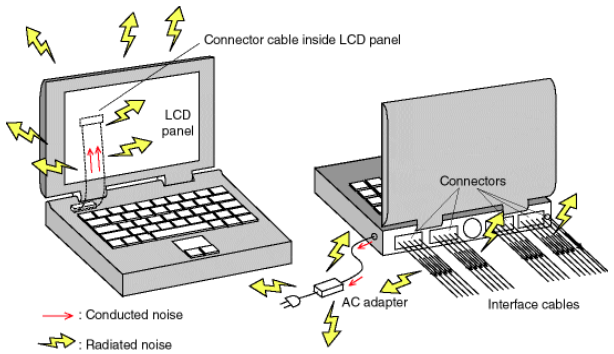


Figure 2.3 Laptop signal leakage path

2.2.3. Measurement system

We carried the measurement at International Radio Interference (CISPR) Special Committee recommended 3×3 m standard electromagnetic anechoic chamber (Semi-Anechoic Chamber) in National Radio Research Laboratory. Height of antenna is 1 meter and the distance between antenna and target

device is 1.5 meter. VDU has the ‘H’-pattern which is commonly used for electromagnetic interference (EMI) experiment.

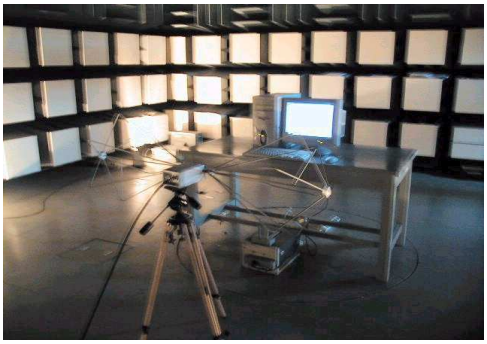


Figure 2.4 Equipment installation for VDU in chamber

EMI Test Receiver (Rohde & Schwarz, ESI 40) is used and Biconical Antenna (EMCO, 3109) is scanning up to 100 MHz. From 100 MHz to 1 GHz scanning is used for log periodic (LP) Antenna (Rohde & Schwarz, HL223).

In order to analyze the characteristics of electromagnetic radiation in the signal transmission cable, electrical analysis was performed about the transmitted signal.

Table 2.1 Parameter setting of EMI receiver for VDU

Center frequency	Detected EMSEC-channel information
Frequency span	1 MHz or Zero Span
Resolution Bandwidth	100 kHz or 120 kHz
Video Bandwidth	3 kHz
Sweep Time	100 ms

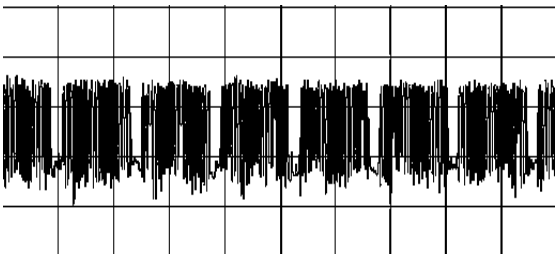
Figure 2.4 shows the measurement installation of VDU in semi-anechoic chamber and Table 2.1 explained the parameters of EMI receiver for detecting VDU leaked signal

2.2.4. Measurement result

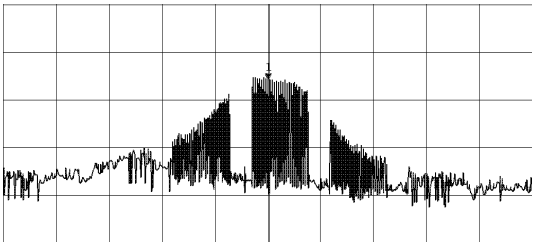
In order to distinguish the leakage electromagnetic signals and other electromagnetic signals, we have to select the primarily electromagnetic leaked frequency. The methods of measuring frequency are followed this process. In order to check the leakage of electromagnetic signals by the monitor signal, we used the frequency domain signal from spectrum analysis device.

In general, the video signal is sent 60, 75 or 85 times per second to the monitor. To configure each screen, the video signal is called a frame. Silence the (BLANK Time) between the frame and the frame is presented and accounted for the entire time frame of usually about 3.3% to 7.2%. This part is no signal, regardless of the content of the video signal.

If you scroll on the screen that displays the 'H' pattern can properly adjust the settings of the spectrum analyzer to determine the leakage electromagnetic waveform of video signal. Figure 2.5 shows the leakage of electromagnetic waves, this pattern is 1024 × 768 @ 60Hz video mode shown in the waveform.



(a) SPAN = 0 MHz

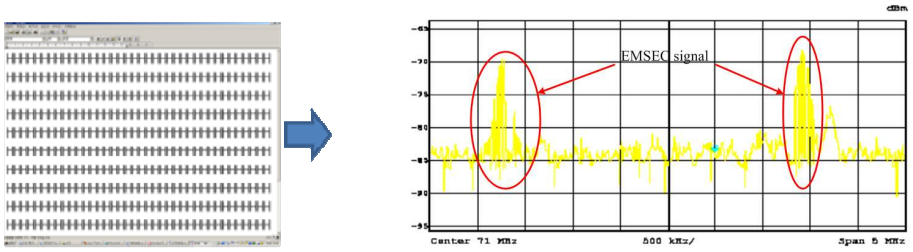


(b) SPAN = 1 MHz

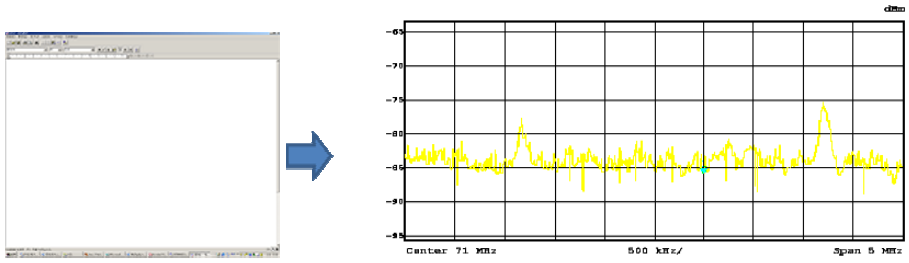
Figure 2.5. Leakage electromagnetic waveform from VDU

As shown in Figure 2.5, the leakage electromagnetic signals show two properties. The empty spaces appear in the middle of the first signal caused BLANK Time between frames. Approximately every 1.6 ms for each cavity appears in Figure 2.5, the full width (SWT is 100ms), the video signal has a refresh rate of 60Hz (i.e., the frame is repeated every 1/60s = 17 ms). This feature is more evident when the receiver's SPAN to 0 MHz in Figure 2.5 (a). This feature is one of the most obvious characteristic that distinguish the leakage electromagnetic signals. Figure 2.6 shows an experiment of a spectral analysis of EMSEC-channel information at 71 MHz center frequency from a desktop computer (Samsung Magicstation DM700) having the ‘H’-pattern video screen (a) and clear mode video screen (b). If the screen is changed, it

may be changed the compromising emanation spectrum. And we search for leakage electromagnetic frequency and record accurately the measurement frequency 100 MHz to 1 GHz.



(a) Radiated electromagnetic waveform at ‘H’-pattern



(b) Radiated electromagnetic waveform at clear mode

Figure 2.6 Measurement of radiated electromanetic at VDU

2.3 Compromising Emanations from Printer

2.3.1 Property of Printer

It is shown that the execution of print command from the PC to the printer

and the print data process in Figure 2.7.

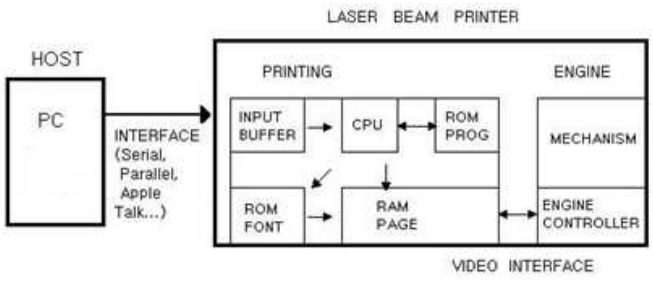


Figure 2.7 Printer data transmitting process

The detailed process was categorized depending on the subject to process the data into process in PC and process in printer, respectively.

A. Process in PC

① The print command from your PC

② The printer driver converts the document to page description language (PDL).

③ The created data is sent to the printer controller through communication cable.

B. Process in Printer

① Data received from the computer is stored in the input buffer in printer.

② The data received in the input buffer is analyzed by the emulator in the program read only memory (PROM).

③ According to the analyzed data, data of the actual contents for print are

stored in the page memory.

④ After confirming the ability of engine to print, data send to the engine.

⑤ Engine controller operates the engine mechanism and received data from the printing controller prints.

C. Characteristics of the transmitted signal

In case of internal signal of PC, The document by the internal printer drivers is converted to PDL, and this data is stored on the hard disk drive (HDD). The data stored in the input buffer analyzes and sent to the engine for print.

2.3.2 Leakage path of printer

The circuit inside the printer is divided into data controller that is responsible for processing and the print engine unit. Control unit printed circuit board (PCB) is built-in device, such as processor, memory and rashes, many types of devices.

Electromagnetic leakage occurs at the junction. The connection cable also helps to act as an antenna, so that the transmitted signal is radiated into space. In other words, the longer the length of the wire, electromagnetic occurs more.

The connector that is connected with a PC and input of the engine can be estimated that the source of the leakage of electromagnetic waves emitted from the printer as shown Figure 2.8. Because it does not exceed the 5V, it seems unlikely far enough to radiate like the VDU leaked signals.

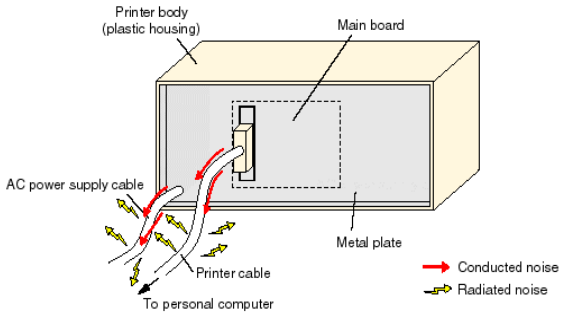


Figure 2.8 Leakage path of printer

2.3.3 Measurement system

We carried the measurement at International Radio Interference (CISPR) Special Committee recommended 3×3 m standard electromagnetic anechoic chamber (Semi-Anechoic Chamber) in National Radio Research Laboratory. Height of antenna is 1 meter and the distance between antenna and target device is 1.5 meter. VDU has the 'H'-pattern which is commonly used for EMI experiment.

EMI Test Receiver (Rohde & Schwarz, ESI 40) is used and Biconical Antenna (EMCO, 3109) is scanning up to 200 MHz. From 200 MHz to 500 MHz scanning is used for LP Antenna (Rohde & Schwarz, HL223).

In order to analyze the characteristics of electromagnetic radiation in the printer, we measured the HP 2100 laser printer, FAX 2850 (Brother laser printer), LAZETT ML-5000A (Samsung laser printer) and GLP 860 (LG laser printer). Table 2.2 explained the parameters of EMI receiver for detecting

printer leaked signal

As a result, the specific signals did not occur over the 500 MHz frequency band the measurement of the entire spectrum from 20 to 1000 MHz. Therefore, the measurement frequency range below 500 MHz, and 25 MHz intervals were measured precisely.

Table 2.2 Parameter setting EMI receiver for printer

Reference Level	-30 dBm
SPAN	30 MHz
RBW	100 kHz
VBW	3 kHz
SWT	100 ms

2.3.4 Measurement result

As described above, the printer is connected in parallel communication with PC. Parallel communication is a method of transmitting separately the lines of eight numbers of ways to send 1- Byte information different from the serial communication. Therefore, it is expected to appear in the mixed form of frequency components are mixed, when analyzing the signal from the frequency domain.

In order to measure the electromagnetic radiation generated during operation of the printer, we used a digital oscilloscope for measuring and analyzed the frequency components by measuring the pattern of the time

domain of the printer. Also we have used the ‘H’-pattern which is used in EMI test in general.

Figure 2.9 represents the frequency components by measuring the pattern of the time domain of the printer by fast fourier transform (FFT) using digital oscilloscope. Printed image is 12 font ‘H’-pattern as like the monitor case and waveform voltage is about 2.5 V. When we printed the ‘H’-pattern, the number of vertical pixel is same as the number of signal bearing waveform. It is determined that printed image can be recoverable to restore the signal using a measure EMSEC waveform from printer. Figure 2.10 (a) shows the fundamental frequency is 7.3 MHz EMSEC waveform and blue lines means no printer signal. Also, it found that the electromagnetic emanation from printer is detected by multiplying frequencies of the fundamental frequency in Figure 2.10 (b).

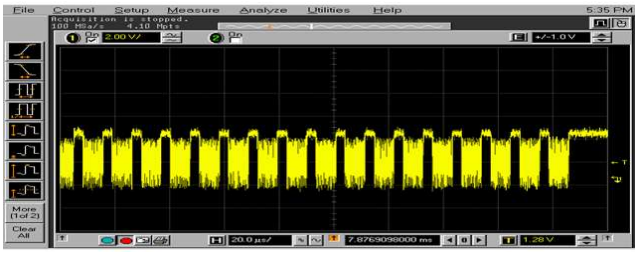
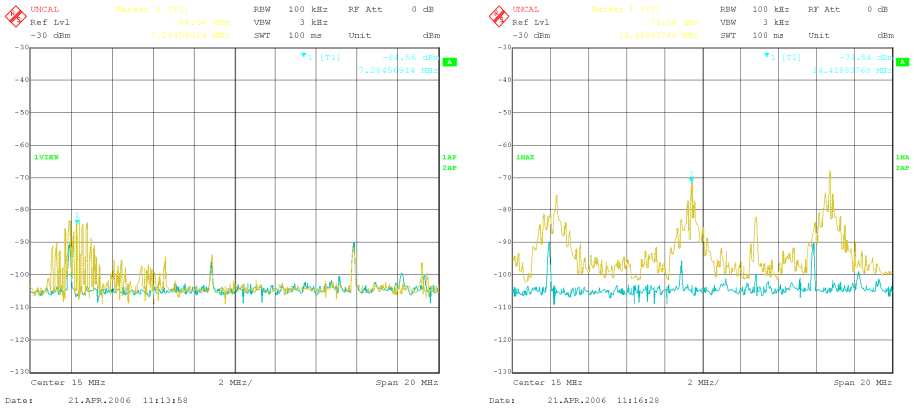


Figure 2.9 Printer radiated spectrum using the oscilloscope



(a) Center frequency : 7.3 MHz (b) 7.3, 14.4, and 21.7 MHz (Maxhold)

Figure 2.10 Printer radiated spectrum using the EMI recevier

2.4 Conclusions

In order to establish a emission security limits of protection against leakage of information, it must be preceded to accurately measure the frequency and level of the signal of the radio wave signal by the printer and the monitor. Also, it should be most advanced in order to measure the EMSEC-channel information from monitor and it must accurately detect the radiated EMSEC-channel information.

When radiated EMSEC-channel information is receiving, it is difficult to find a signal directly based on the only spectral characteristics. So that we measure the pattern in the time domain of the EMSEC-channel information from monitor firstly, and then analyzed the frequency components. Frequency component of EMSEC-channel information from the monitor have a frequency component of harmonic waves of the fundamental frequency.

Changing the 5MHz, 25MHz, and 50MHz SPAN of receiver to explore the radiated EMSEC-channel information from the monitor, we detected by determining the presence or absence of the signal under the display ‘H’-pattern and white pattern. Detected the EMSEC-channel information from monitor shaped the characteristics Vertical Blank Time of (VBT) and Horizontal Blank Time (HBT). The finer vertical line represents the HBT and the envelope of wider line means the VBT.

A measurement result of the radiation electromagnetic spectrum from the printer, it was found to exhibit properties entirely different form of radiation electromagnetic spectrum in the VDU. The main reason for this difference in leakage electromagnetic spectrum characteristics are displayed, it is different for transmitting method of signal.

Since the VDU signal is also sent in three lines R, G, and B, the signal is a synchronized and has the same frequency components. It can be interpreted as one signal component. It is because must undergo further a process of separating the signal eight different electromagnetic radiation one was collected. As a result, reconstruction and receiving electromagnetic radiation of parallel communication signals will become more complex than processing a VDU signal described earlier.

The measured bandwidth of radiated electromagnetic spectrum is about 7.3 MHz and frequency band is from 5 to 300 MHz. Since general form of the information bearing spectrum is also displayed in a round semicircular by showing a bandwidth, it is possible that information is contained this frequency band.

Chapter 3. Reconstruction of Compromising Emanations

3.1 Introduction

In this chapter, you will learn how to restore the system configuration and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and PC monitors that you saw in Chapter 2.

The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, RBW of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system. Whereas, image restoration algorithm for EMSEC system as post-processing is corresponded to the software of EMSEC-system.

That is, the signal processing gain means that to obtain a better *SNR* of the signal by utilizing a variety of a digital signal processing (DSP) processes the digital signals that after digitized via converter analog to digital (AD) signal of electromagnetic radiation that is received via the receiver.

The signal processing gain can be obtained through filtering, correlation, and character recognition algorithms and averaging technique, generated from the information such as a computer monitor, the same signal with a constant

cycle to illustrate the form of periodic signals to be repeated. Averaging technique is presented in the most efficient method how to receive repeated signals of multiple periods continuously.

In this chapter, we introduce how to restore the EMSEC signal from video display system and printer using the image process.

3.2. EMSEC system for Reconstruction

In this study, the data were processed using the of the Agilent vector signal analyzer vector signal analysis (VSA) for receiver. That has the 36 MByte RBW. LP antenna is used for compromising electromagnetic for video signal reconstruction and LP antenna is used for compromising electromagnetic for printer signal reconstruction, respectively. Controller is used for NI-5412 which has the 50~200 MSamples/sec sampling rate, amplitude resolution is 12 bit, and data storage memory is 512 Mbyte. Also, vertical synchronization board is used for NI-5124 arbitrary waveform generator which has the 100 MSamples/sec sampling rate, μHz resolution. Signal processing and analysis tools are implemented by Labview 7.0 as shown Figure 3.1.

3.3 Reconstruction of Compromising Emanations from Video Display Units

3.3.1 Characteristics of EMSEC-channel information from VDUs

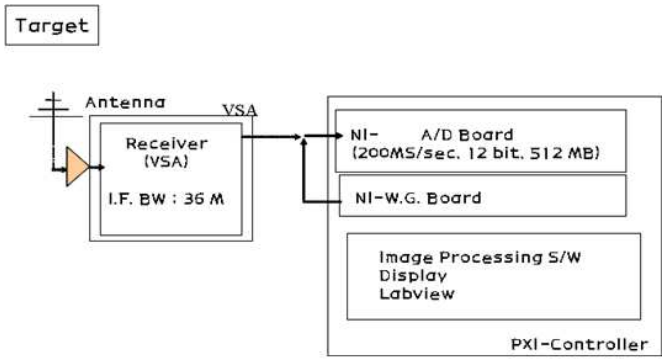


Figure 3.1 Reconstruction of EMSEC-system

Monitor signal which are commonly used refers to an analog monitor signal, and there are the three signals: Red, Green, Blue, Horizontal and vertical sync signals. In the paper, three different video data signal is directly related to the information that is displayed on the monitor.

Generally, a color monitor in each of the three video signals can be displayed with up to 256 levels. As a result, a total of 16,777,216 (256 × 256 × 256) different color are represented. In other words, the number of colors used by Windows when set to 24-bit True color or more, each of the R, G, B signal is a signal with a level of 256.

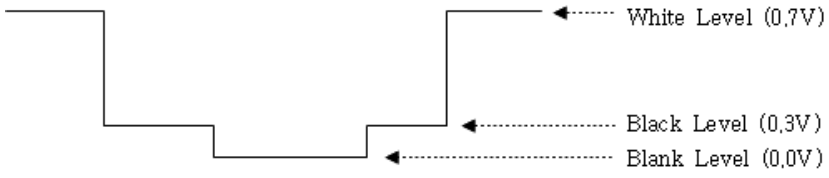


Figure 3.2 Video signal voltage waveform

Figure 3.2 shows the physical waveform of the video signal. If you are using a 24-bit true color video signal from 0.3V to 0.7V, 0.4V evenly divisible by 256 levels and the video level is transmitted at each voltage level. This level represents the saturation of each colors, saturation signal 256 having the highest saturation signal is set to 0. For example, a pure red to represent color saturation of 200 of each of the R, G, B signal should be sent as follows.

Serial form of a monitor signal is sent to the monitor, the transmitted signal consists of interlaced video, such as in Figure 3.3. Therefore, each line of the video signal being sent is sent sequentially.

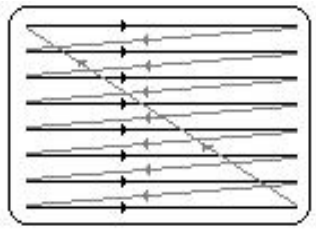


Figure 3.3 Interlaced video display

Vertical blank time is moving time from the end of the line for the first time at the end of the next line. And Horizontal blank time is moving time physically from last line of the first line of the next row and need time to move to the first line of the row. During this time, the data will not be sent. Thus, the video signal is sent through the cable is in the form as in Figure 3.3 [26].

The data in the Figure 3.4 represents one line of the monitor image from the

mainly used in monitor mode 1024 × 768 resolution, these lines are configured into 768 lines of 1024 pixels. Thus, this data is different depending on your monitor resolution indicates the number of pixels.

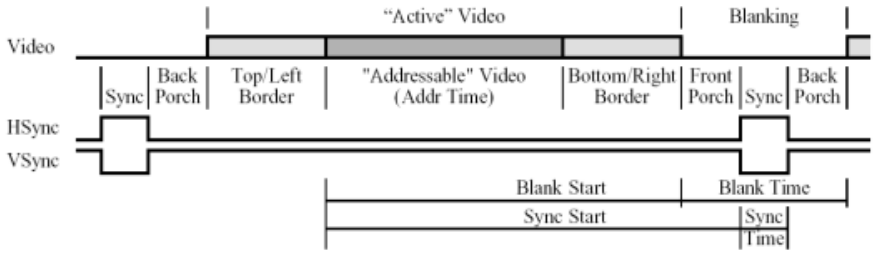


Figure 3.4 Form of video signal

As a result, the frame signal consists of 786,432 (1024 × 768) pixels and 58,982,400 (786,432 × 75) per second to transmit signals using 75Hz refresh can be converted to a frequency of about 59 MHz. Considering the horizontal and vertical blank time, the actual transmission frequency of the signal is higher than previously calculated value.

To predict the leakage electromagnetic radiation frequency of the video signal, the frequency of characters to be represented on the actual monitor, depending on the number of pixels, F_v, (3.1).

$$F_v = \frac{Pixels\ of\ clock}{Number\ of\ character} = \frac{F_{pix}}{N_{char}} \tag{3.1}$$

When video mode is 1024 × 768 at 60 Hz using the ‘H’-pattern, fundamental

frequency can be estimated by

$$F_v = \frac{25.175\ MHz}{8\ pixel} = 3.15 MHz / pixel \tag{3.2}$$

We can estimate the leaked frequencies from VDU using (3.1) and it can be estimated to detect harmonic frequencies of fundamental frequency. Also the harmonic signal amplitude is usually smaller than the size of the center frequency generally. For this reason, it can be limited to 1GHz or less from the 100 MHz frequency band to be measured.

3.3.2 Reconstruction result

To improve the performance of leakage electromagnetic signals reconstruction, RBW of receiver, signal processing gain, and antenna sensitivity are major elements. High RBW receiver or high gain antenna are approaching the hardware part to enhance the performance of reconstruction system. On the other hand, post processing for increasing the signal processing gain is software part of the leakage electromagnetic signal recovery system. In other words, signal processing gain is to improve the *SNR* of the signal using a variety of DSP processing. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals having independt noise. That method is a practical, highly effective and widely used technique for increasing the *SNR* of a periodic signal, such as

that generated by the image-refresh circuitry in a video display system [2, 7].

Signal processing gain can be obtained through filtering, correlation, averaging technique, and character recognition algorithm. Averaging technique presented in the most efficient way because the leakage electromagnetic signals from a VDUs have the form of a periodic signal, the same signal repeated with regular intervals. Figure 3.5 shows the experimental results on the real-time signal using the averaging technique.

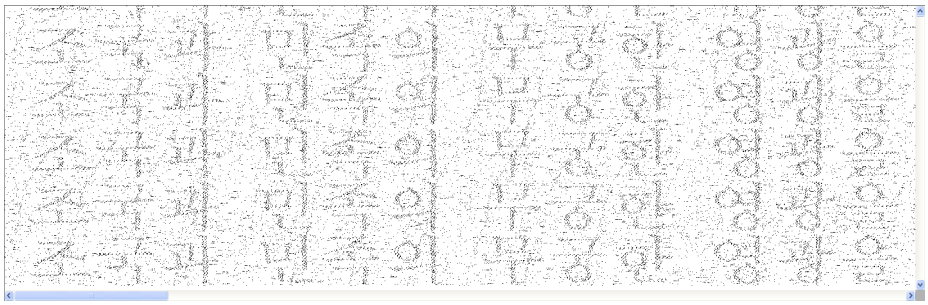


Figure 3.5 Reconstruction image using averaging technique

3.4 Reconstruction of Compromising Emanations from Printer

3.4.1 Characteristics of EMSEC-channel information from Printer

The photosensitive part of laser printer formed the latent image by generating a photo current in the drum by scanning the laser beam on the

drum. It is displayed as the difference of voltage. The semiconductor laser can be turned ON / OFF by modulating the input current. Semiconductor lasers are commonly used as a light source [23].

In this paper, it is recognized as part semiconductor diode optical section as shown Figure 3.6 the cause of the major leakage electromagnetic wave leakage in laser printer. In order to measure the electromagnetic radiation generated during operation of the printer, we used a digital oscilloscope for measuring and analyzed the frequency components by measuring the pattern of the time domain of the printer. Also we have used the 'H'-pattern which is used in EMI test in general.

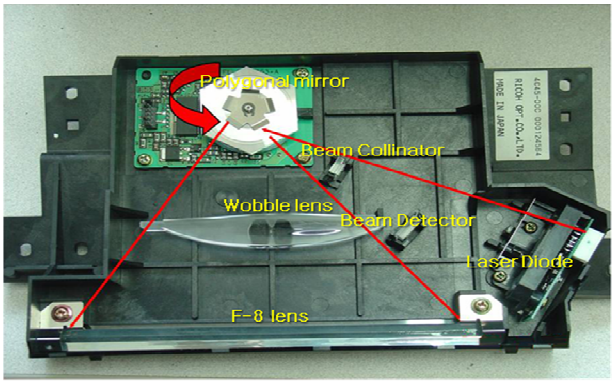
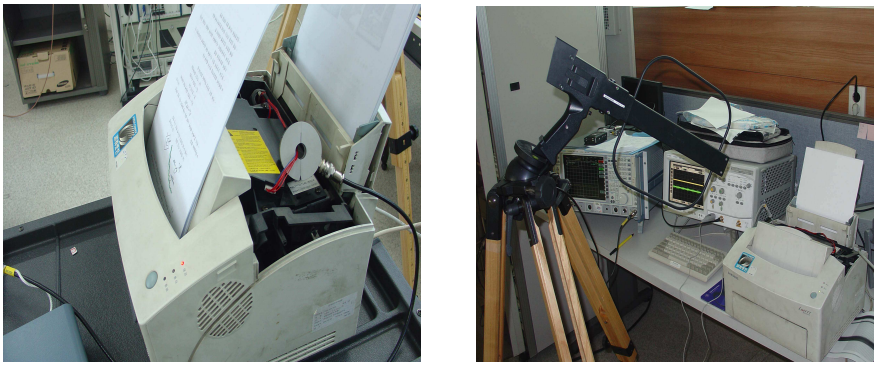


Figure 3.6 Optical part of the laser printer

Because it is transmitted serially in laser printer, the laser printer can be detected and recovery in a similar manner as video display units. However head driver chip is built in the head in inkjet printer (HP Photo 948C), signal can not be detected. In addition to, signal which is transmitted to the nozzle is sent in parallel . It is impossible to restore the receiving the signals. In this reason, we focus on the laser printer for detecting and reconsturction.

We measure the magnetic field range round 5 MHz-300 MHz to reconstruct the leakage of electromagnetic radiation signal printer. A current probe and loop antenna are used for detecting the EMSEC-channel information from printer as shown Figure 3.7. And Table 3.1 summarized the equipment parameters for printer measurement. Figure 3.8 shows the EMSEC-system's GUI and reconstruction results of spectral measurements of the time-domain electromagnetic radiation printer.



(a) Using the current probe (b) Using the loop antenna

Fig 3.7 Measurement for EMSEC signal from laser printer

Table 3.1 Target equipment property for laser printer measurement

Equipment	**Resolution**	**Writing speed**	**Color/Monochrome**
Printer 1	600 dpi*	8 ppm**	Monochrome
Printer 2	600 dpi	16 ppm	Color
Printer 3	600 dpi	4 ppm	Color

* dpi : dots per inch , ** ppm : page per minute

3.4.2. Reconstruction Result

Based on the experimental results, we can see that the resolution of the reconstructed image are affected by distance between antenna and printer and sampling rate. Figure 3.9 (a) and (b) shows the relationship between sampling rate and the restored image.

Incremented sampling rate by 5 MSamples/sec in the range from 5 MSamples/sec to 50 MSamples/sec, the resolution of the restored image enhanced. But an area of the restored image is reduced because AD board memory is limited. We found that there is no problem with the recognition even low Sampling rate of about 5 ~ 10 MSamples/sec.

Figure 3.9 (c) and (d) are restored at the 100 mm and 300 mm separation distance between antenna and target printer, respectively. When restored by detecting the magnetic field components, it is impossible to reconstruct the signal with a distance of about 300 mm less than about. These experimental results can be expected to utilize in order to establish the security level and measurement method. In future work, it can be basis of research to prevent from leaked signal for the various other electronic devices.

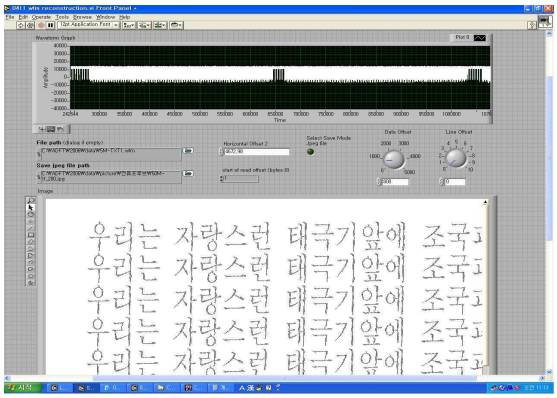
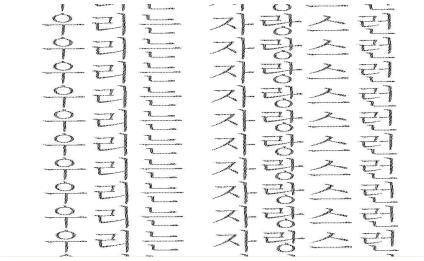
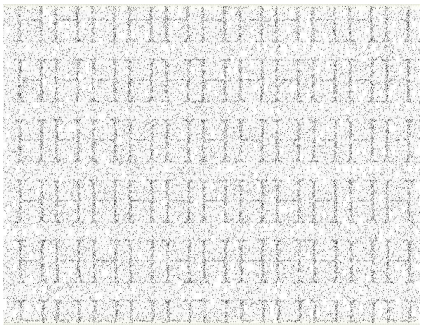


Figure 3.8. EMSEC system's GUI

(a) 5 MSa/sec



(b) 10 MSa/sec



(a) 100 mm

(b) 300 mm

Figure 3.9. EMSEC signal reconstruction from printer

3.5 Adaptive Deringing Filter for Reconstruction

MPEG-1/-2/-4 and H.26x are processed by block-based, where transformation is done by a Discrete Cosine Transforms (DCT) on blocks of 8×8 pixels [27]. Two of the main artifacts from the quantization of the DCT are blocking and ringing. The blocking artifact is seen as an unnatural discontinuity between pixel values of neighboring blocks. The ringing artifact is seen as high frequency irregularities around the image edges. In brief, the blocking artifacts are generated due to the blocks being processed independently and the ringing artifacts due to the coarse quantization of the high frequency components [28]. Deblocking filter is to reduce the blocking ringing and deringing filter is to remove the ringing, respectively.

We propose an adaptive deringing filter for image restoration of EMSEC-channel information focusing on deringing filter algorithm that is used in post-processing method in MPEG-4. When we reconstructed the EMSEC-channel informaiton without any other image processing, the horizontal signal is lost easily comparing the vertical signal. That is the reason why EMSEC-channel information can be detected easily at high rising or falling edge. The Figure 3.10 shows the EMSEC-channel information reconstruction result without image processing. We can see the many horizontal pixels in reconstructed image can’t recover from the original image. To compensate for the recovery of EMSEC-channel information property, we propose the adaptive deranging filter for image restoration of EMSEC-channel information.

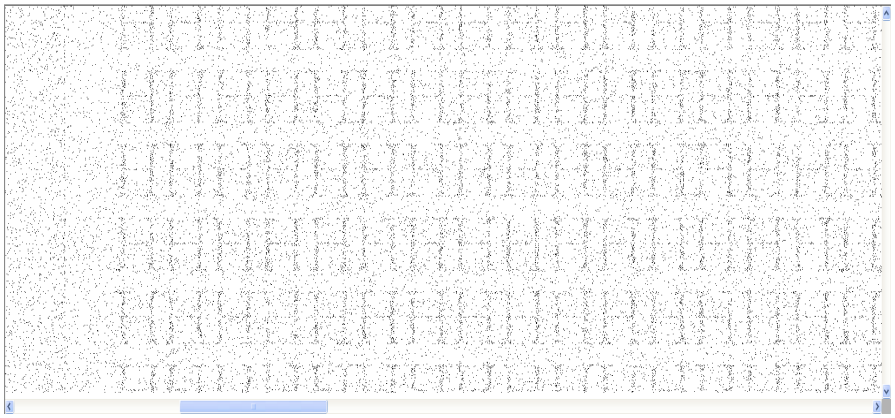


Figure 3.10 Reconstructed image without post-processing

We process the windowing with 16×16, 8×8 or 4×4 macro blocks to calculate the sum of differences (*SD*). The *SD* is calculated as follows :

$$SD(u,v) = \sum_{j=0}^{B-1} \sum_{i=0}^{B-1} X(i+u, j+v) \tag{3.2}$$

where, B is the size of macro blocks such as 16, 8 and 4, X is the reconstructed image not using the image processing, (i, j) is the spatial location within the reconstructed image and (u, v) is the candidate motion vector. If final *SD* value is over threshold obtained by experiment, that macro blocks is replaced by 255 and the macro block is replace by 0 otherwise as shown by Figure 3.11

When we used the window size 16 for calculating the SD, resolution of reconstructed image is not good but process time is fast by reducing the

complexity. The size of the macro block is reduced, the operation speed is slower but it is more accurate restoration image from EMSEC-channel information.

Figure 3.12 shows the reconstructed image using the adaptive deranging filter which filter size is 4×4. We can recognize more accurate than the reconstructed image without any other image processing.

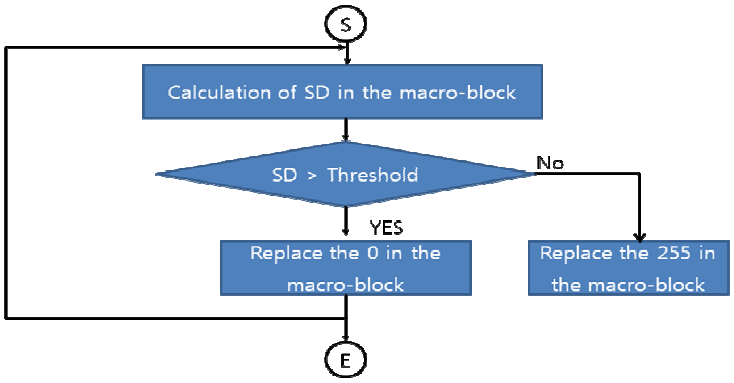


Figure 3.11 Algorithm flow of adaptive deringing filter for EMSEC-channel information

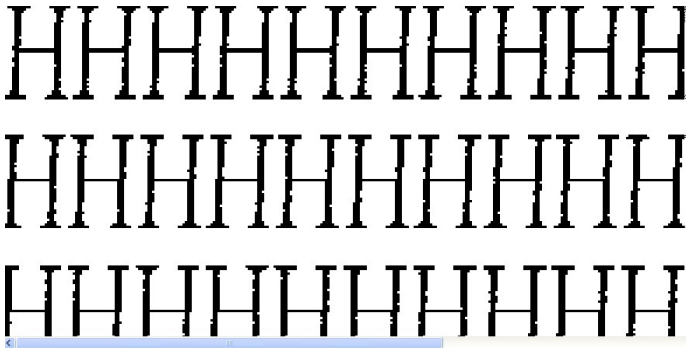


Figure 3.12 Reconstructed image using the adaptive deranging filter

Also, we used four different target characters which are Korean, Chinese, English characters and Arabic numeral. When we adjusted the adaptive deranging filter as the post- image processing, we can obtain that the minimum peak signal-to-noise ratio (*PSNR*) enhancement of reconstructed images using the adaptive deranging filter is 2 and maximum *PSNR* enhancement is 10 comparing the original reconstructed image in this experiments. *PSNR* is most commonly used to measure the quality of reconstruction image. The signal in this case is the original data, and the noise is the error introduced by reconstruction from the EMSEC-channel information. *PSNR* is most easily defined via the mean squared error (*MSE*). Given a $m \times n$ monochrome original image I and its noisy reconstruction image K, *MSE* is defined as :

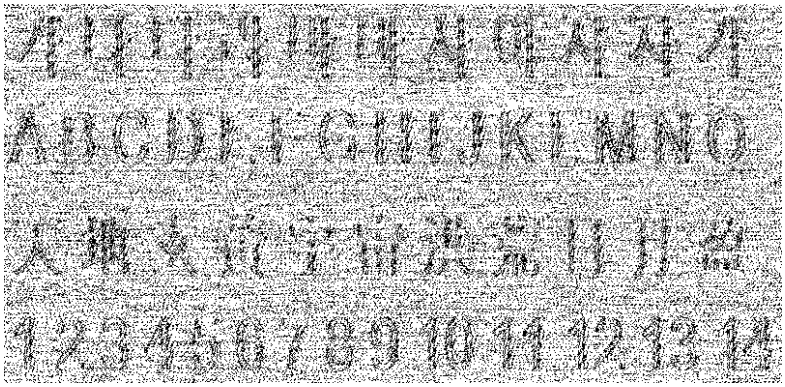
$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \tag{3.3}$$

The *PSNR* is defined as :

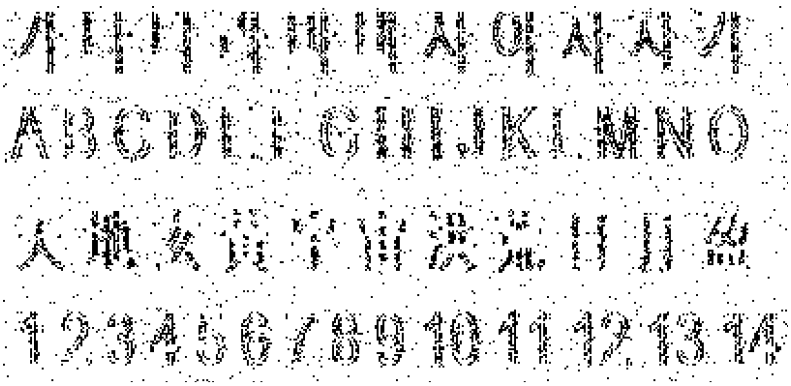
$$PSNR = 10 \log_{10} \left(\frac{MAX_I^{\ 2}}{MSE} \right) = 20 \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \tag{3.4}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bit per sample, this is 255. Figure 3.13 showes the *PSNR* comparison between the reconstructed image without post-

processing and the reconstructed image using the adpative dering filter whose filter size is 4. And chinsese character is more difficult to reconstruct the image comparing other characters due to the many storkes of the chinese charcter.



(a) Reconstructed image without image processing (*PSNR* : 58.55)



(b) Reconstructed image using the adaptive filter (*PSNR* : 68.34)

Figure 3.13 Comparison of *PSNR* Enhancement filter

3.6 Conclusion

In this study, configure your system and build the leakage electromagnetic signal reconstruction algorithm in order to improve the performance of the system by applying a averaging technique as a post-processing algorithm to reconstruction of the VDUs and printer.

By applying the post-processing algorithm, the reconstructed image with improved *SNR*, the noise is removed from the histogram equalization algorithm and a combination of multi-threshold histogram computation algorithms, the experimental results and the morphological algorithm can be obtained. It is easier to find the frequency of the electromagnetic wave leakage of the advantages of real-time processing and fast detection. In this experiment, for real-time processing with optimal speed and excellent *SNR* at 100 MSamples/sec, respectively, 50, 100, 150, 200 MSamples/sec, results of experiments done to restore the signal was possible to restore the video. In addition to, we propose the adaptive deringing filter to reconstruct the EMSEC-channel information from PC and printer. When we adjusted our proposal algorithm as post-image processing for EMSEC-system, we can obtain that the minimum *PSNR* enhancement of reconstructed images using the adaptive deranging filter is 2 and maximum *PSNR* enhancement is 10 comparing the original reconstructed image.

We can see that the resolution of the reconstructed image is affected by distance between antenna and printer and sampling rate. Increasing the

sampling rate, the resolution of the restored image enhanced. But an area of the restored image is reduced because AD board memory is limited. We found that there is no problem with the recognition even low Sampling rate of about 5 ~ 10 MSa/sec. Also, it is impossible to reconstruct the signal with a distance of about 300 mm less than about. These experimental results can be expected to utilize in order to establish the security level and measurement method. In future work, it can be basis of research to prevent from leaked signal for the various other electronic devices.

Chapter 4 Characteristic of Frequency Correlation EMSEC Channel in indoor environments

4.1 Introduction

Many researchers have investigated the EMSEC channel model and signal attenuation related to the channel environments. Previous model is too simple to reflect a realistically complex environment, and may give rise to some discrepancies between simulation results and real measurements. Although radio attenuation fluctuates according to the environment and distance between the transmitter (TX) and the receiver (RX), these previous works [1, 7, 24, 25] assumed that the radio attenuations are constant in order to obtain security limit and guide test method.

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable TRA. TRA is defined as the sum of all types of radio attenuations such as free space loss and additional radiation pathloss in the environment. The expected noise level and attenuation values are random variables that, in the absence of better data, have to be modelled as being normally distributed with some mean and variance determined from the statistical evaluation of a large number of measurements in various indoor environments [7]. We analyzed the pathloss characteristics of an indoor

EMSEC-channel under various environments on the basis of the measurements. For each environment, we obtained the TRA using its probability distribution to overcome the drawbacks of the previous works [1, 7, 24, 25].

4.2Channel Measurement

4.2.1 Measurement System

To analyze the characteristics of the compromising emanations, we performed frequency-domain measurements using vector network analyzer (VNA) and a pair of biconical and broadband LP antennas (Schwarzbeck VULB9161) from 100 MHz to 1000 MHz. Our measurement system yielded, S_{21} the forward transmission coefficient between the TX and RX antennas. For each frequency setup, a known sinusoidal signal was transmitted, and the magnitude and phase of the received signal were obtained. During the CTF measurements, the VNA was set to transmit 1601 continuous-wave tones uniformly distributed over the frequency bands in the 100 MHz to 1000 MHz range with a maximum frequency resolution at a frequency step of 0.56 MHz. This frequency resolution yielded a maximum excess delay of approximately 1.7 μs and a maximum distance range of approximately 533 m.

4.2.2 Measurement Scenarios and Environment

If the eavesdropper is located in an open area, the free-space loss will be

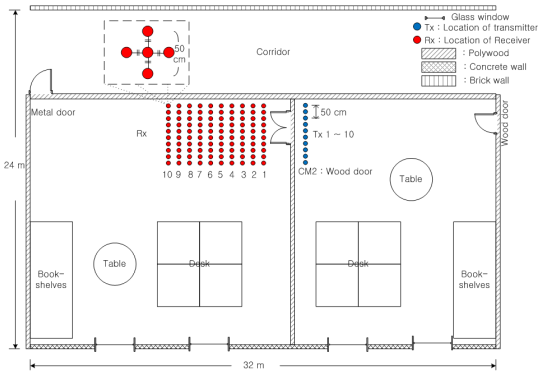
the dominant attenuation. Because residential and office areas are easily and secretly targeted by EMSEC-channel attacks, calculation of the TRA with regard to these environments is necessary. Measurement scenarios were set up by considering the property of the compromising emanations. Accordingly, the TX antenna was fixed in 10 different positions, whereas the RX antenna was moved along 50 positions at intervals of 0.5 m. The distance between the TX and the RX antennas ranged from 1 m to 10 m in each channel model (CM). Figure 4.1 shows the locations of the TX and RX antennas and the channel environment. Because the frequency spectrum of the compromising emanations from a target device is widely spread and its intensity is very weak, we set the transmit power to 1 mW.

To reflect the characteristics of the compromising emanation, we pay more attention to the non-line-of-site (NLOS) case than the line-of-site (LOS) case. The measurements were carried out in a modern office building having concrete walls, metal doors, wood doors, and glass windows.

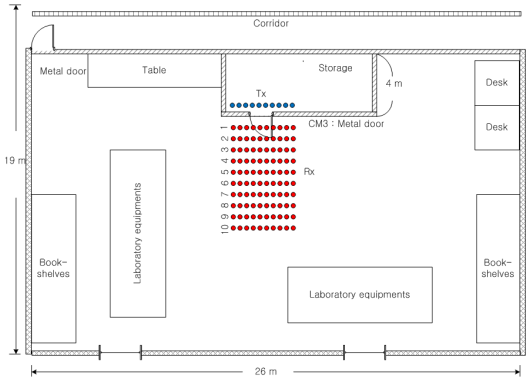
Table 4.1 Description of indoor EMSEC-channel models (CMs)

Channel Model	**Type**	**Material**	**LOS/NLOS**
CM1	Free space	Air	LOS
CM2	Twin door	Wood	NLOS
CM3	Single door	Metal	NLOS
CM4	Window	Glass/Metal	NLOS
CM5	Wall to wall	Concrete	NLOS

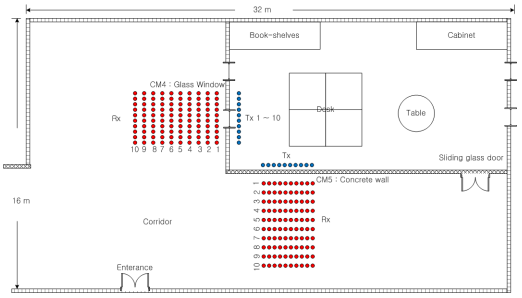
Table 4.1 summarises the scenarios in which five environments composed of various materials, LOS/NLOS cases, and structures were selected to study the propagation of compromising emanation under the influence of various materials, structure, sizes, and layouts.



(a)Environment 1



(b)Environment 2



(c)Environment 3 and 4

Figure 4.1 Channel environments

4.3 Analysis of Indoor EMSEC-Channel for Compromising Emanations

For the conventional channel-characteristic analysis, the root-mean-square delay spread and the mean-excess delay are essential parameters. However, the EMSEC-channel analysis is generally used to evaluate the electromagnetic field strength of the target equipment. Because the compromising emanation from target equipment in buildings are generally attenuated with the walls of the buildings and the distance between the target equipment and the receiver, the received electromagnetic field strength is a very important parameter in the determination of the emission security limits. Moreover, the delay parameters are compensated for by the horizontal and vertical synchronization parameters using the number of lines and frame frequency when the EMSEC-channel information is reconstructed [7]. Therefore, we focused on the attenuation of the received signals with respect to distance, frequency band, and channel environment instead of the delay parameters.

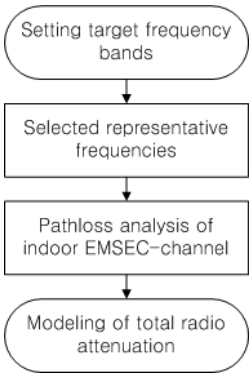


Figure 4.2 Outline description of our proposed approach

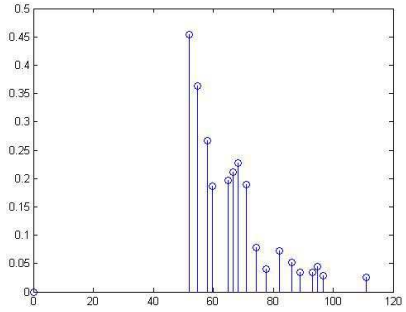
Figure 4.2 illustrates the procedure we used to propose the emission security limits. First, we set the target frequency bands from 100 MHz to 1000 MHz. Next, frequency correlation coefficients are calculated to find the representative frequencies at target frequency band for analysis pathloss characteristics on EMSEC-channel. We evaluated the TRA considering target frequency band and channel environment.

4.3.1 Frequency Correlation Property on Indoor EMSEC Channel

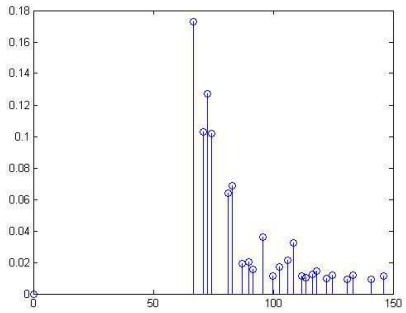
For considering the frequency correlation of the indoor EMSEC-channel, we used the EMSEC-channel measurements from 100 MHz to 1000 MHz frequency bands in Subsection 4.2. We can obtain the channel impulse response (CIR) of EMSEC-channel based on these measurements. Figure 4.3 showes examples of channel impulse responses at CM4 and CM5. Usually, for the LOS data, the first arrival path depend on distance. While for the

NLOS data, first arrival path is depend on distance and CMs, has very differentiation each CMs.

From the convolution between our measured leaked signal and the continus wave (CW) from VNA in the frequency domain, we obtained the envelope of the measured leaked signal which are applied the signal attenuation due to the channel environment. Because, the attenuation of the trasmitted signal from the VNA is reflected in the attenuation of EMSEC-channel information related to the channel environment. Figure 4.4 shows the example of envelope of measured EMSEC-channel information at CM2 and distance 7 meter.



(a)CM4 at distance d = 5 meter



(b)CM5 at distance d = 10 meter

Figure 4.3 Examples of channel impulse responses at CM4 and CM5

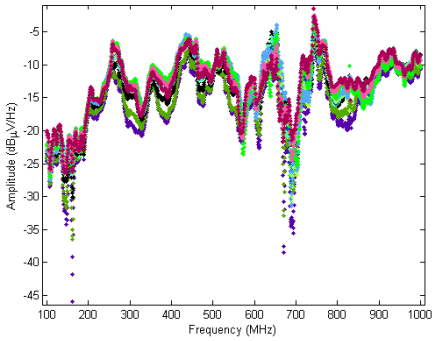


Figure 4.4 Example of envelope of measured leaked signal at CM2

For the characterization of the frequency correlation properties from the 100 MHz to 1000 MHz frequency bands, the cross-correlation coefficient was used to represent the correlation level of the received signal amplitudes between frequency tones. This process was presented in [29].

$$\rho_a(\Delta f) = \frac{C_a(f, f+\Delta f)}{\sqrt{C_a(f, f)}\sqrt{C_a(f+\Delta f, f+\Delta f)}} \tag{4.1}$$

where $C_a(f_1,f_2)=E[\{a(f_1)-m_a(f_1)\}\{a(f_2)-m_a(f_2)\}]$, $a(f_1)$ is the amplitude of the channel gain at frequency tone f_1, $m_a(f_1)$ is the mean of $a(f_1)$ and Δf is a frequency interval. The frquency interval increases from 1 MHz to interval bandwidth (BW) 100 MHz by multiples of the frequency step 0.5625 MHz in Section 2. We selected the interval BW is 100 MHz, because a multiple of BW = 50 MHz is needed for practical compromising for readable video

signals [7]. $\rho_a(\Delta f)$ is the average cross-correlation coefficient at the Δf as shown Figure 4.5. Because the eavesdropper is located in cluttered environments except free space practically, we did not consider the CM1. We simulated the frequency correlation coefficients as increasing the frequency interval to find the all frequency correlations at interval BW.

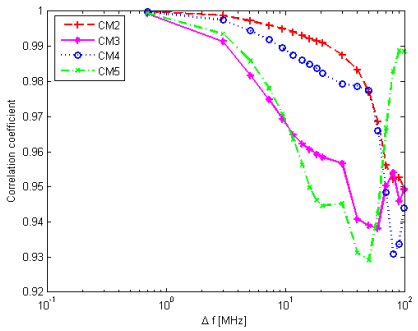
The cross-correlation coefficients become smaller as the frequency interval wider generally. But it is shown that the cross-correlation among the frequency tones is high from 0.6 to 0.9. Fig. 4.5 shows an examples of the correlation coefficients at a distance of 3 m on the 400–500 MHz and a distance of 9 m on the 800–900 MHz using (2) on the channel environments.

The calculated cross-correlation coefficients in this study are listed in Table 4.2. On the basis of these results, we represented the nine representative frequencies (f_r) as 200 MHz, 300 MHz, 400 MHz, 500 MHz, 600 MHz, 700 MHz, 800 MHz and 900 MHz for our target frequency bands to analyze the pathloss characteristics on the indoor EMSEC-channel.

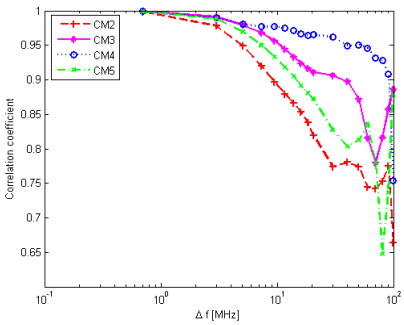
Table 4.2 Frequency correlaiton coefficients of indoor EMSEC-channel models

Frequency	CM2		CM3		CM4		CM5	
(MHz)	Min	Max	Min	Max	Min	Max	Min	Max
(100,200)	0.60	0.97	0.88	0.99	0.72	0.98	0.85	0.99
(200,300)	0.65	0.99	0.78	0.98	0.77	0.99	0.77	0.98
(300,400)	0.71	0.99	0.83	0.99	0.82	0.99	0.87	0.99
(400,500)	0.72	0.99	0.81	0.99	0.73	0.98	0.71	0.99

(500,600)	0.65	0.97	0.88	0.99	0.72	0.98	0.85	0.99
(600,700)	0.68	0.99	0.78	0.98	0.77	0.99	0.77	0.98
(700,800)	0.75	0.99	0.65	0.99	0.78	0.99	0.65	0.99
(800,900)	0.64	0.99	0.73	0.99	0.59	0.98	0.74	0.99
(900,1000)	0.64	0.99	0.81	0.99	0.78	0.98	0.71	0.98



(a)400–500 MHz (d = 3 meter)



(b)800–900 MHz (d = 9 meter)

Figure 4.5 Examples of frequency correlation coefficients

4.3.2 Pathloss Characteristics on the Indoor EMSEC-Channel

To develop an efficient EMSEC system, pathloss properties must be evaluated with respect to the possible noise level and TRA. Pathloss modeling can be simplified by assuming that the frequency dependence and the distance dependence can be treated independently of each other [30]. We can find the pathloss equation of the frequency-correlation indoor EMSEC-channel with the frequency and the distance *d* between TX and RX using the logarithmic equation [31]

$$PL(d, f) = 20 \cdot \log_{10} f + 10 \cdot \log_{10} k - 10 \cdot n \cdot \log_{10} d, \quad (4.2)$$

Where *n* is the pathloss exponent and *k* is the received power amplitude. We find *n* and *k* using least-squares (LS) curve fitting based on variation in the measured received power with distance for different CMs and frequency bands.

We summarized the detailed parameters of pathloss equation in Table 4.3. The root-mean-square error (RMSE) between measured parameters and estimated parameters is obtained using LS-curve fitting. Figure 4.6 shows the measured received power and LS-fitted curves represented by black solid lines for each CM.

CM3 and CM4 had a metal door and metal window frame between the TX

and RX, respectively, in which the EMSEC-channel information was effectively shielded. We conjecture that CM3 and CM4 had relatively higher power attenuation than CM2 and CM5, which were composed of wood and concrete, respectively. In other words, owing to the lower power attenuation of CM2 and CM5, they were more vulnerable to unintentional compromising emanation compared to CM3 and CM4. If the single security limit is typically applied for various indoor environments and frequency bands, signal leakage is a concern. The emission security limits are thus necessary for considering the influcence of channel environment in order to protect leakage important signal from eavesdropping.

Table 4.3 Estimation parameters of indoor EMSEC-channel models

Representative frequency, f_r	CMs	k	n	RMSE
f_r = 100 MHz (100–200 MHz)	CM2	0.012	2.30	0.0004
	CM3	0.016	2.84	0.0003
	CM4	0.002	2.29	0.0001
	CM5	0.015	1.17	0.0092
f_r = 200 MHz (200–300 MHz)	CM2	0.066	2.29	0.0016
	CM3	0.031	2.83	0.0003
	CM4	0.002	2.29	0.0001
	CM5	0.027	1.06	0.0103
f_r = 300 MHz (300–400 MHz)	CM2	0.089	2.33	0.0019
	CM3	0.018	2.82	0.0004

	CM4	0.002	2.32	0.0003
	CM5	0.054	1.36	0.0075
f_r = 400 MHz (400–500 MHz)	CM2	0.089	2.37	0.0009
	CM3	0.014	2.92	0.0003
	CM4	0.002	2.40	0.0001
	CM5	0.029	1.20	0.0035
f_r = 500 MHz (500–600 MHz)	CM2	0.108	2.41	0.0019
	CM3	0.054	2.93	0.0001
	CM4	0.007	2.33	0.0001
	CM5	0.032	1.14	0.0066
f_r = 600 MHz (600–700 MHz)	CM2	0.080	2.40	0.0039
	CM3	0.005	2.90	0.0001
	CM4	0.008	2.33	0.0001
	CM5	0.024	1.20	0.0042
f_r = 700 MHz (700–800 MHz)	CM2	0.109	2.38	0.0011
	CM3	0.025	2.88	0.0001
	CM4	0.009	2.32	0.0001
	CM5	0.021	1.32	0.0042
f_r = 800 MHz (800–900 MHz)	CM2	0.153	2.34	0.0041
	CM3	0.024	2.92	0.0001
	CM4	0.007	2.41	0.0001
	CM5	0.019	1.26	0.0043
f_r = 900 MHz	CM2	0.050	2.32	0.0009

(900–1000 MHz)	CM3	0.002	2.94	0.0001
	CM4	0.001	2.50	0.0001
	CM5	0.016	1.14	0.0062

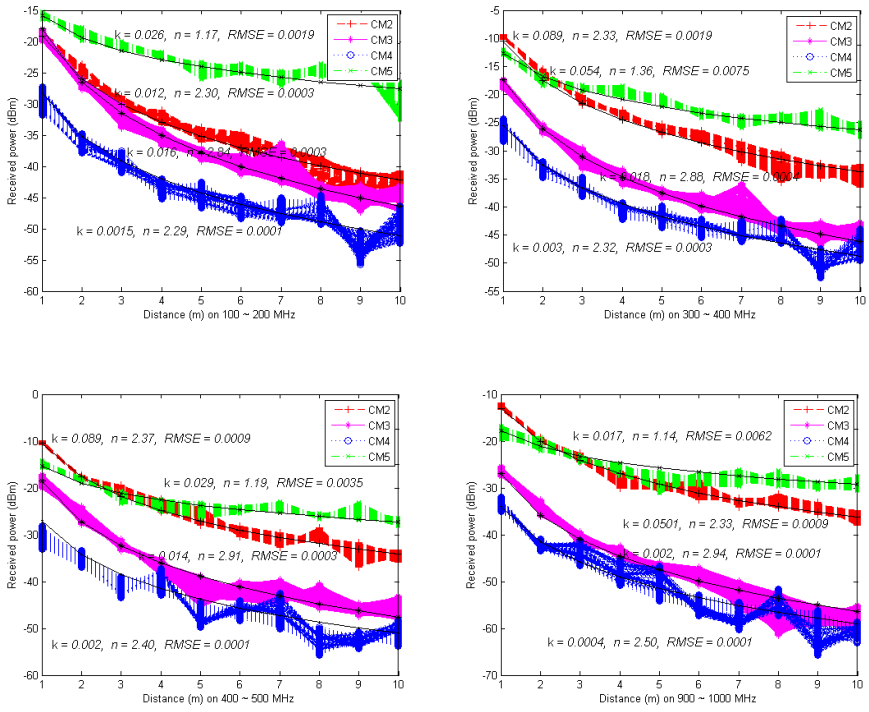


Figure 4.6 Example of LS-curve fitting on received power

Some researchers adopted the two-ray Rayleigh fading model to represent the digital channel for compromising emanation, in which the pathloss exponent n was a constant value of 2 [7, 24]. Other researchers took the value of *n* as 2 at 900 MHz and 2.2 at frequencies from 1.2 GHz to 4 GHz [25].

However, we calculated the pathloss exponent using LS-curve fitting with

the measured value of 500 points each CMs and frequency bands respectively. And then, we found that the pathloss exponent value ranged from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with propagation environments, such as an empty office, a concrete wall, a wood or metal door, or a glass window.

4.4 Conclusion

To propose the emission security limits, we set the target frequency bands from 100 MHz to 1000 MHz, firstly. Next, frequency correlation coefficients are calculated to find the representative frequencies at target frequency band for analysis pathloss characteristics on EMSEC-channel. The cross-correlation among the frequency tones is a little bit high from 0.6 to 0.9. We represented the nine representative frequencies as 200 MHz, 300 MHz, 400 MHz, 500 MHz, 600 MHz, 700 MHz, 800 MHz and 900 MHz on the basis of these results.

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable TRA. TRA is defined as the sum of all types of radio attenuations such as free space loss and additional radiation pathloss in the environment.

We calculated the pathloss exponent using LS-curve fitting with the measured value of 500 points each CMs and frequency bands respectively. And then, we found that the pathloss exponent value ranged from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with

propagation environments, such as an empty office, a concrete wall, a wood or metal door, or a glass window. CM3 and CM4 had a metal door and metal window frame between the TX and RX, respectively, in which the EMSEC-channel information was effectively shielded. We conjecture that CM3 and CM4 had relatively higher power attenuation than CM2 and CM5, which were composed of wood and concrete, respectively.

Chapter 5 Emission Security Limits for Compromising Emanations

5.1 Introduction

In this chapter, we present a periodic and aperiodic emission security limits using the measurement and analysis of electromagnetic emission security channel in chapter 4. Based on investigation about currently known security limits, suitable and actual security limits are proposed. These emission security limits can be used as the basis of the limited the leakage electromagnetic radiation of information appliance devices for authentication.

5.2 Parameters for Security Limits

In this section, we propose security limits on compromising emanation based on the measurement and analysis of the frequency correlation indoor EMSEC-channels, as described in Chapter 4.

Figure 5.1 shows the EMSEC system configuration at each stage for determination of emission security limits. EMSEC system' *SNR* is proportional to system gains such as antenna gain and signal processing gain, and inversely proportional to total radio attenuation in the radiation path and environmental noise strength [7, 25]. The *SNR* is defined as

$$SNR = \frac{E_{max} \cdot G_a \cdot G_p}{a_{total} \cdot E_{n,B} \cdot f_n}, \qquad (dB) \quad (5.1)$$

where, E_{max}= maximum field strength that the test standard permits

B = the impulse bandwidth used in the test

a_{total}= is defined by total radio attenuation(TRA) such as free space pathloss and additional radiation pathloss by the building walls

G_a = the gain of the best directional antenna that is feasible for use by the eavesdropper

G_p = the processing gain that can be achieved with techniques such as periodic averaging

$E_{n,B}$ = the field strength of natural and man-made radio noise at the location of the eavesdropping antenna within a bandwidth B

f_n = the noise factor of the eavesdropper's receiver

(5.1) can be expressed by the logarithm (dB) as following (5.2)

$$SNR = E_{max} + G_a + G_p - a_{total} - E_{n,B} - f_n, \qquad (dB) \quad (5.2)$$

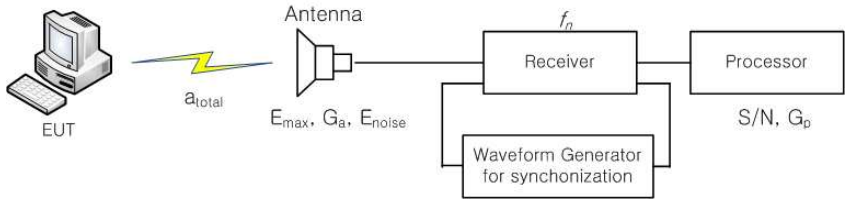


Figure 5.1 EMSEC's system configuration

This method consider that the minimal background noise that the eavesdropper faces even under good receiving conditions, the gain from antenna types that can be used covertly, and the gain from the use of suitable detection and signal processing methods for the signal of interest the closest distance between antenna and target device for which protection is needed. They achieved the signal-to-noise ratio that a radio-frequency eavesdropper under these conditions using (5.2).

Finally, we can obtain the emission limits level to derive each parameter to obtain the best signal-to-noise ratio from (5.2). Subsection 5.2.1~5.2.6 are presented the details of each parameter.

5.2.1. Total radio attenuation

The value a_{total} is defined by TRAs such as free space pathloss and additional radiation pathloss by the building walls. We assumed the maximum distance to be 10 m since the EMSEC system would not be closer than 10 m in indoor environments. Therefore, the TRA, a_{total} is defined at a representative frequency, f_r, receiver power amplitude k, and pathloss exponent n which are depends on channel environments as

$$a_{total} = PL(10, f_r) = 20 \cdot \log_{10} f_r + 10 \cdot \log_{10} k - 10 \cdot n. \quad (dB) \tag{5.3}$$

A comparison of the available literature on outdoor radio noise shows that rather limited data is available on indoor radio signal attenuations caused by building materials [7]. Previous work [1, 7, 24, 25] assumed that radio attenuations would have constant values. They mentioned that indoor ratio signal attenuation by building materials clear data are far less. They adjusted that the survey publications [32, 33] provide data for the frequency range of 900 MHz to 100 GHz, which is of particular interest to designers of mobile personal communicaiton systems and wireless networking applications [7]. However, this data shows only a few trends and mostly documents a significant variability between buildings. The survey [33] lists a number of alternative models that have been used to describe attenuation in buildings. Example values from published measurements mentioned in [33] include 1.4 dB for a cloth-covered office, 3 dB for wood and brick sliding, 7 dB for a 200 mm concrete block wall, 13 dB for another concrete wall, and 12 and 16 dB for floors in different buildings, where at 900 MHz, in addition to free sapce loss, attenuations of 10~25 dB have been reported. For the VHF frequency range, they found a study [34], which looked at 35 and 150 MHz signals from a far away station and found that signal levels inside buildings are in the order of 20~25 dB lower than outside in the street and that the building attenuation was in the range 5~45 dB in about 90 % of all measurements made with a sightly lower attenuation for 150 MHz. They want to ensure protection even for rooms whose attenuation by building materials is located in the lowest decile of the available statisics and therefore use total radio attenuation is 15 dB at 10 meter.

However, the radio attenuations have to be modelled as being normally distributed with a mean and variance determined through statistical evaluation of a large number of measurements in various environments. Accordingly, we measure and analyze the frequency correlation indoor EMSEC-channel under indoor environments. Based on these results, we found that the TRA in dB can be modelled as a random process that follows a Rician distribution at each channel. The cumulative distribution function (CDF) of the total radio attenuation with Rician fitting at CM2 at 400–500 MHz and CM4 at 900–1000 MHz is shown in Figure 5.2. The empirical CDF shows good agreement with the CDF of the Rician distribution.

Let *s* denote the direct-waves peak amplitude and σ denote the standard deviation of the overall total radio attenuation a_{total}, then the Rician *k*-factor is given as

$$k = \frac{s^2}{2\sigma^2}. \tag{5.4}$$

The Rician CDF is calculated as follows

$$C_{Rice}(a_{total}) = exp[-(k + \frac{a_{total}^{\ 2}}{2\sigma^2})]\sum_{m=0}^{\infty}(\frac{\sigma\sqrt{2k}}{a_{total}})^m I_m(\frac{a_{total}\sqrt{2k}}{\sigma}) \tag{5.5}$$

and $I_m()$ is a modified m-th order Bessel function of the first kind [31]. And Table 5.1 summarises the *s* and σ values of measured channels, the RMSE

of the measured results with Rician fitting result, and the 90% probability of TRA for each CM and frequency band.

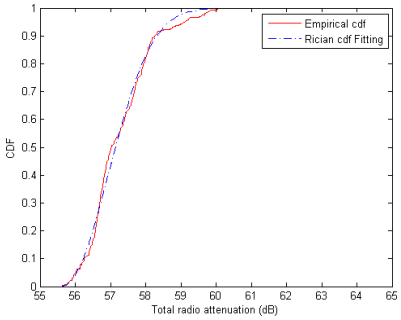
Table 5.1 Rician CDF parameters of indoor EMSEC-channel model

Frequency	CMs	s	σ	RMSE	TRA (dB)
100	CM2	0.77	1.18	0.06	41
–	CM3	0.84	1.25	0.02	43
200	CM4	2	2.17	0.05	48
MHz	CM5	2.6	2.44	0.04	29
200	CM2	0.03	1.05	0.06	33
–	CM3	0.51	1.09	0.17	42
300	CM4	1.64	0.90	0.03	48
MHz	CM5	0.66	1.30	0.04	24
300	CM2	0.40	1	0.06	32
–	CM3	0.70	1.20	0.03	42
400	CM4	1.86	2.07	0.05	47
MHz	CM5	1	0.87	0.03	24
400	CM2	0.23	0.71	0.02	31
–	CM3	2.73	1.59	0.06	45
500	CM4	1.46	0.86	0.05	50
MHz	CM5	0.39	0.67	0.04	25
500	CM2	0.94	1.53	0.049	30
–	CM3	2.36	1.21	0.024	51

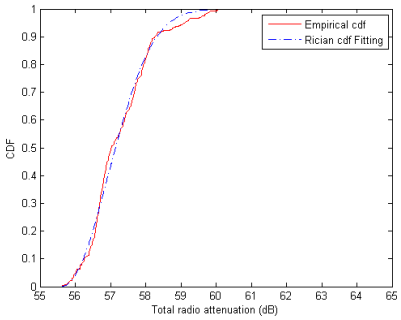
600 MHz	CM4	0.78	1.30	0.018	51
	CM5	0.59	0.70	0.021	24
600 – 700 MHz	CM2	3.47	2.79	0.042	36
	CM3	1.69	1.09	0.030	49
	CM4	3.01	1.89	0.063	51
	CM5	1.20	0.56	0.036	26
700 – 800 MHz	CM2	0.18	0.70	0.019	31
	CM3	0.99	1.89	0.032	51
	CM4	3.22	1.08	0.031	51
	CM5	0.66	1.08	0.032	29
800 – 900 MHz	CM2	1.92	1.03	0.063	29
	CM3	3.90	1.02	0.020	57
	CM4	2.05	2.02	0.016	52
	CM5	1.13	1.19	0.024	28
900 – 1000 MHz	CM2	1.1	1.01	0.03	34
	CM3	1	1.6	0.06	57
	CM4	0.99	1.05	0.02	57
	CM5	1.77	0.98	0.004	27

We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment : 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4,

and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.



(a)CM2 at 400–500 MHz (s = 0.23, σ = 0.71)



(b)CM4 at 900–1000 MHz (s = 0.99, σ = 1.05)

Figure 5.2 Rician CDF fitting of total radio attenuation

5.2.2. Radio noise

A standard survey-data reference for the noise levels to be expected in various environments throughout the radio spectrum exists in the form of

ITU-R Recommendation P.372 [35], which summarizes the results from numerous noise intensity measurements and categorizes their origin.

Environmental noise was the radio noise around the wireless information devices and eavesdroppers, and derived expressions presented in the ITU-R Recommendation P.372 [35]. Radio noise to the environment based on the recommendation of the noise can be expressed as follows:

$$E_{n,b}(dB\mu V) = F_a(dB) + 20\log f_{MHz} + 10\log B_{MHz} - 36.8, \qquad (dB) \quad (5.6)$$

where, F_a is external noise figure, f_{MHz} is frequency and B_{MHz} is receiver's BW. F_a is presented equation (5.7). External noise is shown by the following equation (5.7) on the recommendations

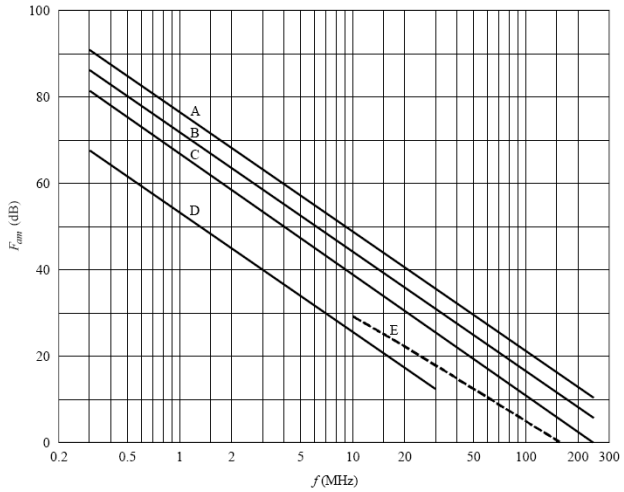
$$F_a = c - d \cdot \log(f) \qquad (dB) \quad (5.7)$$

where, c and d are constant values which are different by region and the value is categorized by commercial area, residential area, rural areas, not rural and cosmic noise in the from 0.3 MHz to 250MHz frequency band in Table 5.2 and Figure 5.3.

Table 5.2 Parameters c and d

Environment	***c***	***d***
Commertial area	76.8	27.7

Residential area	72.5	27.7
Rural areas	67.2	27.7
Not rural	53.6	28.6
Cosmic noise	52.0	23.0



A:commertial area, B: residential area, C: rural areas, D: not rural, E: cosmic noise

Figure 5.3 External noise figure corresponding to environment

5.2.3. Antenna gain

In the commercial market, the highest antenna gain in the 100–1000 MHz frequency band is commonly 17 *dBi* [36]; hence, we adopt an antenna gain, G_a, of 17 *dBi* for our target frequency bands to obtain rigorous emission security limits.

5.2.4. Signal processing gain

The advantage of signal processing, using various DSP to processes the digital signals that after digitized via AD converter signal of electromagnetic radiation that is received via the receiver shows the advantage to get through a method for improving the *SNR* of the signal.

The advantage of the signal processing, the signal of electromagnetic radiation that can be obtained through filtering, Correlation, and character recognition algorithms and averaging, generated from the information equipment such as a computer monitor, the same signal with a constant cycle to illustrate the form of periodic signals to be repeated. Averaging techniques is the most efficient method how to receive repeated signals of multiple periods continuously.

Received waveforms are mixed up noise component and signal component. Let us consider the case to match the phase of the signal to match with a plurality of cycles these received waveforms. Because the signal component is applied to the same phase, the voltage of the signal will be doubled. However, because it has a random phase to each other when it is assumed to be random noise, synthesis, noise component shows the effect of power is double the two signals having different phases. As a result, the signal voltage increased, power is increased, in the case of noise.

Thus, the advantages of the signal processing by these methods can be generalized as follows. We adopted an averaging technique as a post

processing method for image in order to improve the *SNR* of the reconstructed EMSEC-channel information. This method is a practical, highly effective, and widely used technique for increasing the *SNR* of a periodic signal, such as a signal generated by the image-refresh circuitry in VDUs [2, 7]. We used the common video resolution mode of 1280×1024 at 75 Hz, which is composed of 1,799,408 pixels [26]. G_p is defined as (5.8) [7]

$$G_p = 10 \cdot \log_{10} M, \qquad (dB) \tag{5.8}$$

where M indicates the number of the periodic signal applied to the correct phase. Since M is related to the available acquisition memory in the receiver as (5.9), we used high performance acquisition storage, which has a maximum memory of 512 MB and 12 bit resoultion, 2 byte is used for store. The maximum M is 213 and G_p is calculated about 23 dB using Equation (5.8).

$$M = \frac{512 \times 12bit \times 10^6}{1{,}799{,}408 \times 16bit} = 213 \tag{5.9}$$

As a result, the number of signal period which can be applied to the exact phase, is a primary parameter, the advantages of signal processing can be obtained by averaging technique method, when it was not applied to the correct phase in the course of the treatment is, it is possible to take advantage of the signal processing lower than this.

5.2.5. Minimum *SNR* for reconstruction

The final output of the reconstructed image after applying signal processing methods has been changed to a digital signal after the signal received by the antenna and receiver will have a certain amount of *SNR*, but if they will be recognized as the information.

Figure 5.4 shows the characteristics of the restoration image that is presented in the paper [7]. Vertical axis shows the *SNR* value, shown in 5 dB increments. In this example, must have a *SNR* of 10 dB or more, at least it is believed to be possible to recognize a correct character, and when you want to use a larger font and using such detection algorithm and character recognition than this is judged possible to character recognition in the signal lower *SNR*.

The paper of Markus, *SNR* of the restored image has been suggested that can be recognized as an information unless you 0 dB or more at least when you take into account the effect of improving a variety of multiple.

5.2.6 Receiver noise factor

A noise figure of receiver is the ratio between *SNR* at output and *SNR* at input on receiver. It is an index showing the effect of the noise by the receiver and a receiver having the lower noise figure is better.

We assume the attacker uses a receiver with a noise figure of f_n = 10 dB given for the Dynamic Sciences R-1250 and an impulse bandwidth of B = 50 MHz for same condition Kuhn's receiver noise figure [7].

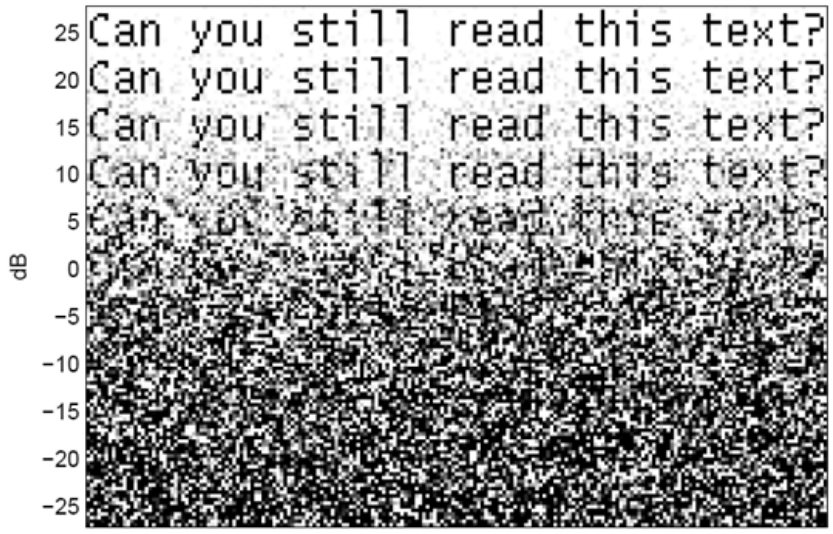


Figure 5.4 Video signal with varying *SNR*

5.2.7. Calculation of Emission Security Limit

Video display images are easily recovered by the periodic property of their EMSEC-channel information, whereas printer and fax images, which exhibit aperiodicity in their EMSEC-channel information, are reproduced by a single operation. From this point of view, the periodic emission security limit is considered to be the processing gain, G_p, when using the averaging image processing technique. However, it is difficult to obtain the processing gain for an aperiodic emission security limit. Hence, we apply a processing gain in order to divide periodic and aperiodic emission security limits. Emission security limits can be classified into confidentiality classes A and B. Class B

is for confidential equipment handling sensitive data; therefore, it requires stronger protection than class A [1].

Table 5.1 lists the TRA (a_{total}) from 100 MHz to 1000 MHz for each CM. a_{total} has a range from 24 dB at CM5 to 57 dB at CM3 and CM4. We calculated the emission security limits for class B using (5). E_{max} is 21 dBμV/m for class B at 200-300 MHz when the *SNR* is 0 dB, the receiver' s BW is 50 MHz, and the distance is 10 m. From (5.2), it is found that the emission security limits for class A are 45 dBμV/m on the same frequency band.

5.3 Proposed Emission Security Limits

In this subsection 5.2.7, E_{max} is 21 dBμV/m for class B at 200–300 MHz when the *SNR* is 0 dB, the receiver' s BW is 50 MHz, and the distance is 10 m. From (5.2), it is found that the emission security limits for class A are 45 dBμV/m on same frequency band. Because the general spectrum analyzers allow a maximum impulse BW of either 1 MHz or 5 MHz, measurements with a BW of 50 MHz are not possible using the commonly used spectrum analyzers. Therefore, the corresponding limit is 20 dB lower at a BW of 5 MHz [2]. We can therefore obtain the emission security limit for BW 5 MHz as 1 dBμV/m for class B and 25 dBμV/m for class A at 200–300 MHz .

Table 5.3 presents our calculated emission security limits using the frequency correlation indoor EMSEC-channel analysis at distance *d* of 10 m, a BW of 50 MHz and 5 MHz, respectively. We can ignore the ± 1 dB

interval of the calculated security limits to fall into several groups. For stricter emission security limits against eavesdropping, we selected a more rigid emission security limit by grouping.

Table 5.3 Calculated periodic emission security limits (unit : *dBμV/m*)

Frequency (MHz)	BW = 50 MHz		BW = 5 MHz	
	Class A	Class B	Class A	Class B
100-200	45	24	24	4
200–300	45	21	25	1
300–400	44	21	24	1
400–500	47	22	27	2
500–600	49	21	29	1
600–700	48	23	28	3
700–800	48	26	28	6
800–900	49	25	29	5
900–1000	55	25	35	5

Table 5.4 Proposed emission security limits (unit : *dBμV/m*)

Frequency (MHz)	Aperiodic EMSEC-channel information		Periodic EMSEC-channel information	
	Class A	Class B	Class A	Class B
100-200	47	27	24	4
200–400	47	24	24	1
400–600	51	24	28	1
600–700	51	26	28	3
700–900	51	28	28	5
900–1000	58	28	35	5

The periodic emission security limits for BW 5 MHz are 1, 1, 2, and 1 *dBμV/m* for class B in the 200–600 MHz, these can be grouped as 1 *dBμV/m*. In addition, the periodic emission security limits for BW 5 MHz are 27, 29, 28, 28, and 29 *dBμV/m* for class A in the 400–900 MHz range, these can be grouped as 28 *dBμV/m*. Similarly, the periodic emission security class limits for BW 5 MHz can be grouped 24 *dBμV/m* for class A in the 100~400 MHz. Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

Finally, we present our proposed periodic and aperiodic emission security limits in the target frequency bands using the frequency correlation indoor EMSEC-channel analysis at a BW of 5 MHz and distance *d* of 10 m in Table 5.4. In general, with existing EMC standards [4, 5], class B has a strict value 10 dB higher than class A without consideration of various channel environments. Class A and class B for the proposed emission security limits are influenced by the TRA, which is affected by the frequency and channel environment. Therefore, the difference in the emission security limits between class A and class B implies the difference between the maximum and minimum values of the TRA, which are affected by the channel environment and frequency band.

5.4 Comparison with Public Standards and Other Security Limits

5.4.1 CISPR22 and MIL-STD-461E

For comparison, we selected the CISPR22 class B standard [4], which is used globally as a radiated emission standard for IT equipment in commercial EMC standards, and the United States military EMC standard MIL-STD-461E/R102 [5] for mobile army and navy equipment radiation. Existing security limits [7, 25] and the civilian [4] and military [5] EMC standards are tunned to the same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits to prove their reliability and practicality. We have to take into account the different BW and antenna distances. To increase the impulse BW from 120 kHz for other EMC standards to 5 MHz for the proposed emission security limits, we have to raise the permitted field strength by 32 dB, in order to keep the equivalent spectral density constant. The limits have to be raised further by 20 dB to convert the measurement distance from 1 to 10 m [7].

The emission limits under the CISPR22 class B and class A standards are 62 *dBμV/m* and 72 *dBμV/m*, respectively, from 30 MHz to 230 MHz. For the CISPR22 class B and class A standards, the limits are 69 *dBμV/m* and 79 *dBμV/m* from 230 MHz to 1000 MHz, respectively. The MIL-STD-461E class B standard is 24 *dBμV/m* at 100 MHz, which linearly increases up to 32 *dBμV/m* at 1000 MHz. The MIL-STD-461E class A standard is 44 *dBμV/m* at

100 MHz, which linearly increases up to 52 *dBμV/m* at 1000 MHz at a distance of 10 m and a BW of 5 MHz.

Other measurement parameters of the compared limits such as the antenna gain, signal processing gain, both natural and man-made radio noise, and noise factor are used to determine the *SNR* for EMSEC system Eq. (4). Because the civil and military EMC standards [4, 5] consider the unintentional generation, propagation and reception of electromagnetic energy with reference to the unwanted effects to other IT devices, general EMC standards did not applied for these the measurement parameters because it does not take into account the *SNR*. In addition, other security limits [1, 7, 25] are applied by ITU-R P.372 [31] for natural and man-made noise factor as like the proposed security limits to consider the *SNR* and these security limits same as noise figure as our security limits.

Previous works and published EMC standards used the same security limit for all kinds of equipment in various environments. However, we proposed the emission security limits based on measurement and analysis of the EMSEC-channel in various real indoor environments. The proposed emission security limits are considered as the level of confidentiality and TRA based on the channel environment and frequency bands.

5.4.2 Security limits for Markus G. Kuhn

Most foreign countries classified for the leakage electromagnetic shielding

standards and criteria without disclosing. However, to present the related research in the field of academic methods and standards are often derived the leakage electromagnetic shielding standards. University of Cambridge, UK, Markus G. Kuhn presented these method his doctoral thesis and ITU-T K.84 is generated the test methods and guide against information leaks through unintentional EM emissions. In this section, these existing two security limits are explained

Markus method is presented by deriving the eavesdropper's the signal-to-noise ratio (*SNR*) that. Therefore, that method is to calculate the *SNR* of the obtained signal gain and the noise component from the target devices passing through antenna, receiver and signal processing device

To define stricter emission security limits than the EMC standards, for the worst case scenario we assumed that the *SNR* is less than 0 dB because of unreadable text for reconstruction [7], the receiver' s BW is 50 MHz, and the distance is 10 m. To protect the equipment against an EMSEC-channel attack, we calculated the maximum field strength, E_{max} which is the emission security limit, to satisfy $SNR \leq 0$ dB using the logarithmic equation (4).

In (5.2), E_{noise} and f_n are set to 27 dBμV/m and 10 dB, respectively, as given in [2]. In the commercial market, the highest antenna gain in the 100 MHz to 1000 MHz frequency bands is commonly 17 *dBi* [33]; hence, we adopt an antenna gain G_a of 17 *dBi* for our target frequency bands to obtain rigorous emission security limits. When in setting the standards for the Worst Case was mentioned represent the effect of 45 dB in 5 dB attenuation due to buildings in front of the building by at least 5 dB attenuation can be applied.

(5.2) assigned to each of these parameters was presented in front of the signal to restore requires at least 0 dB *SNR* final, you can get the upper level of electromagnetic radiation in Worst Case conditions for the protection of information leakage.

As a result, if the conditions set out above, the leakage electromagnetic wave generated by the information device to be released into the 1 *dBμV/m* or less, is the conclusion that can be protected against information leaks. The Kuhn' s security limit [7] is 1 *dBμV/m*, assuming a constant radio attenuation at a distance of 10 m and a receiver BW of 5 MHz in the VHF and UHF bands. In addition to, [25] proposes the security limit that is 49.5 *dBμV/m* from 100 MHz to 500, 50.7 *dBμV/m* from 500 MHz to 1000 MHz, and 56.8 *dBμV/m* at 1000 MHz. Because constant radio attenuation was not considered the influence of channel environment, the Kuhn' s emission security limit did not reflect the pathloss characteristics of the compromising emanation in a real environment.

5.4.3. ITU-T K.84 Guideline

A. The guiding concept

Whereas proposed method by Markus our is laid the foundation for computing the *SNR* with an emphasis on noise component that appears during signal transmission system, the provided method provided by NTT represents the shape of deriving a base shield on the basis of the minimum input level of the receiver. Also in this method, the parameters set the same system as

Figure 5.1, is considered are minimum receiver input voltage level and minimum *SNR* required to restore the signal.

B. Antenna factor

Antenna factor is a parameter showing the electromagnetic field generated around the antenna and is expressed by the following equation.

$$A_f(dB) = E(dB\mu V) - V(dB\mu V) \tag{5.10}$$

If the input impedance of the antenna is matched to 50Ω, with the gain of the antenna *G*, the antenna factor may be calculated as Equation (12) in general.

$$A_f = 20 \cdot \log_{10}(f[MHz]) - G - 29.79 \tag{5.11}$$

The most ideal antenna factor has a value of 0, which is a mode in which the output signal is generated by an electromagnetic field around without any loss. The antenna having the small antenna factor shows the high performance.

C. Minimum input voltage level

This parameter represents the sensitivity of the receiver and shows a minimum signal voltage level can be processed at the receiver. If the bandwidth is wider, the minimum input voltage level increases as fallen to its

characteristics sensitivity. The input voltage level of the signal has a form such as (5.12).

$$E_{\min} = V_{\min} + SNR + A_f \qquad (5.12)$$

Here, *SNR* is the strength ration between the signal required for signal reproduction and noise. In other words, performance is reduced to increase in noise so that a recognized signal noise is increased by the characteristic in response to the increase in bandwidth.

D. Minimum *SNR* for restoration

The NTT data has been presented classified into three types: a used receiver, is shown by dividing the *SNR* value that is required for signal recovery when using the receiver, respectively. Table 5.5 shows the required *SNR* for the each receiver.

Table 5.5 Examples of receiver and required *SNR*

Receiver	**Classification of Receiver**	**Minimum *SNR***
Receiver I	Amateur receiver	20 dB
Receiver II	General-purpose EMC receiver	15 dB
Receiver III	Special receiver for TEMPEST	0 dB

E. Maximum distance for restoration EMSEC signal

NTT document derived the maximum distance that can be restored the EMSEC signal.

(1) Antenna factor

They have selected the lowest antenna factor by investigating the Yagi antenna amateur radio for VHF bands. The selected antennas have the antenna factor from 2.2 dB at 144 MHz to 19.0 dB at 2.4 GHz.

(2) Minimum input voltage level

Checking the specifications of the receiver, minimum input voltage level was presented to -13 dBμV of 120 kHz receiver bandwidth in general. The reception bandwidth required at least 3 MHz to recover information from the received signal. The minimum input voltage level of the receiver is calculated (5.13).

$$-13+10\log_{10}(3\times10^{6}/1.2\times10^{5})=0.98\ dB\mu V \qquad (5.13)$$

(3) Calculation of limit level

Using the TEMPEST equipment, it is possible to restore the leak electromagnetic waves only *SNR* of 0 dB or more. It is assigned to derive equation (5.13) by obtained parameters , a limited level is obtained 3.18 dBμV at 144 MHz, 13.28 dBμV at 1.2 GHz

Compared with the class B and class A of VCCI, a Japanese EMI certification standards, the level is derived, if the EMSEC signal is radiated in a space surrounded by the reinforced wall, TEMPEST receiver as shown in Figure 5.5 it is determined that it is possible to restore and reception of signals up to about the 105 meter.

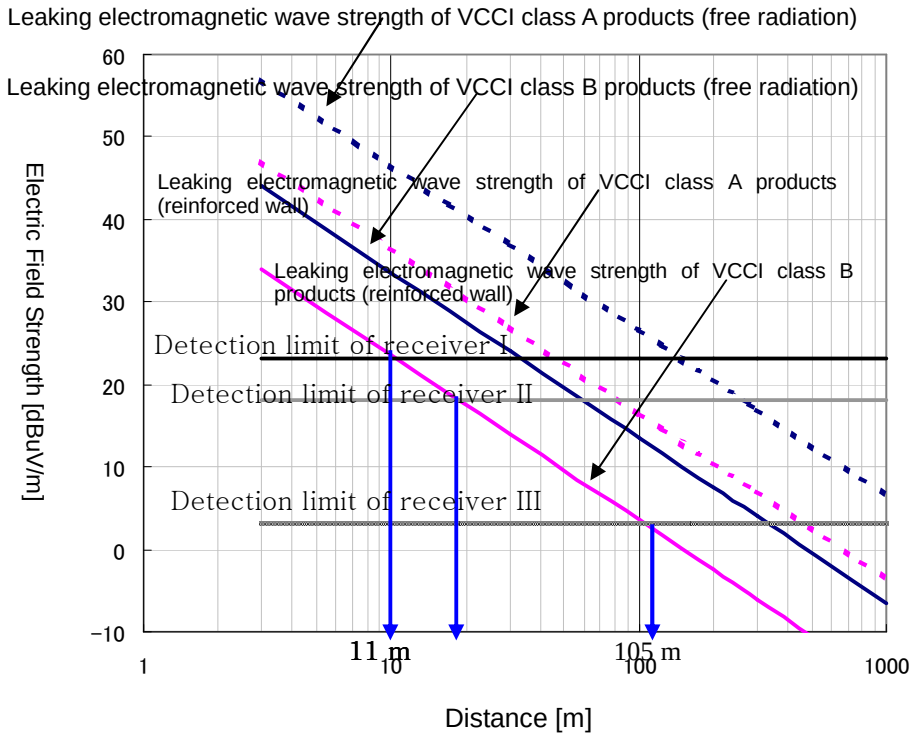


Figure 5.5 Relationship between possible electric field strength and distance for EMSEC

Fig. 5.6 shows the comparison between our proposed security limits and the other standards. The proposed periodic emission security limit for class B is

19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 0–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [25] is from 0.3 dB to 7.3 dB. However, Kuhn used the mimimum constant radio attenuation values to propose the security limits using the three survey documents [32,33, 34].

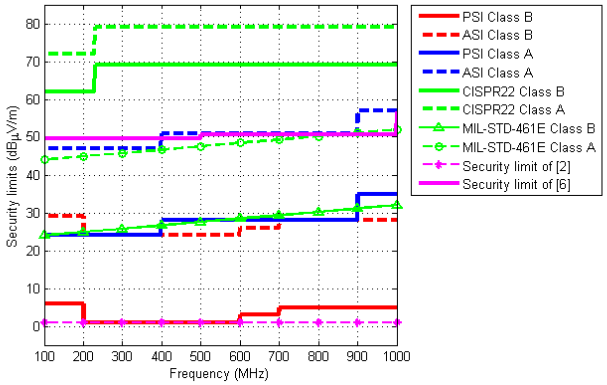


Figure 5.6 Comparison between our proposed security limits and other security limits and EMC standards

5.5 Conclusion

In this chapter, we present our proposed periodic and aperiodic emission security limits in the target frequency bands using the frequency correlation indoor EMSEC-channel analysis. In chapter 4, we measure and analyze the frequency correlation indoor EMSEC-channel under indoor environments. Based on these results, we found that the TRA in dB can be modelled as a random process that follows a Rician distribution at each channel. We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment: 29–41dB at CM2, a 42–57 dB at CM3, 47–57 dB at CM4, and 24–29 at CM5.

Emission security limits class A and class B are influenced by TRA which is affected by frequency and channel environment. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. And periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 900-1000 MHz, respectively. The difference with emission security limits of class A and class B implies the difference between the maximum and minimum values of the TRA which are affected by channel environments and frequency band. In addition, the differences with the PECI and AECI of emission security limits have the processing gain, 23 *dBi* owing to the redundancy caused by repetitive signals. So, that the PECI is easily leaked and

reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

For our proposed security limit's reliability and practicality, we compared the existing security limits, including the civilian and military EMC standards as same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits. The proposed periodic emission security limit for class B is 19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 2–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB only. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [6] is from 0.3 dB to 7.3 dB. However, Kuhn used the mimimum constant radio attenuation values to propose the security limits using the three survey documents [32,33, 34].

Chapter 6. Summary and further study

Radio wave is unintentionally emitted from information technology equipment. The important information can be reproduced by these received electromagnetic waves using the high sensitive antenna and receiver intentionally. This phenomenon is referred to as compromising emanations (CEs) or Electromagnetic emanation security (EMSEC).

While important documents related to these compromising emanations have been withheld from the public by military organizations. In addition, existing general EMC standards and security limits for compromising emanations are unsuitable for emission security purposes. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary. In our study, we focused on establishing the security limits for the compromising emanations in indoor environments.

Secondly, we represent how to build the EMSEC-system and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and PC monitors that you saw in Chapter 2. The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, RBW of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system.

Whereas, post-processing image restoration algorithm for a EMSEC system is a portion corresponding to the software of EMSEC system.

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system. But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic-compromising emanations need to be considered in order to establish emission security limits. We reconstructed the EMSEC-channel information from VUDs and printer using the averaging technique and proposed the adaptive deringing filter.

Next, we perform the electromagnetic emanation security (EMSEC)-channel measurements in the 100–1000 MHz frequency bands. Second, we analyze the pathloss characteristics of the indoor EMSEC-channel based on these measurements. We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). Also, the pathloss exponent value have a range from 1.06 to 2.94

depending on frequency band and the CMs, which in turn differed with propagation environments.

Through this EMSEC-channel analysis, we affirm that the total radio attenuation, which is one of the key parameters for determining the security limits for compromising emanations, follows the Rician distribution. However, previous work assumed that radio attenuations would have constant values. We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment, 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4, and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.

With these results, we propose that periodic and aperiodic emission security limits can be classified into two levels depending on the total radio attenuation and the extent of required confidentiality. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. Similarly, periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 700-1000 MHz, respectively.

Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

The proposed security limits are compared with other security limits and existing civil and military EMC standards as same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits. The proposed periodic emission security limit for class B is 19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 2–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB only. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [25] is from 0.3 dB to 7.3 dB.

Future works may include characterization and reconstruction of FAX, inkjet printer and other electronics. And it is need to EMSEC-channel analysis in more complex environments.

Bibliography

[1] *International Telecommunication Union*, "Test methods and guide against information leak through unintentional EM emission," in *ITU-T SG5*, *Rec. K.84*, Geneva, 2011.

[2] T. Tosaka, Y. Yamanaka, and K. Fukunaga, "Evaluation method of information in electromagnetic disturbance radiated from PC display using time varying stripe image," *IEICE*, 2010.

[3] *National Security Agency*, "Compromising emanations laboratory test requirements, Electromagnetics," in *NSTISSAM TEMPEST/1-92*, Dec. 1992.

[4] *International Electro-technical Commision*, "Information technology equipment, radio disturbance characteristics, limits and methods of measurement," in *IEC CISPR22 edition 6.0*, Sep. 2008.

[5] US Department of Defense, "Requirements for the control of electromagnetic interference characteristics of subsystems and equipment,", in *DOD MIL-STD-461E* Aug. 1999.

[6] R. M. Showers, "A comparison of military and civilian EMC standards," *IEEE Int. Symp. on Electromagn. Compat.*, pp.284-288, Aug. 1999.

[7] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," *Technical Report, UCAM-CL-TR-577*, Dec. 2003.

[8] Deborah Russell, G.T. Gangemi Sr. : Computer Security Basics. Chapter 10 : TEMPEST, O'Reilly & Associates, 1991.

[9] A. J. Mauriello, “Join a government program to unveil Tempest-spec mysteries”, *EDN*, Vo. 28, no. 13, pp. 191-195, June 23, 1983.

[10] Anton Kohling, “TEMPEST – an introduction and overview on compromising emanations, one aspect of information security”, *EMV*, Stuttgart, Feb. 1992.

[11] John Young, “How Old is TEMPEST?”, online response , Feb. 2000. http://cryptome.org/tempest-old.htm

[12] Wim van Eck, “Electromagnetic Radiation from Video Display Units : An Eavesdropping Risk?”, *Computer & Security*, vol. 4, pp. 269-286, 1985.

[13] W. Rankl, W. Effing, “Smart Card Handbook”, *John Wiley & Sons*, 2004.

[14] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis.” In Michael Wiener (Ed.), *Advances in Cryptology*. . *CRYPTO’99, LNCS* 1666, Springer, pp. 388.397, 1999.

[15] Suresh Chari et al., “Towards Sound Approaches to Counteract Power-Analysis Attacks.”, *Advances in Cryptology* . *CRYPTO’99, Proceedings, Lecture Notes in Computer Science* 1666, Springer-Verlag, pp. 398.412, 1999.

[16] T.S. Messerges, E.A. Dabbish, R.H. Sloan, “Examining smart-card security under the threat of power analysis attacks.”, *IEEE Tran. on Computers*, Vol. 51, No. 5, May 2002, pp. 541.552.

[17] Jean-Jacques Quisquater, David Samyde, “ElectroMagnetic Analysis (EMA): Measuresand Counter-Measures for Smard Cards.”, *Smart Card*

Programming and Security (E-smart2001), Cannes, France, LNCS 2140, September 2001, pp. 200.210.

[18] K. Gandolfi, C. Mourtel, F. Olivier, “Electromagnetic Analysis: Concrete Results.”, *CryptographicHardware and Embedded Systems* . *CHES* 2001, LNCS 2162, Springer, 2001, pp. 251.261.

[19] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi, “The EM Side-Channel(s).”, *4th International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS 2523, Springer, 2002, pp. 29–45.

[20] Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi, “Multi-channel Attacks.”, 5th International Workshop on Cryptographic Hardware and *Embedded Systems, LNCS* 2779, Springer, 2003, pp. 2–16.

[21] Suresh Chari, Josyula R. Rao, Pankaj Rohatgi, “Template Attacks.”, *4th International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS 2523, Springer, 2002, pp. 13–28.

[22] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanation of wired and wireless keyboards," *18th Int. Symp. USENIX*, pp.1–16, Mar. 2009.

[23] T. Tosaka, K. Taira, Y. Yamanaka, K. Fukunaga, A. Nishikata, and M. Hattori, "Reconstruction of printed image using electromagnetic disturbance from laser printer," *IEICE Trans. Commun.*, vol.E90-B, no.3, pp.711–715, Mar. 2007.

[24] D. G. Sun, W. Q. Huang, and Z. W. Zhao, "Modeling the radiated compromising emanation for digital channel," *IEEE Conf. on Robot., Autom. and Mechatronics*, pp.1–5, Dec. 2006.

[25] M. Zoyousefein, S. Hashemniaye, and A. Ghorbani, "Security limits for electromagnetic radiation from CRT displays," *2nd Int. Conf. on Comput. and Electr. Eng.*, pp.452–456, Dec. 2009.

[26] VESA and Industry Standards and Guidelines for Computer Display Monitor Timing, ver.1.0, rev.11, May, 2007.

[27] Michael Yuen, H.R. Wu, "A survey of hybrid MC/DPCM/DCT video coding distortions," *Signal Processing*, vol. 70, pp. 247-278, July 1998.

[28] *International Telecommunication Union*, "Examples for H.263 Encoder/Decoder Implementations," *in ITU-T Rec. H.263 Appendix III*, June 2000.

[29] A. Leon-Garcia, "Random Processes," in Probability and Random Processes for Electrical Engineering, *Addison-Wesley*, Reading, 1994.

[30] H. Arslan, Z. N. Chen, and M.-G. Di Benedetto, "Ultra Wideband Wireless Communication," pp.190, *John Wiley & Sons*, 2006.

[31] T. S. Rappaport, "Wireless Communications," pp.13–26, *Prentice Hall*, 2007.

[32] *International Telecommunication Union*, "Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz.", *ITU-R P.1238-7 Rec.*, Geneva, 2012.

[33] Homayoun Hashemi: The Indoor Radio Propagation Channel. *Proceedings of the IEEE*, Vol. 81, No. 7, July 1993, pp. 943–968.

[34] L. P. Rice: Radio Transmission into Buildings at 35 and 150 mc [MHz]. Bell System Technical Journal, Vol. 38, No. 1, January 1959, pp. 197–210.

[35] *International Telecommunication Union*, "Radio noise." *ITU-R SG3, Rec. P.372-7*, Geneva, 2001.

[36] Antenna Research Associate (ARA), "MWH SERIES antenna datasheets."

초 록

컴퓨터와 같은 정보통신기기를 사용하는 동안 비의도적으로 발생되는 전자파를 고성능의 수신기를 통해 수신하여 적절한 신호처리를 하게 되면 사용 중인 정보를 복원할 수 있다는 것이 여러 문서나 논문을 통해 많이 알려져 있다. 이러한 기술을 통한 기밀의 정보 누출을 방지하기 위해 미국을 비롯한 선진국을 중심으로 1950년대 중반부터 CE (Compromising emanation) 혹은 EMSEC (Electromagnetic emanation security) 로 일컬어지는 규제 기준을 제정하여 시행하고 있다. 가장 일반적으로 알려진 기준은 미국 NSA의 NACSIM 5100A와 NATO의 AMSG720B 등이 있으며, 그 내용의 일부를 제외하고는 실제 제한 기준레벨, 테스트 절차 등은 아직도 비밀로 취급되고 있다.

정보의 누출에 대한 보호레벨 수립을 위해 모니터 및 프린터 신호에 의한 전자파의 신호 주파수와 레벨을 정확히 측정함으로써 누출 가능성에 대한 평가가 이루어져야 하므로 2장에서는 모니터 및 프린터 신호 및 신호의 전송 및 처리 과정에서 자유공간으로 방사되는 전자파 신호의 특성을 분석하고, 신호레벨의 정확한 측정을 위해 필요한 조건들을 기술하였다. 탐지된 누설전자파 신호를 분석하여 3장에서는 그 신호 복원과정과 신호 이득을 높일 수 있는 후처리 과정으로 현재 가장 일반적으로 효과적인 *SNR* 이득을 얻을 수 있는 averaging technique 방법과 MPEG-4에서 이용하고 있는 후처리 과정중 하나인 deranging filter의 아이디어를 착안한 adaptive

deranging filter를 이용하여 모니터 및 프린터 신호에 대하여 복원 시스템과 복원영상 결과를 제시하였다. 실험결과, 후처리 이미지처리 기법으로 적응형 deranging 필터를 사용한 경우 후처리 이미지 처리를 하지 않은 복원 이미지와 비교 시 PSNR의 개선이 최소 2에서 최대 10만큼 개선됨을 알 수 있었다.

4장에서는 다양한 채널환경에서 측정된 데이터를 바탕으로 누설전자파 채널을 분석하고 주파수 상관성이 반영된 거리감쇄 수식을 제안했다. 이를 바탕으로 누설전자파 보호레벨 결정에 중요한 파라미터 중 하나인 총전파감쇠량(Total radio attenuation, TRA)이 주파수나 채널환경에 상관없이 상수값을 사용한 기존의 연구결과와는 다르게 총전파감쇠량이 채널과 주파수에 영향을 받는 값임을 밝히고 TRA의 확률분포값이 rician distribution을 따름을 확인했다.

5장에서는 후처리 신호처리 과정을 지난 누설전자파 복원영상의 *SNR*은 최소입력전압, 안테나 이득 및 신호처리 이득에 비례하고 총전파감쇠량, 배경노이즈 및 수신기 잡음레벨에 반비례함을 바탕으로 누설전자파 신호 특성과 신호의 중요도에 따라 class A와 class B로 나누어 주기신호와 비주기 신호에 대한 누설전자파 보호레벨을 제안했다. Class A의 주기성 누설전자파 방사보호레벨은 100-400 MHz에서는 24 $dB\mu V/m$, 400-900 MHz에서는 28 $dB\mu V/m$, 900-1000 MHz에서는 35 $dB\mu V/m$ 값을 각각 제안한다. 유사하게 Class B의 주기성 누설전자파 방사보호레벨은 100-200 MHz에서는 4 $dB\mu V/m$, 200-600 MHz에서는 1 $dB\mu V/m$, 600-7000 MHz에서는 3 $dB\mu V/m$, 700-1000 MHz에서는 5 $dB\mu V/m$ 값을 각각 제안한다.

주기성 누설전자파 방사보호레벨과 비주기성 방사보호레벨 간의 차이는 신호처리 이득인 약 23 dB 만큼의 차이가 발생되며 이는 주기성을 가지는 누설전자파 신호가 신호복원이 쉽기 때문에 강인한 보호레벨이 필요함을 말한다. 한편, class A 보호레벨과 class B 보호레벨과의 차이는 채널환경과 주파수, 신호의 보안정도에 의한 값의 차이임을 알 수 있다.

본 논문의 마지막은 우리가 제안한 누설전자파 방사보호레벨의 신뢰성을 확인하기 위하여 기존의 표준레벨인 CISPR EMC 기준값과 군에서 사용하고 있는 MIL-STD-461E 값 및 기존의 Kuhn의 방사보호레벨 및 ITU-T K.84의 방법을 함께 비교하였다.

주요어 : 누설전자파, 채널모델링, 주파수 상관관계, Rician 분포

학번 : 2006-30856

creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

공학박사 학위논문

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATION AND ITS RECONSTRUCTION

누설전자파를 위한 방사 보안 레벨 및 신호 복원

2013년 8월

서울대학교 대학원

Department of Electrical Engineering

Lee Hee-Kyung

공학박사 학위논문

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

누설전자파를 위한 방사 보안 레벨 및 신호 복원

2013년 8월

서울대학교 대학원

Department of Electrical Engineering

Lee Hee-Kyung

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

지도 교수 김 성 철

이 논문을 공학박사 학위논문으로 제출함

2013년 8월

서울대학교 대학원

전기, 컴퓨터공학부

이 희 경

이희경의 박사 학위논문을 인준함

2013년 8월

위 원 장 남 상 욱 (인)

부위원장 김 성 철 (인)

위 원 김 남 수 (인)

위 원 이 종 호 (인)

위 원 김 용 화 (인)

Abstract

EMISSION SECURITY LIMITS FOR COMPROMISING EMANATIONS AND ITS RECONSTRUCTION

LEE HEE-KYUNG
Department of Electrical Engineering and Computer Science
The Graduate School
Seoul National University

In this dissertation, reconstruction of electromagnetic emanation security (EMSEC)-channel information for video display units and printer are reconstructed using the averaging technique and proposed adaptive deringing filter. Also, emission security limits are proposed based on the analysis of the indoor EMSEC-channel. An emitted waveform from equipment which manages the important information can be detected and restored intentionally using the sensitive antenna and high performance receiver. These documents related to the EMSEC have classified by high confidentiality so that these are prohibited to publish by military organization. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary.

Firstly, we try to identify the exact a signal characteristics and the frequency components to measure and analyze the spectrum of electromagnetic waves which are contained information on personal computer (PC) and printer. The target devices are the desktop, laptop and laser printer which is generally used in the domestic offices in this study. The printer processed a large amount of information for a short period of time, there may be leaked the information in this process. To verify the leakage of electromagnetic spectrum that contains information, we measure and analyze the whole spectrum from 100 MHz to 1000 MHz.

Secondly, we represent how to build the EMSEC-system and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and video display unit (VDU) of PC. The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, resolution bandwidth (RBW) of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system. Whereas image restoration algorithm for EMSEC system as post-processing is a portion corresponding to the software of EMSEC system.

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective

and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system. But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic compromising emanations need to be considered in order to establish emission security limits. In addition to, we propose the adaptive deringing filter to reconstruct the EMSEC- channel information from PC and printer. We can obtain that the minimum peak signal-to-noise ratio (*PSNR*) enhancement is 2 and maximum *PSNR* enhancement is 10 compared with the original reconstructed image.

Next, we perform the EMSEC-channel measurements in the 100–1000 MHz frequency bands. Second, we analyze the pathloss characteristics of the indoor EMSEC-channel based on these measurements. We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). Also, the pathloss exponent value have a range from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with propagation environments.

Through this EMSEC-channel analysis, we affirm that the TRA, which is one of the key parameters for determining the security limits for compromising emanations, follows the Rician distribution. However, previous work assumed that radio attenuations would have constant values. We found that the TRA does not show significant differences depending on the frequency bands and

has the following range depending on the environment, 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4, and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.

Based on the experimental results of this study, we propose security limits on periodic as well as aperiodic EMSEC-channel information. The proposed security limits on compromising emanations are classified into two levels according to the TRA and the level of required confidentiality. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. And periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 700-1000 MHz, respectively.

Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits. We can then compare our security limits with other security limits and existing civil and military EMC standards.

Future works may include characterization and reconstruction of FAX, smartcard and other electronics. And it is need to EMSEC-channel analysis in more complex environments.

Keywords: Compromising emanation (CE), Electromagnetic Emanation security (EMSEC), Channel analysis, Rician distribution

Student Number: 2006-30856

Contents

List of Tables

List of Figures

Chapter 1. Introduction

The use of information and communication devices has raised over the years as accelerating the information age. Electronic devices has the convenient that can be handled quickly and easily, also has the risk of leakage by electromagnetic radiation which occurs when the data communication at the same time.

Such phenomena are referred to as compromising emanations (CEs) or electromagnetic emanation security (EMSEC) [1]. Information leakage from electronic equipment is achieved through the following path. Electronic equipment includes complex electronic circuitry inside. Within these circuits, electronic components such as central processing unit (CPU), memory, and oscillator component, and each part is built are connected by wires. The exchange of information between the wires, it is shown that the electromagnetic leakage occurs in this process. Leakage of electromagnetic waves that are generated by the baseband signal that is caused by a short rise time and falling time of the transients and harmonic components will have the same frequency components of the original signal. Therefore, electromagnetic waves were collected by a high-sensitivity receiver, which is also able to reconstruct the original signal using a simple signal processing process. In addition, the larger the size of the signal and the far the radiation of the electromagnetic. It is important to prevent equipment that is handling confidential information from emitting such unintentional electromagnetic

radiation.

We assumed that the location between the target information technology (IT) device and the antenna for eavesdropping is a communication channel [2], it is defined by EMSEC-channel. In addition, we regarded that the EMSEC-channel analysis to mean the analysis of the electromagnetic leakage signals from the electronic devices and EMSEC-channel attack is s any attack based on information gained intentionally due to unintentional electromagnetic radiation particularly in equipment that is handling important information. All electronic devices unintentionally radiate information-bearing electromagnetic waves, which is called EMSEC-channel information.

While important documents related to these compromising emanations have been withheld from the public by military organizations, basic information about these emanations has been declassified by the National Security Agency (NSA) [3]. However, information on the actual security limits and the test procedures used to determine those limits have been omitted from published versions, and some declassified documents cited only terminology and the widely known electromagnetic compatibility (EMC) test [4, 5]. In addition, there exist differences in test procedures, the type of detector used, and frequency ranges between the civilian and military EMC standards and security limits for compromising emanations [6]. Therefore, civilian and military EMC standards related to IT devices are unsuitable for emission security purposes [6, 7]. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary.

In order to take countermeasures to prevent information leakage due to electromagnetic information leakage will be preceded by a study about what frequency bands are weak at eavesdropping and some extent the level of information leakage. That is, to raise reasonable countermeasures on the based on the information about the leaked electromagnetic frequency range and the size of the signal leakage. Therefore, we measured and analyzed the electromagnetic spectrum of general IT and communication devices to identify the common characteristics of the leakage radiation leakage.

1.1 Historic background and previous work

Since at least the early 1960s, it has been known to military organizations that computer generate electromagnetic radiation that not only interferes with radio reception, but also leaks information about the data being processed. It has known as compromising emanations or Transient ElectroMagnetic Pluse STandard (TEMPEST) radiation, the unintentional electromagnetic broadcast of data has been a significant concern in sensitive military and diplomatic computer applications. TEMPEST, referred originally to a classified by US government program aimed at such EMSEC problems at developing protection standards. It has since then become a synonym for compromising emanations.

National compromising emanations test standards “NAG1A” and “FS22” is defined firstly by the US government in the 1950s and 1960s [8]. “National Communications Security Information Memorandum 5100: Compromising

Emanations Laboratory Test Standard, Electromagnetics" is revised in 1970 and a later version. "NACSIM 5100A" was defined in 1981. The names of the standards keep changing. "NSTISSAM TEMPEST/1-92" appears to be the current incarnation, of which extracts were declassified in 1999 [3]. However, the released parts reveal mostly only material that can also be found in the open computing, security, and EMC literature while the actual emanation limits, test procedures, and even definitions of some terms remain classified as military secrets. NATO equivalent "AMSG 720B", still classified documents and were therefore not accessible to the author [9, 10].

Electromagnetic radiation as a computer security risk was mentioned in the open literature as early as 1966 [11, 12]. But there is any kind of technical details on specific risks and eavesdropping techniques. The concept was brought to the attention of the broader public by a 1985 paper [12] and a 5-minute TV demonstration on the BBC program, in which van Eck demonstrated that the screen content of a video display unit (VDU) could be recovered at a distance using low cost home built equipment.

The most popular form of portable cryptographic module is the smartcard [13], a credit-card is shaped plastic card with embedded microcontroller. The type interfaces are either five electrical surface contacts for power supply, reset, ground, clock, and a bi-directional serial port or an induction loop. Research interest in compromising emanations from smartcards increased significantly when Kocher, Jaffe, and Jun [14] demonstrated the power analysis of high-frequency current fluctuations with cryptanalytic techniques on block ciphers. In their Differential Power Analysis attack, they

demonstrated the reconstruction of DES sub-key bits merely from access to a number of known plain or cipher texts, the corresponding power-line current curves and knowledge of the cipher algorithm being used. They showed that it is feasible to evaluate power-line information without prior reverse engineering of the low-level design of the executed software and that it is instead sufficient to look for correlations with single bits in intermediate results of the executed algorithm. The correlation process takes care of locating the specific machine instructions that leak the compromising energy. A number of improvements of the attack, attacks on other algorithms and countermeasure methods have been published since then [15, 16], including variants that measure magnetic-field fluctuations above the chip surface [17-20], as well as an attack on an SSL accelerator module inside a closed server from 5 m distance [21].

Several researchers have reported on electromagnetic compromising emanations from video displays [7], computer keyboards [22], and printers [23]. Sun [24] simulated the simple channel transfer function (CTF) of compromising emanations with a commonly used two-ray Rayleigh fading model. However, this model is too simple to reflect a realistically complex environment, and may give rise to some discrepancies between simulation results and real measurements. ITU-T SG5 [1] reported on the test methods and provided a guideline against information leaks through unintentional electromagnetic emissions. Kuhn [7] discussed security limit on video signals as compromising emanation. Although radio attenuation fluctuates according to the environment and distance between the transmitter (TX) and the receiver

(RX), these previous works [1, 7, 24, 25] assumed that the radio attenuations are constant in order to obtain security limit and guide test method.

1.2 Motivation and scope

In our study, we focused on establishing the emission security limits for the compromising emanations in indoor environments. Several researchers have been reported the dominant leakage frequency bands for various electronic devices [2, 7, 22, 23, 25]. Table 1 shows that the leakage frequencies have the range from 105 MHz to 950 MHz for several types of electronic equipment. Accordingly, we selected from 100 MHz to 1000 MHz in all the frequency bands because the compromising frequency bands are different from the confidential signals and the hidden antennas in device.

Table 1. Leaked frequencies of various electronic equipment types

Frequency (MHz)	Equipment	Reference
105–165	PS/2, USB and Wireless Keyboard	[22]
328.3	Laser printer	[23]
285, 324, 350, 648	Toshiba440 laptop	[7]
292, 480, 700, 740	Dell D1025HE monitor	
310–340, 440–475,	SONY VAIO PCG	[2]
775–810, 910–950	personal computer	

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). TRA is defined as the sum of all types of radio attenuations such as free space loss

and additional radiation pathloss in the environment. The expected noise level and attenuation values are random variables that, in the absence of better data, have to be modelled as being normally distributed with some mean and variance determined from the statistical evaluation of a large number of measurements in various indoor environments [7].

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system [2, 7, 25].

But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic-compromising emanations need to be considered in order to establish emission security limits. Based on the experimental results of this study, we propose security limits on periodic as well as aperiodic EMSEC-channel information. The proposed seculity limits on compromising emanations are classified into two levels according to the TRA and the level of required confidentiality. We can then compare our security limits with other security limits and existing civil and military EMC standards.

This dissertation is organized as follows: In Chapter 2, we investigate the characteristics EMSEC-channel information and detecet the EMSEC leaked freuqency band from VDUs and printer. In Chapter 3, detected EMSEC-channel information is reconstructed using the averaging technique and proposed the adpative deringing filter. In Chapter 4, we present the indoor EMSEC-channel measurement for compromising emanation on 100–1000 MHz. Also, we analyze the pathloss characteristics of indoor EMSEC-channel on the basis of experimental data. In Chapter 5, we find the random distribution of TRA and propose periodic and aperiodic emission security limits based on the 90 % TRA confidence level. In brief, we show the comparison between the proposed emission security limits and other security limits and EMC standards. Finally, in Section 6, we present our conclusions.

Chapter 2. Detection of Compromising Emanations

2.1 Introduction

The PC and Printer are the most frequently used IT devices around us. It is well known that the risk of information leakage by the leakage electromagnetic wave emitted from the VDU of PC in many researches. In case of PC, it is urgently needed to countermeasure which is possible for detection and reconstruction of important information from PC a long distance particularly.

We try to identify the exact a signal characteristics and the frequency components to measure and analyze the spectrum of electromagnetic waves which are contained information on PC. The target devices are the desktop and laptop which is generally used in the domestic offices in this study.

The printer processed a large amount of information for a short period of time, there may be leaked the information in this process. To verify the leakage of electromagnetic spectrum that contains information, we measure and analyze the whole spectrum.

In this study, only the first laser printer, to the parallel communication in the most widely used. Printer can be divided by the page printer and line printer depending on the printing method. The page printer refers to a laser printer to print the data you want to print a page-by-page. On the other hand,

line printers are dot matrix printers and inkjet printers to print line-by-line. According how to communicate with a PC, printer can be divided into parallel communication printer and serial communication printer, too. In this paper, the laser printer which are most widely used the parallel communication were included.

2.2 Compromising Emanations from Video Display Units

Firstly, we identify the basic theory of the VDU signal transmission arising from internal and external to infer the characteristics of electromagnetic waves caused by the leakage before measuring the leakage electromagnetic spectrum that occurs on PC.

2.2.1. Property of Video Display Units

A. VDU signal process

Figure 2.1 is shown on the process which VDU signal is generated the display by a PC monitor.

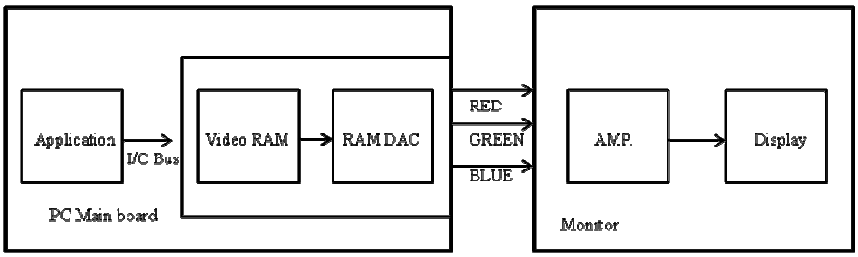


Figure 2.1 VDU Signal Process

(1) Signal process of PC

① The video data is generated by an application program

② Generated video data is converted in the form of video output to the monitor via video card.

③ Red, green, blue color data with the synchronization signal will be sent to the monitor at the same time.

(2) Signal process of monitor

① Received analog signal from the PC is changed adaptively and sent to the cathode ray tube (CRT) via the Main Board.

② Analog data is transmitted to the three electron guns at the rear of the CRT via main Board.

B. Characteristics of transmission signal

It is expected to occur mainly electromagnetic leakage in the process signal amplification to fit inside the CRT and emission part of the PC and the monitor connection.

2.2.2. Leakage path of Video Display Units

A. Signal leakage causes

Leakage electromagnetic waveform occurs in PC clock oscillator, Digital ICs, switching power, and the electromagnetic waves that occur on the inside of the unit flows through the input/output (I/O) cables, power lines, or PCB. Conducted signal is radiated into free space through PCB that acts as an

antenna or power line cable, I/O signal. It mainly takes place radiation where the change in impedance such as the power line or PCB, I / O cable and the junction of the wires or connections.

B. Signal leakage path

Leakage electromagnetic waveform from the PC, monitor and peripheral devices conducted and radiated directly or indirectly external signal lines, ground or power lines, etc.

(1) Desktop

Desktop is connected to longer cable and more many cables comparing Laptop. Whereas liquid crystal display (LCD) uses the characteristics of the electric field along the direction of the change in the molecular arrangement of liquid crystal using low voltage signal, CRT is amplified by the large voltage causing the electron beam from the electron gun emitting a fluorescent screen. Therefore, electromagnetic waves emitted from CRT will appear larger than the LCD monitor.

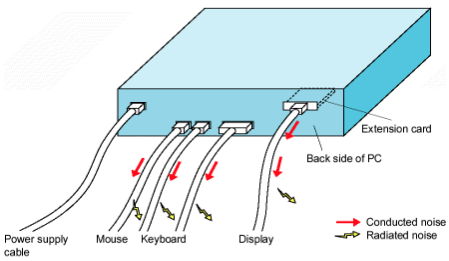


Figure 2.2 Desktop signal leakage paths

(2) Laptop

Electromagnetic waveform from the body of the laptop and the cables is radiated and the cable between the LCD panel and the laptop body are emitted. The laptop operates as a high-speed signal. Because the case is made of plastic, it does not have the shielding effect and is radiated a high level of electromagnetic waveform from the computer generally.

Many cable is connected, so it is occurred the electromagnetic radiation from the cable.

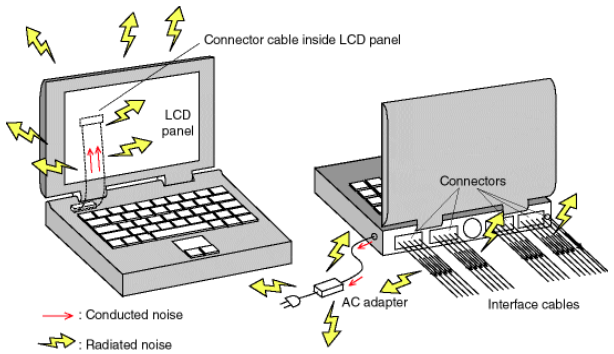


Figure 2.3 Laptop signal leakage path

2.2.3. Measurement system

We carried the measurement at International Radio Interference (CISPR) Special Committee recommended 3×3 m standard electromagnetic anechoic chamber (Semi-Anechoic Chamber) in National Radio Research Laboratory. Height of antenna is 1 meter and the distance between antenna and target

device is 1.5 meter. VDU has the ‘H’-pattern which is commonly used for electromagnetic interference (EMI) experiment.

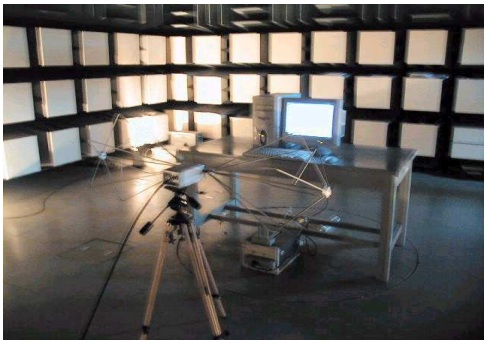


Figure 2.4 Equipment installation for VDU in chamber

EMI Test Receiver (Rohde & Schwarz, ESI 40) is used and Biconical Antenna (EMCO, 3109) is scanning up to 100 MHz. From 100 MHz to 1 GHz scanning is used for log periodic (LP) Antenna (Rohde & Schwarz, HL223).

In order to analyze the characteristics of electromagnetic radiation in the signal transmission cable, electrical analysis was performed about the transmitted signal.

Table 2.1 Parameter setting of EMI receiver for VDU

Center frequency	Detected EMSEC-channel information
Frequency span	1 MHz or Zero Span
Resolution Bandwidth	100 kHz or 120 kHz
Video Bandwidth	3 kHz
Sweep Time	100 ms

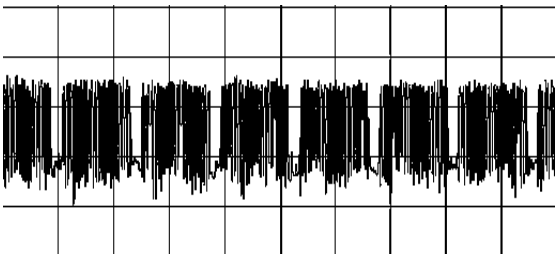
Figure 2.4 shows the measurement installation of VDU in semi-anechoic chamber and Table 2.1 explained the parameters of EMI receiver for detecting VDU leaked signal

2.2.4. Measurement result

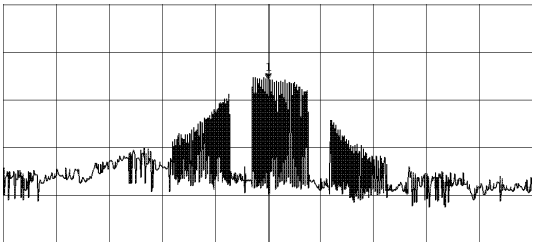
In order to distinguish the leakage electromagnetic signals and other electromagnetic signals, we have to select the primarily electromagnetic leaked frequency. The methods of measuring frequency are followed this process. In order to check the leakage of electromagnetic signals by the monitor signal, we used the frequency domain signal from spectrum analysis device.

In general, the video signal is sent 60, 75 or 85 times per second to the monitor. To configure each screen, the video signal is called a frame. Silence the (BLANK Time) between the frame and the frame is presented and accounted for the entire time frame of usually about 3.3% to 7.2%. This part is no signal, regardless of the content of the video signal.

If you scroll on the screen that displays the 'H' pattern can properly adjust the settings of the spectrum analyzer to determine the leakage electromagnetic waveform of video signal. Figure 2.5 shows the leakage of electromagnetic waves, this pattern is 1024 × 768 @ 60Hz video mode shown in the waveform.



(a) SPAN = 0 MHz

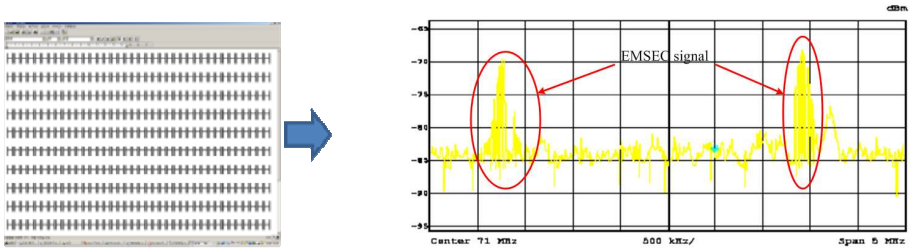


(b) SPAN = 1 MHz

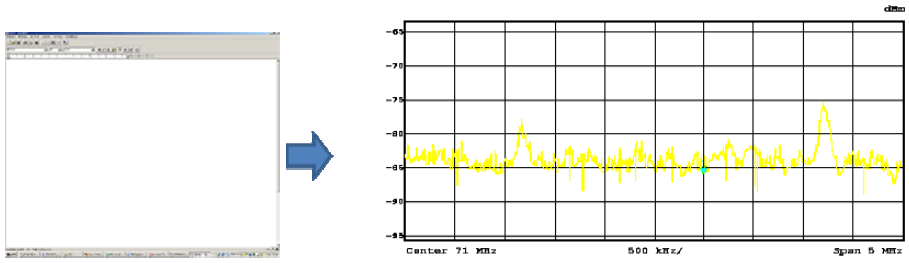
Figure 2.5. Leakage electromagnetic waveform from VDU

As shown in Figure 2.5, the leakage electromagnetic signals show two properties. The empty spaces appear in the middle of the first signal caused BLANK Time between frames. Approximately every 1.6 ms for each cavity appears in Figure 2.5, the full width (SWT is 100ms), the video signal has a refresh rate of 60Hz (i.e., the frame is repeated every 1/60s = 17 ms). This feature is more evident when the receiver's SPAN to 0 MHz in Figure 2.5 (a). This feature is one of the most obvious characteristic that distinguish the leakage electromagnetic signals. Figure 2.6 shows an experiment of a spectral analysis of EMSEC-channel information at 71 MHz center frequency from a desktop computer (Samsung Magicstation DM700) having the ‘H’-pattern video screen (a) and clear mode video screen (b). If the screen is changed, it

may be changed the compromising emanation spectrum. And we search for leakage electromagnetic frequency and record accurately the measurement frequency 100 MHz to 1 GHz.



(a) Radiated electromagnetic waveform at ‘H’-pattern



(b) Radiated electromagnetic waveform at clear mode

Figure 2.6 Measurement of radiated electromanetic at VDU

2.3 Compromising Emanations from Printer

2.3.1 Property of Printer

It is shown that the execution of print command from the PC to the printer

and the print data process in Figure 2.7.

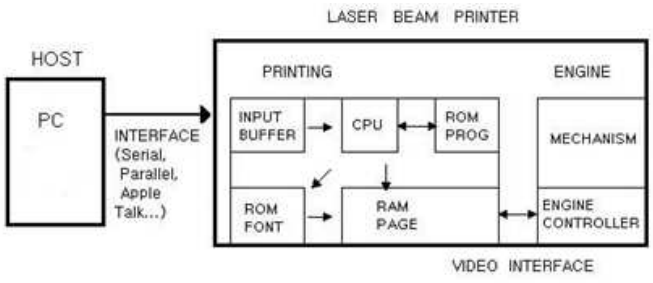


Figure 2.7 Printer data transmitting process

The detailed process was categorized depending on the subject to process the data into process in PC and process in printer, respectively.

A. Process in PC

① The print command from your PC

② The printer driver converts the document to page description language (PDL).

③ The created data is sent to the printer controller through communication cable.

B. Process in Printer

① Data received from the computer is stored in the input buffer in printer.

② The data received in the input buffer is analyzed by the emulator in the program read only memory (PROM).

③ According to the analyzed data, data of the actual contents for print are

stored in the page memory.

④ After confirming the ability of engine to print, data send to the engine.

⑤ Engine controller operates the engine mechanism and received data from the printing controller prints.

C. Characteristics of the transmitted signal

In case of internal signal of PC, The document by the internal printer drivers is converted to PDL, and this data is stored on the hard disk drive (HDD). The data stored in the input buffer analyzes and sent to the engine for print.

2.3.2 Leakage path of printer

The circuit inside the printer is divided into data controller that is responsible for processing and the print engine unit. Control unit printed circuit board (PCB) is built-in device, such as processor, memory and rashes, many types of devices.

Electromagnetic leakage occurs at the junction. The connection cable also helps to act as an antenna, so that the transmitted signal is radiated into space. In other words, the longer the length of the wire, electromagnetic occurs more.

The connector that is connected with a PC and input of the engine can be estimated that the source of the leakage of electromagnetic waves emitted from the printer as shown Figure 2.8. Because it does not exceed the 5V, it seems unlikely far enough to radiate like the VDU leaked signals.

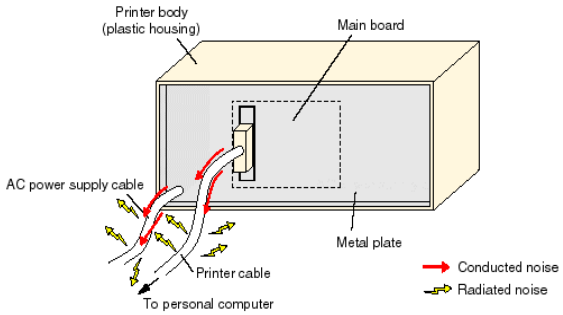


Figure 2.8 Leakage path of printer

2.3.3 Measurement system

We carried the measurement at International Radio Interference (CISPR) Special Committee recommended 3×3 m standard electromagnetic anechoic chamber (Semi-Anechoic Chamber) in National Radio Research Laboratory. Height of antenna is 1 meter and the distance between antenna and target device is 1.5 meter. VDU has the 'H'-pattern which is commonly used for EMI experiment.

EMI Test Receiver (Rohde & Schwarz, ESI 40) is used and Biconical Antenna (EMCO, 3109) is scanning up to 200 MHz. From 200 MHz to 500 MHz scanning is used for LP Antenna (Rohde & Schwarz, HL223).

In order to analyze the characteristics of electromagnetic radiation in the printer, we measured the HP 2100 laser printer, FAX 2850 (Brother laser printer), LAZETT ML-5000A (Samsung laser printer) and GLP 860 (LG laser printer). Table 2.2 explained the parameters of EMI receiver for detecting

printer leaked signal

As a result, the specific signals did not occur over the 500 MHz frequency band the measurement of the entire spectrum from 20 to 1000 MHz. Therefore, the measurement frequency range below 500 MHz, and 25 MHz intervals were measured precisely.

Table 2.2 Parameter setting EMI receiver for printer

Reference Level	-30 dBm
SPAN	30 MHz
RBW	100 kHz
VBW	3 kHz
SWT	100 ms

2.3.4 Measurement result

As described above, the printer is connected in parallel communication with PC. Parallel communication is a method of transmitting separately the lines of eight numbers of ways to send 1- Byte information different from the serial communication. Therefore, it is expected to appear in the mixed form of frequency components are mixed, when analyzing the signal from the frequency domain.

In order to measure the electromagnetic radiation generated during operation of the printer, we used a digital oscilloscope for measuring and analyzed the frequency components by measuring the pattern of the time

domain of the printer. Also we have used the ‘H’-pattern which is used in EMI test in general.

Figure 2.9 represents the frequency components by measuring the pattern of the time domain of the printer by fast fourier transform (FFT) using digital oscilloscope. Printed image is 12 font ‘H’-pattern as like the monitor case and waveform voltage is about 2.5 V. When we printed the ‘H’-pattern, the number of vertical pixel is same as the number of signal bearing waveform. It is determined that printed image can be recoverable to restore the signal using a measure EMSEC waveform from printer. Figure 2.10 (a) shows the fundamental frequency is 7.3 MHz EMSEC waveform and blue lines means no printer signal. Also, it found that the electromagnetic emanation from printer is detected by multiplying frequencies of the fundamental frequency in Figure 2.10 (b).

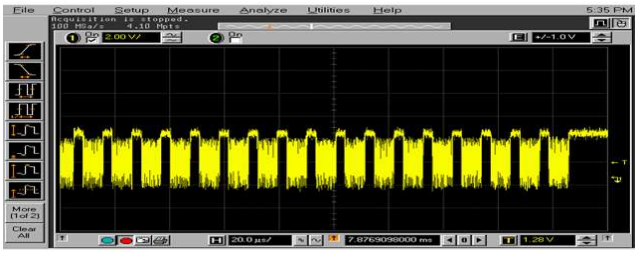
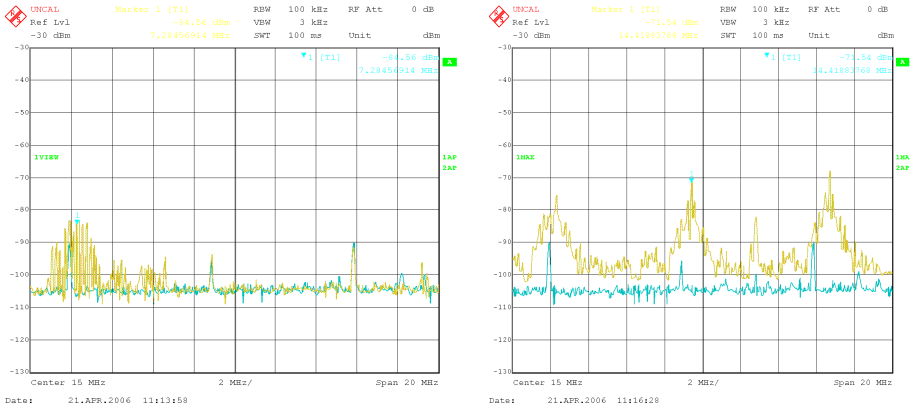


Figure 2.9 Printer radiated spectrum using the oscilloscope



(a) Center frequency : 7.3 MHz (b) 7.3, 14.4, and 21.7 MHz (Maxhold)

Figure 2.10 Printer radiated spectrum using the EMI recevier

2.4 Conclusions

In order to establish a emission security limits of protection against leakage of information, it must be preceded to accurately measure the frequency and level of the signal of the radio wave signal by the printer and the monitor. Also, it should be most advanced in order to measure the EMSEC-channel information from monitor and it must accurately detect the radiated EMSEC-channel information.

When radiated EMSEC-channel information is receiving, it is difficult to find a signal directly based on the only spectral characteristics. So that we measure the pattern in the time domain of the EMSEC-channel information from monitor firstly, and then analyzed the frequency components. Frequency component of EMSEC-channel information from the monitor have a frequency component of harmonic waves of the fundamental frequency.

Changing the 5MHz, 25MHz, and 50MHz SPAN of receiver to explore the radiated EMSEC-channel information from the monitor, we detected by determining the presence or absence of the signal under the display ‘H’-pattern and white pattern. Detected the EMSEC-channel information from monitor shaped the characteristics Vertical Blank Time of (VBT) and Horizontal Blank Time (HBT). The finer vertical line represents the HBT and the envelope of wider line means the VBT.

A measurement result of the radiation electromagnetic spectrum from the printer, it was found to exhibit properties entirely different form of radiation electromagnetic spectrum in the VDU. The main reason for this difference in leakage electromagnetic spectrum characteristics are displayed, it is different for transmitting method of signal.

Since the VDU signal is also sent in three lines R, G, and B, the signal is a synchronized and has the same frequency components. It can be interpreted as one signal component. It is because must undergo further a process of separating the signal eight different electromagnetic radiation one was collected. As a result, reconstruction and receiving electromagnetic radiation of parallel communication signals will become more complex than processing a VDU signal described earlier.

The measured bandwidth of radiated electromagnetic spectrum is about 7.3 MHz and frequency band is from 5 to 300 MHz. Since general form of the information bearing spectrum is also displayed in a round semicircular by showing a bandwidth, it is possible that information is contained this frequency band.

Chapter 3. Reconstruction of Compromising Emanations

3.1 Introduction

In this chapter, you will learn how to restore the system configuration and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and PC monitors that you saw in Chapter 2.

The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, RBW of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system. Whereas, image restoration algorithm for EMSEC system as post-processing is corresponded to the software of EMSEC-system.

That is, the signal processing gain means that to obtain a better *SNR* of the signal by utilizing a variety of a digital signal processing (DSP) processes the digital signals that after digitized via converter analog to digital (AD) signal of electromagnetic radiation that is received via the receiver.

The signal processing gain can be obtained through filtering, correlation, and character recognition algorithms and averaging technique, generated from the information such as a computer monitor, the same signal with a constant

cycle to illustrate the form of periodic signals to be repeated. Averaging technique is presented in the most efficient method how to receive repeated signals of multiple periods continuously.

In this chapter, we introduce how to restore the EMSEC signal from video display system and printer using the image process.

3.2. EMSEC system for Reconstruction

In this study, the data were processed using the of the Agilent vector signal analyzer vector signal analysis (VSA) for receiver. That has the 36 MByte RBW. LP antenna is used for compromising electromagnetic for video signal reconstruction and LP antenna is used for compromising electromagnetic for printer signal reconstruction, respectively. Controller is used for NI-5412 which has the 50~200 MSamples/sec sampling rate, amplitude resolution is 12 bit, and data storage memory is 512 Mbyte. Also, vertical synchronization board is used for NI-5124 arbitrary waveform generator which has the 100 MSamples/sec sampling rate, μHz resolution. Signal processing and analysis tools are implemented by Labview 7.0 as shown Figure 3.1.

3.3 Reconstruction of Compromising Emanations from Video Display Units

3.3.1 Characteristics of EMSEC-channel information from VDUs

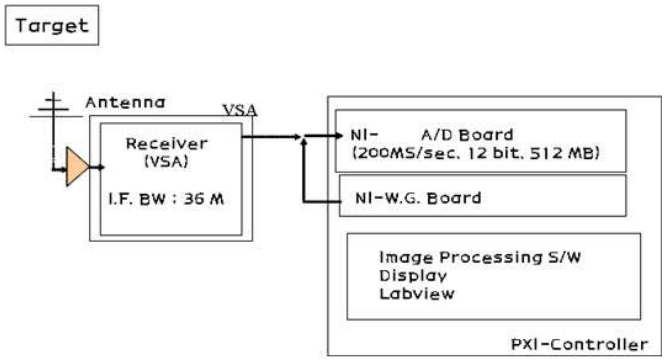


Figure 3.1 Reconstruction of EMSEC-system

Monitor signal which are commonly used refers to an analog monitor signal, and there are the three signals: Red, Green, Blue, Horizontal and vertical sync signals. In the paper, three different video data signal is directly related to the information that is displayed on the monitor.

Generally, a color monitor in each of the three video signals can be displayed with up to 256 levels. As a result, a total of 16,777,216 (256 × 256 × 256) different color are represented. In other words, the number of colors used by Windows when set to 24-bit True color or more, each of the R, G, B signal is a signal with a level of 256.

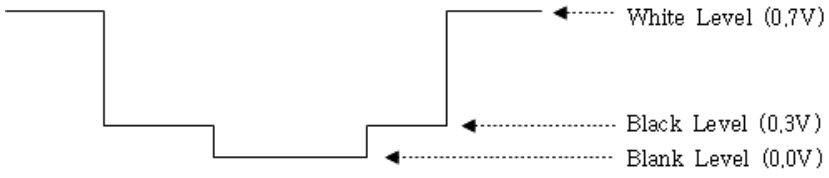


Figure 3.2 Video signal voltage waveform

Figure 3.2 shows the physical waveform of the video signal. If you are using a 24-bit true color video signal from 0.3V to 0.7V, 0.4V evenly divisible by 256 levels and the video level is transmitted at each voltage level. This level represents the saturation of each colors, saturation signal 256 having the highest saturation signal is set to 0. For example, a pure red to represent color saturation of 200 of each of the R, G, B signal should be sent as follows.

Serial form of a monitor signal is sent to the monitor, the transmitted signal consists of interlaced video, such as in Figure 3.3. Therefore, each line of the video signal being sent is sent sequentially.

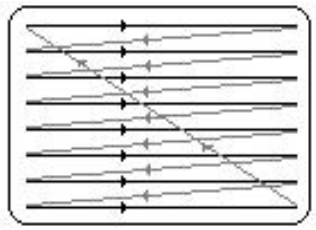


Figure 3.3 Interlaced video display

Vertical blank time is moving time from the end of the line for the first time at the end of the next line. And Horizontal blank time is moving time physically from last line of the first line of the next row and need time to move to the first line of the row. During this time, the data will not be sent. Thus, the video signal is sent through the cable is in the form as in Figure 3.3 [26].

The data in the Figure 3.4 represents one line of the monitor image from the

mainly used in monitor mode 1024 × 768 resolution, these lines are configured into 768 lines of 1024 pixels. Thus, this data is different depending on your monitor resolution indicates the number of pixels.

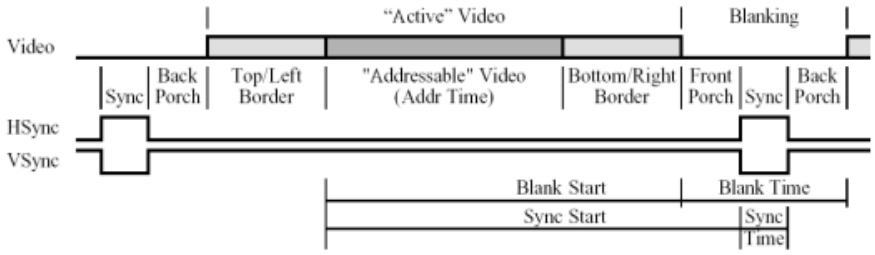


Figure 3.4 Form of video signal

As a result, the frame signal consists of 786,432 (1024 × 768) pixels and 58,982,400 (786,432 × 75) per second to transmit signals using 75Hz refresh can be converted to a frequency of about 59 MHz. Considering the horizontal and vertical blank time, the actual transmission frequency of the signal is higher than previously calculated value.

To predict the leakage electromagnetic radiation frequency of the video signal, the frequency of characters to be represented on the actual monitor, depending on the number of pixels, F_v, (3.1).

$$F_v = \frac{Pixels\ of\ clock}{Number\ of\ character} = \frac{F_{pix}}{N_{char}} \tag{3.1}$$

When video mode is 1024 × 768 at 60 Hz using the ‘H’-pattern, fundamental

frequency can be estimated by

$$F_v = \frac{25.175\ MHz}{8\ pixel} = 3.15 MHz / pixel \tag{3.2}$$

We can estimate the leaked frequencies from VDU using (3.1) and it can be estimated to detect harmonic frequencies of fundamental frequency. Also the harmonic signal amplitude is usually smaller than the size of the center frequency generally. For this reason, it can be limited to 1GHz or less from the 100 MHz frequency band to be measured.

3.3.2 Reconstruction result

To improve the performance of leakage electromagnetic signals reconstruction, RBW of receiver, signal processing gain, and antenna sensitivity are major elements. High RBW receiver or high gain antenna are approaching the hardware part to enhance the performance of reconstruction system. On the other hand, post processing for increasing the signal processing gain is software part of the leakage electromagnetic signal recovery system. In other words, signal processing gain is to improve the *SNR* of the signal using a variety of DSP processing. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals having independt noise. That method is a practical, highly effective and widely used technique for increasing the *SNR* of a periodic signal, such as

that generated by the image-refresh circuitry in a video display system [2, 7].

Signal processing gain can be obtained through filtering, correlation, averaging technique, and character recognition algorithm. Averaging technique presented in the most efficient way because the leakage electromagnetic signals from a VDUs have the form of a periodic signal, the same signal repeated with regular intervals. Figure 3.5 shows the experimental results on the real-time signal using the averaging technique.

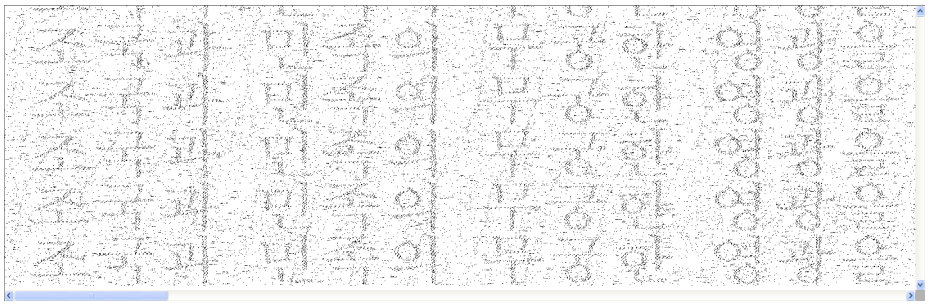


Figure 3.5 Reconstruction image using averaging technique

3.4 Reconstruction of Compromising Emanations from Printer

3.4.1 Characteristics of EMSEC-channel information from Printer

The photosensitive part of laser printer formed the latent image by generating a photo current in the drum by scanning the laser beam on the

drum. It is displayed as the difference of voltage. The semiconductor laser can be turned ON / OFF by modulating the input current. Semiconductor lasers are commonly used as a light source [23].

In this paper, it is recognized as part semiconductor diode optical section as shown Figure 3.6 the cause of the major leakage electromagnetic wave leakage in laser printer. In order to measure the electromagnetic radiation generated during operation of the printer, we used a digital oscilloscope for measuring and analyzed the frequency components by measuring the pattern of the time domain of the printer. Also we have used the 'H'-pattern which is used in EMI test in general.

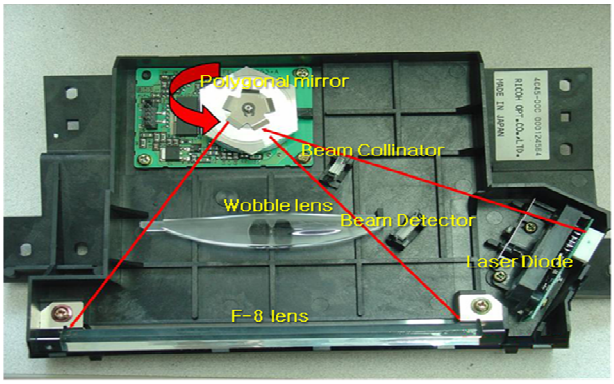
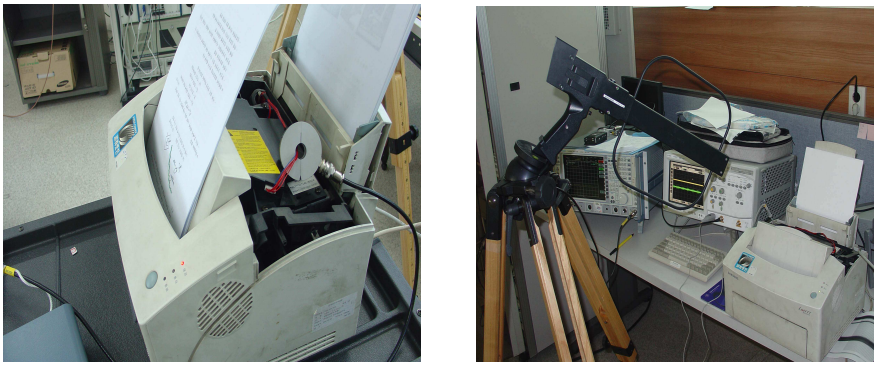


Figure 3.6 Optical part of the laser printer

Because it is transmitted serially in laser printer, the laser printer can be detected and recovery in a similar manner as video display units. However head driver chip is built in the head in inkjet printer (HP Photo 948C), signal can not be detected. In addition to, signal which is transmitted to the nozzle is sent in parallel . It is impossible to restore the receiving the signals. In this reason, we focus on the laser printer for detecting and reconsturction.

We measure the magnetic field range round 5 MHz-300 MHz to reconstruct the leakage of electromagnetic radiation signal printer. A current probe and loop antenna are used for detecting the EMSEC-channel information from printer as shown Figure 3.7. And Table 3.1 summarized the equipment parameters for printer measurement. Figure 3.8 shows the EMSEC-system's GUI and reconstruction results of spectral measurements of the time-domain electromagnetic radiation printer.



(a) Using the current probe (b) Using the loop antenna

Fig 3.7 Measurement for EMSEC signal from laser printer

Table 3.1 Target equipment property for laser printer measurement

Equipment	**Resolution**	**Writing speed**	**Color/Monochrome**
Printer 1	600 dpi*	8 ppm**	Monochrome
Printer 2	600 dpi	16 ppm	Color
Printer 3	600 dpi	4 ppm	Color

* dpi : dots per inch , ** ppm : page per minute

3.4.2. Reconstruction Result

Based on the experimental results, we can see that the resolution of the reconstructed image are affected by distance between antenna and printer and sampling rate. Figure 3.9 (a) and (b) shows the relationship between sampling rate and the restored image.

Incremented sampling rate by 5 MSamples/sec in the range from 5 MSamples/sec to 50 MSamples/sec, the resolution of the restored image enhanced. But an area of the restored image is reduced because AD board memory is limited. We found that there is no problem with the recognition even low Sampling rate of about 5 ~ 10 MSamples/sec.

Figure 3.9 (c) and (d) are restored at the 100 mm and 300 mm separation distance between antenna and target printer, respectively. When restored by detecting the magnetic field components, it is impossible to reconstruct the signal with a distance of about 300 mm less than about. These experimental results can be expected to utilize in order to establish the security level and measurement method. In future work, it can be basis of research to prevent from leaked signal for the various other electronic devices.

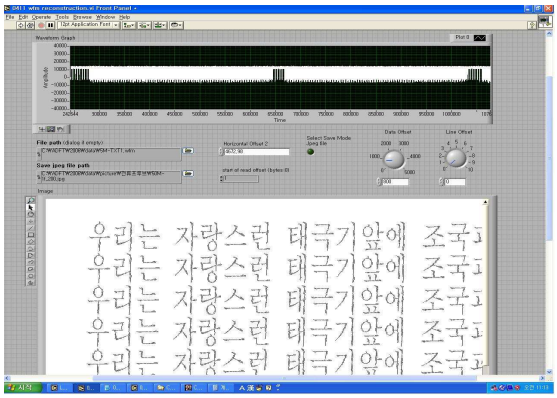
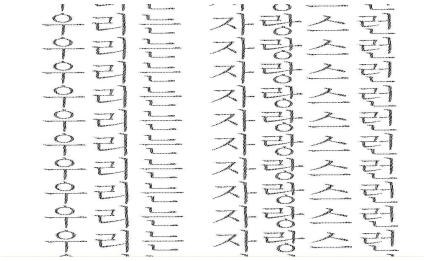
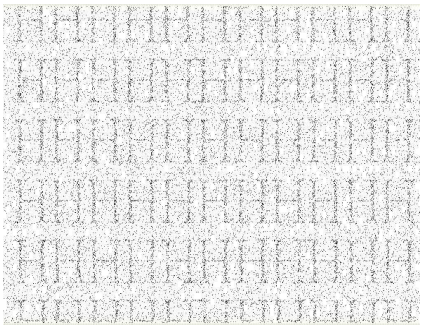


Figure 3.8. EMSEC system's GUI

(a) 5 MSa/sec



(b) 10 MSa/sec



(a) 100 mm

(b) 300 mm

Figure 3.9. EMSEC signal reconstruction from printer

3.5 Adaptive Deringing Filter for Reconstruction

MPEG-1/-2/-4 and H.26x are processed by block-based, where transformation is done by a Discrete Cosine Transforms (DCT) on blocks of 8×8 pixels [27]. Two of the main artifacts from the quantization of the DCT are blocking and ringing. The blocking artifact is seen as an unnatural discontinuity between pixel values of neighboring blocks. The ringing artifact is seen as high frequency irregularities around the image edges. In brief, the blocking artifacts are generated due to the blocks being processed independently and the ringing artifacts due to the coarse quantization of the high frequency components [28]. Deblocking filter is to reduce the blocking ringing and deringing filter is to remove the ringing, respectively.

We propose an adaptive deringing filter for image restoration of EMSEC-channel information focusing on deringing filter algorithm that is used in post-processing method in MPEG-4. When we reconstructed the EMSEC-channel informaiton without any other image processing, the horizontal signal is lost easily comparing the vertical signal. That is the reason why EMSEC-channel information can be detected easily at high rising or falling edge. The Figure 3.10 shows the EMSEC-channel information reconstruction result without image processing. We can see the many horizontal pixels in reconstructed image can’t recover from the original image. To compensate for the recovery of EMSEC-channel information property, we propose the adaptive deranging filter for image restoration of EMSEC-channel information.

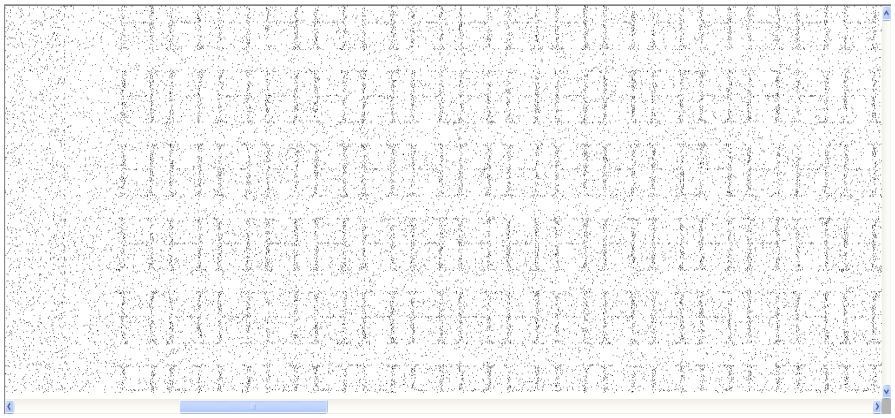


Figure 3.10 Reconstructed image without post-processing

We process the windowing with 16×16, 8×8 or 4×4 macro blocks to calculate the sum of differences (*SD*). The *SD* is calculated as follows :

$$SD(u,v) = \sum_{j=0}^{B-1} \sum_{i=0}^{B-1} X(i+u, j+v) \tag{3.2}$$

where, B is the size of macro blocks such as 16, 8 and 4, X is the reconstructed image not using the image processing, (i, j) is the spatial location within the reconstructed image and (u, v) is the candidate motion vector. If final *SD* value is over threshold obtained by experiment, that macro blocks is replaced by 255 and the macro block is replace by 0 otherwise as shown by Figure 3.11

When we used the window size 16 for calculating the SD, resolution of reconstructed image is not good but process time is fast by reducing the

complexity. The size of the macro block is reduced, the operation speed is slower but it is more accurate restoration image from EMSEC-channel information.

Figure 3.12 shows the reconstructed image using the adaptive deranging filter which filter size is 4×4. We can recognize more accurate than the reconstructed image without any other image processing.

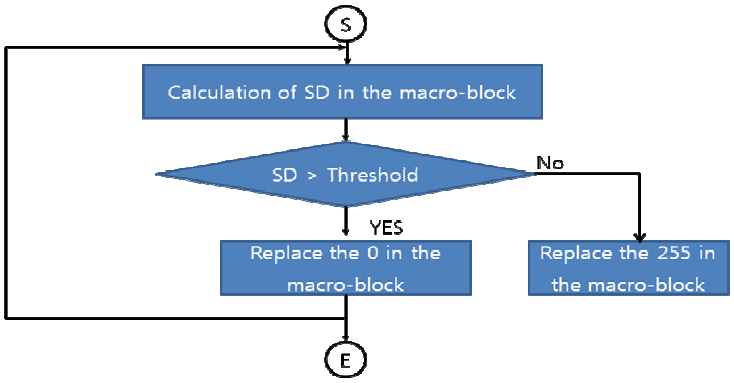


Figure 3.11 Algorithm flow of adaptive deringing filter for EMSEC-channel information

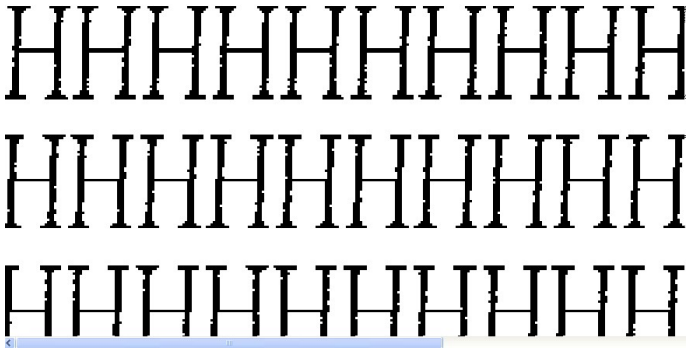


Figure 3.12 Reconstructed image using the adaptive deranging filter

Also, we used four different target characters which are Korean, Chinese, English characters and Arabic numeral. When we adjusted the adaptive deranging filter as the post- image processing, we can obtain that the minimum peak signal-to-noise ratio (*PSNR*) enhancement of reconstructed images using the adaptive deranging filter is 2 and maximum *PSNR* enhancement is 10 comparing the original reconstructed image in this experiments. *PSNR* is most commonly used to measure the quality of reconstruction image. The signal in this case is the original data, and the noise is the error introduced by reconstruction from the EMSEC-channel information. *PSNR* is most easily defined via the mean squared error (*MSE*). Given a $m \times n$ monochrome original image I and its noisy reconstruction image K, *MSE* is defined as :

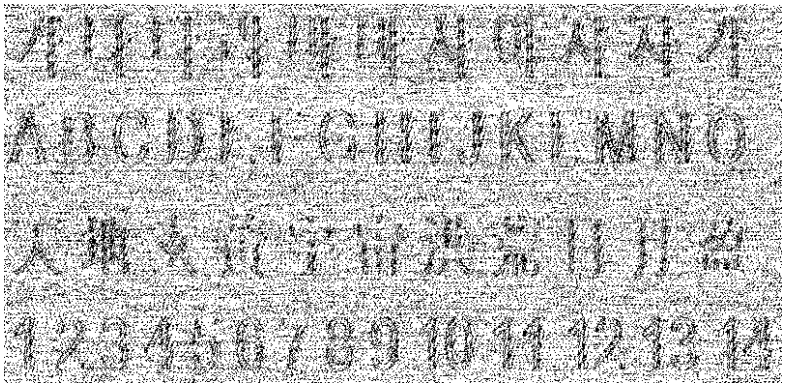
$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \tag{3.3}$$

The *PSNR* is defined as :

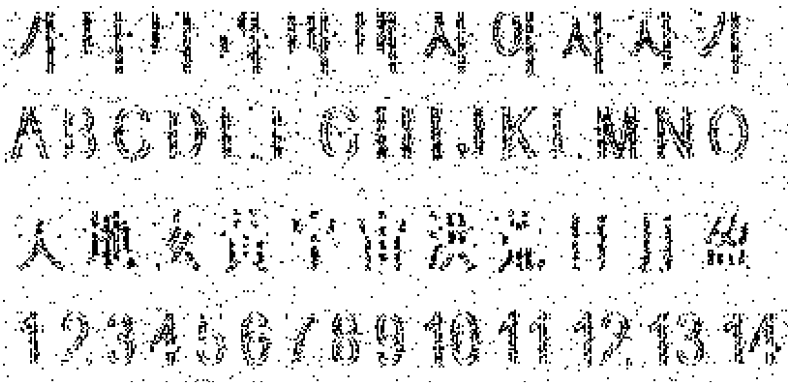
$$PSNR = 10 \log_{10} \left(\frac{MAX_I^{\ 2}}{MSE} \right) = 20 \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \tag{3.4}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bit per sample, this is 255. Figure 3.13 showes the *PSNR* comparison between the reconstructed image without post-

processing and the reconstructed image using the adpative dering filter whose filter size is 4. And chinsese character is more difficult to reconstruct the image comparing other characters due to the many storkes of the chinese charcter.



(a) Reconstructed image without image processing (*PSNR* : 58.55)



(b) Reconstructed image using the adaptive filter (*PSNR* : 68.34)

Figure 3.13 Comparison of *PSNR* Enhancement filter

3.6 Conclusion

In this study, configure your system and build the leakage electromagnetic signal reconstruction algorithm in order to improve the performance of the system by applying a averaging technique as a post-processing algorithm to reconstruction of the VDUs and printer.

By applying the post-processing algorithm, the reconstructed image with improved *SNR*, the noise is removed from the histogram equalization algorithm and a combination of multi-threshold histogram computation algorithms, the experimental results and the morphological algorithm can be obtained. It is easier to find the frequency of the electromagnetic wave leakage of the advantages of real-time processing and fast detection. In this experiment, for real-time processing with optimal speed and excellent *SNR* at 100 MSamples/sec, respectively, 50, 100, 150, 200 MSamples/sec, results of experiments done to restore the signal was possible to restore the video. In addition to, we propose the adaptive deringing filter to reconstruct the EMSEC-channel information from PC and printer. When we adjusted our proposal algorithm as post-image processing for EMSEC-system, we can obtain that the minimum *PSNR* enhancement of reconstructed images using the adaptive deranging filter is 2 and maximum *PSNR* enhancement is 10 comparing the original reconstructed image.

We can see that the resolution of the reconstructed image is affected by distance between antenna and printer and sampling rate. Increasing the

sampling rate, the resolution of the restored image enhanced. But an area of the restored image is reduced because AD board memory is limited. We found that there is no problem with the recognition even low Sampling rate of about 5 ~ 10 MSa/sec. Also, it is impossible to reconstruct the signal with a distance of about 300 mm less than about. These experimental results can be expected to utilize in order to establish the security level and measurement method. In future work, it can be basis of research to prevent from leaked signal for the various other electronic devices.

Chapter 4 Characteristic of Frequency Correlation EMSEC Channel in indoor environments

4.1 Introduction

Many researchers have investigated the EMSEC channel model and signal attenuation related to the channel environments. Previous model is too simple to reflect a realistically complex environment, and may give rise to some discrepancies between simulation results and real measurements. Although radio attenuation fluctuates according to the environment and distance between the transmitter (TX) and the receiver (RX), these previous works [1, 7, 24, 25] assumed that the radio attenuations are constant in order to obtain security limit and guide test method.

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable TRA. TRA is defined as the sum of all types of radio attenuations such as free space loss and additional radiation pathloss in the environment. The expected noise level and attenuation values are random variables that, in the absence of better data, have to be modelled as being normally distributed with some mean and variance determined from the statistical evaluation of a large number of measurements in various indoor environments [7]. We analyzed the pathloss characteristics of an indoor

EMSEC-channel under various environments on the basis of the measurements. For each environment, we obtained the TRA using its probability distribution to overcome the drawbacks of the previous works [1, 7, 24, 25].

4.2Channel Measurement

4.2.1 Measurement System

To analyze the characteristics of the compromising emanations, we performed frequency-domain measurements using vector network analyzer (VNA) and a pair of biconical and broadband LP antennas (Schwarzbeck VULB9161) from 100 MHz to 1000 MHz. Our measurement system yielded, S_{21} the forward transmission coefficient between the TX and RX antennas. For each frequency setup, a known sinusoidal signal was transmitted, and the magnitude and phase of the received signal were obtained. During the CTF measurements, the VNA was set to transmit 1601 continuous-wave tones uniformly distributed over the frequency bands in the 100 MHz to 1000 MHz range with a maximum frequency resolution at a frequency step of 0.56 MHz. This frequency resolution yielded a maximum excess delay of approximately 1.7 μs and a maximum distance range of approximately 533 m.

4.2.2 Measurement Scenarios and Environment

If the eavesdropper is located in an open area, the free-space loss will be

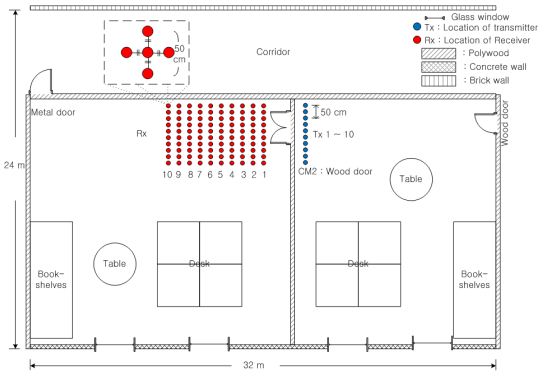
the dominant attenuation. Because residential and office areas are easily and secretly targeted by EMSEC-channel attacks, calculation of the TRA with regard to these environments is necessary. Measurement scenarios were set up by considering the property of the compromising emanations. Accordingly, the TX antenna was fixed in 10 different positions, whereas the RX antenna was moved along 50 positions at intervals of 0.5 m. The distance between the TX and the RX antennas ranged from 1 m to 10 m in each channel model (CM). Figure 4.1 shows the locations of the TX and RX antennas and the channel environment. Because the frequency spectrum of the compromising emanations from a target device is widely spread and its intensity is very weak, we set the transmit power to 1 mW.

To reflect the characteristics of the compromising emanation, we pay more attention to the non-line-of-site (NLOS) case than the line-of-site (LOS) case. The measurements were carried out in a modern office building having concrete walls, metal doors, wood doors, and glass windows.

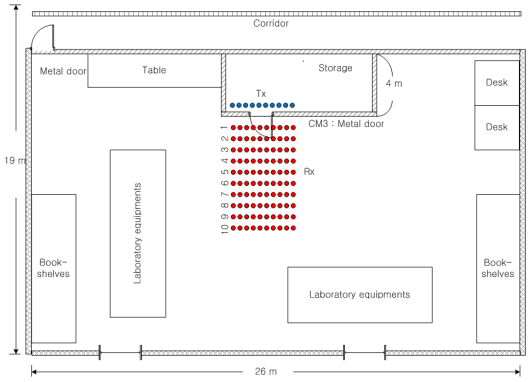
Table 4.1 Description of indoor EMSEC-channel models (CMs)

Channel Model	**Type**	**Material**	**LOS/NLOS**
CM1	Free space	Air	LOS
CM2	Twin door	Wood	NLOS
CM3	Single door	Metal	NLOS
CM4	Window	Glass/Metal	NLOS
CM5	Wall to wall	Concrete	NLOS

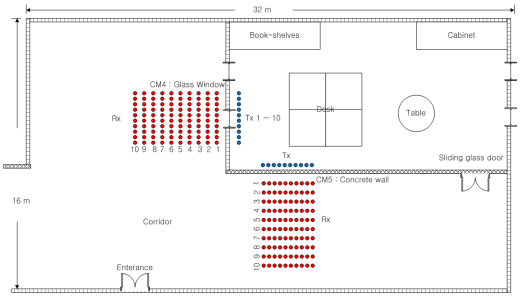
Table 4.1 summarises the scenarios in which five environments composed of various materials, LOS/NLOS cases, and structures were selected to study the propagation of compromising emanation under the influence of various materials, structure, sizes, and layouts.



(a)Environment 1



(b)Environment 2



(c)Environment 3 and 4

Figure 4.1 Channel environments

4.3 Analysis of Indoor EMSEC-Channel for Compromising Emanations

For the conventional channel-characteristic analysis, the root-mean-square delay spread and the mean-excess delay are essential parameters. However, the EMSEC-channel analysis is generally used to evaluate the electromagnetic field strength of the target equipment. Because the compromising emanation from target equipment in buildings are generally attenuated with the walls of the buildings and the distance between the target equipment and the receiver, the received electromagnetic field strength is a very important parameter in the determination of the emission security limits. Moreover, the delay parameters are compensated for by the horizontal and vertical synchronization parameters using the number of lines and frame frequency when the EMSEC-channel information is reconstructed [7]. Therefore, we focused on the attenuation of the received signals with respect to distance, frequency band, and channel environment instead of the delay parameters.

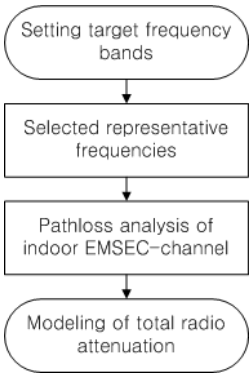


Figure 4.2 Outline description of our proposed approach

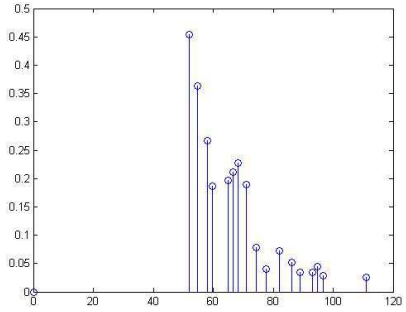
Figure 4.2 illustrates the procedure we used to propose the emission security limits. First, we set the target frequency bands from 100 MHz to 1000 MHz. Next, frequency correlation coefficients are calculated to find the representative frequencies at target frequency band for analysis pathloss characteristics on EMSEC-channel. We evaluated the TRA considering target frequency band and channel environment.

4.3.1 Frequency Correlation Property on Indoor EMSEC Channel

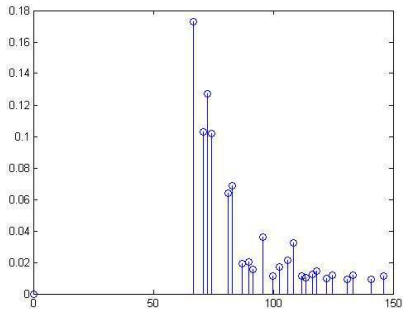
For considering the frequency correlation of the indoor EMSEC-channel, we used the EMSEC-channel measurements from 100 MHz to 1000 MHz frequency bands in Subsection 4.2. We can obtain the channel impulse response (CIR) of EMSEC-channel based on these measurements. Figure 4.3 showes examples of channel impulse responses at CM4 and CM5. Usually, for the LOS data, the first arrival path depend on distance. While for the

NLOS data, first arrival path is depend on distance and CMs, has very differentiation each CMs.

From the convolution between our measured leaked signal and the continus wave (CW) from VNA in the frequency domain, we obtained the envelope of the measured leaked signal which are applied the signal attenuation due to the channel environment. Because, the attenuation of the trasmitted signal from the VNA is reflected in the attenuation of EMSEC-channel information related to the channel environment. Figure 4.4 shows the example of envelope of measured EMSEC-channel information at CM2 and distance 7 meter.



(a)CM4 at distance d = 5 meter



(b)CM5 at distance d = 10 meter

Figure 4.3 Examples of channel impulse responses at CM4 and CM5

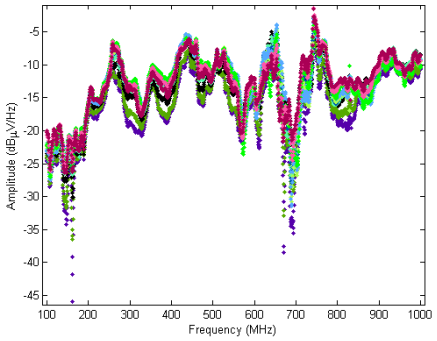


Figure 4.4 Example of envelope of measured leaked signal at CM2

For the characterization of the frequency correlation properties from the 100 MHz to 1000 MHz frequency bands, the cross-correlation coefficient was used to represent the correlation level of the received signal amplitudes between frequency tones. This process was presented in [29].

$$\rho_a(\Delta f) = \frac{C_a(f, f+\Delta f)}{\sqrt{C_a(f, f)}\sqrt{C_a(f+\Delta f, f+\Delta f)}} \tag{4.1}$$

where $C_a(f_1,f_2)=E[\{a(f_1)-m_a(f_1)\}\{a(f_2)-m_a(f_2)\}]$, $a(f_1)$ is the amplitude of the channel gain at frequency tone f_1, $m_a(f_1)$ is the mean of $a(f_1)$ and Δf is a frequency interval. The frquency interval increases from 1 MHz to interval bandwidth (BW) 100 MHz by multiples of the frequency step 0.5625 MHz in Section 2. We selected the interval BW is 100 MHz, because a multiple of BW = 50 MHz is needed for practical compromising for readable video

signals [7]. $\rho_a(\Delta f)$ is the average cross-correlation coefficient at the Δf as shown Figure 4.5. Because the eavesdropper is located in cluttered environments except free space practically, we did not consider the CM1. We simulated the frequency correlation coefficients as increasing the frequency interval to find the all frequency correlations at interval BW.

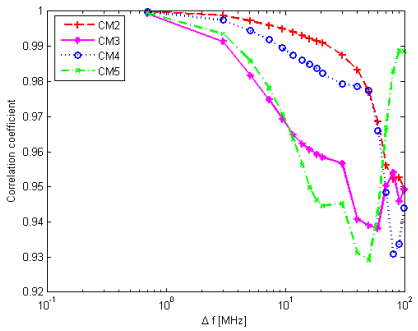
The cross-correlation coefficients become smaller as the frequency interval wider generally. But it is shown that the cross-correlation among the frequency tones is high from 0.6 to 0.9. Fig. 4.5 shows an examples of the correlation coefficients at a distance of 3 m on the 400–500 MHz and a distance of 9 m on the 800–900 MHz using (2) on the channel environments.

The calculated cross-correlation coefficients in this study are listed in Table 4.2. On the basis of these results, we represented the nine representative frequencies (f_r) as 200 MHz, 300 MHz, 400 MHz, 500 MHz, 600 MHz, 700 MHz, 800 MHz and 900 MHz for our target frequency bands to analyze the pathloss characteristics on the indoor EMSEC-channel.

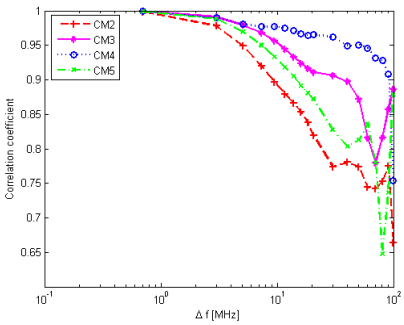
Table 4.2 Frequency correlaiton coefficients of indoor EMSEC-channel models

Frequency	CM2		CM3		CM4		CM5	
(MHz)	Min	Max	Min	Max	Min	Max	Min	Max
(100,200)	0.60	0.97	0.88	0.99	0.72	0.98	0.85	0.99
(200,300)	0.65	0.99	0.78	0.98	0.77	0.99	0.77	0.98
(300,400)	0.71	0.99	0.83	0.99	0.82	0.99	0.87	0.99
(400,500)	0.72	0.99	0.81	0.99	0.73	0.98	0.71	0.99

(500,600)	0.65	0.97	0.88	0.99	0.72	0.98	0.85	0.99
(600,700)	0.68	0.99	0.78	0.98	0.77	0.99	0.77	0.98
(700,800)	0.75	0.99	0.65	0.99	0.78	0.99	0.65	0.99
(800,900)	0.64	0.99	0.73	0.99	0.59	0.98	0.74	0.99
(900,1000)	0.64	0.99	0.81	0.99	0.78	0.98	0.71	0.98



(a)400–500 MHz (d = 3 meter)



(b)800–900 MHz (d = 9 meter)

Figure 4.5 Examples of frequency correlation coefficients

4.3.2 Pathloss Characteristics on the Indoor EMSEC-Channel

To develop an efficient EMSEC system, pathloss properties must be evaluated with respect to the possible noise level and TRA. Pathloss modeling can be simplified by assuming that the frequency dependence and the distance dependence can be treated independently of each other [30]. We can find the pathloss equation of the frequency-correlation indoor EMSEC-channel with the frequency and the distance *d* between TX and RX using the logarithmic equation [31]

$$PL(d, f) = 20 \cdot \log_{10} f + 10 \cdot \log_{10} k - 10 \cdot n \cdot \log_{10} d, \quad (4.2)$$

Where *n* is the pathloss exponent and *k* is the received power amplitude. We find *n* and *k* using least-squares (LS) curve fitting based on variation in the measured received power with distance for different CMs and frequency bands.

We summarized the detailed parameters of pathloss equation in Table 4.3. The root-mean-square error (RMSE) between measured parameters and estimated parameters is obtained using LS-curve fitting. Figure 4.6 shows the measured received power and LS-fitted curves represented by black solid lines for each CM.

CM3 and CM4 had a metal door and metal window frame between the TX

and RX, respectively, in which the EMSEC-channel information was effectively shielded. We conjecture that CM3 and CM4 had relatively higher power attenuation than CM2 and CM5, which were composed of wood and concrete, respectively. In other words, owing to the lower power attenuation of CM2 and CM5, they were more vulnerable to unintentional compromising emanation compared to CM3 and CM4. If the single security limit is typically applied for various indoor environments and frequency bands, signal leakage is a concern. The emission security limits are thus necessary for considering the influcence of channel environment in order to protect leakage important signal from eavesdropping.

Table 4.3 Estimation parameters of indoor EMSEC-channel models

Representative frequency, f_r	CMs	k	n	RMSE
f_r = 100 MHz (100–200 MHz)	CM2	0.012	2.30	0.0004
	CM3	0.016	2.84	0.0003
	CM4	0.002	2.29	0.0001
	CM5	0.015	1.17	0.0092
f_r = 200 MHz (200–300 MHz)	CM2	0.066	2.29	0.0016
	CM3	0.031	2.83	0.0003
	CM4	0.002	2.29	0.0001
	CM5	0.027	1.06	0.0103
f_r = 300 MHz (300–400 MHz)	CM2	0.089	2.33	0.0019
	CM3	0.018	2.82	0.0004

	CM4	0.002	2.32	0.0003
	CM5	0.054	1.36	0.0075
f_r = 400 MHz (400–500 MHz)	CM2	0.089	2.37	0.0009
	CM3	0.014	2.92	0.0003
	CM4	0.002	2.40	0.0001
	CM5	0.029	1.20	0.0035
f_r = 500 MHz (500–600 MHz)	CM2	0.108	2.41	0.0019
	CM3	0.054	2.93	0.0001
	CM4	0.007	2.33	0.0001
	CM5	0.032	1.14	0.0066
f_r = 600 MHz (600–700 MHz)	CM2	0.080	2.40	0.0039
	CM3	0.005	2.90	0.0001
	CM4	0.008	2.33	0.0001
	CM5	0.024	1.20	0.0042
f_r = 700 MHz (700–800 MHz)	CM2	0.109	2.38	0.0011
	CM3	0.025	2.88	0.0001
	CM4	0.009	2.32	0.0001
	CM5	0.021	1.32	0.0042
f_r = 800 MHz (800–900 MHz)	CM2	0.153	2.34	0.0041
	CM3	0.024	2.92	0.0001
	CM4	0.007	2.41	0.0001
	CM5	0.019	1.26	0.0043
f_r = 900 MHz	CM2	0.050	2.32	0.0009

(900–1000 MHz)	CM3	0.002	2.94	0.0001
	CM4	0.001	2.50	0.0001
	CM5	0.016	1.14	0.0062

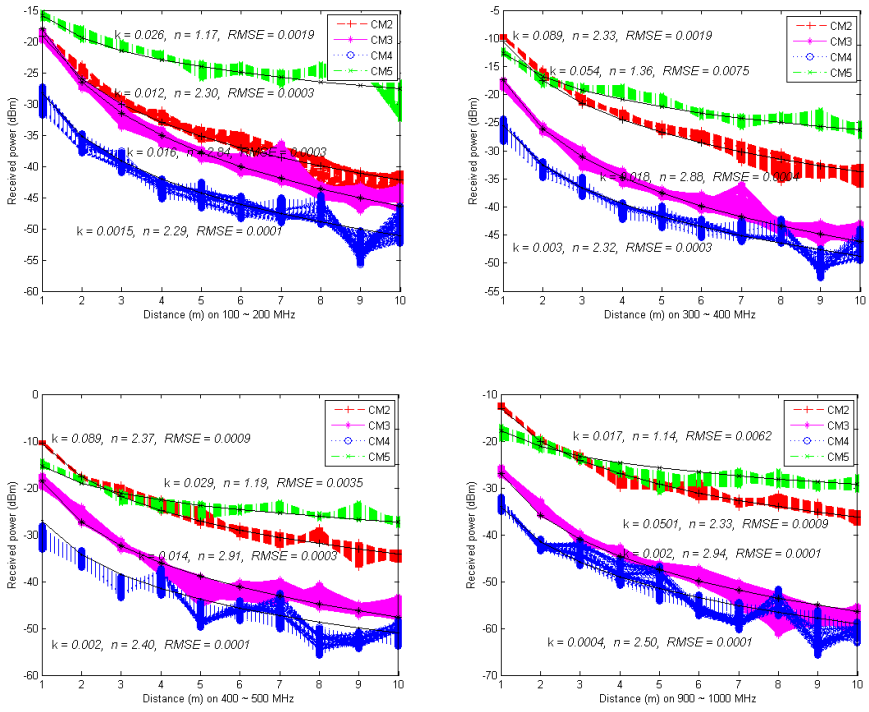


Figure 4.6 Example of LS-curve fitting on received power

Some researchers adopted the two-ray Rayleigh fading model to represent the digital channel for compromising emanation, in which the pathloss exponent n was a constant value of 2 [7, 24]. Other researchers took the value of *n* as 2 at 900 MHz and 2.2 at frequencies from 1.2 GHz to 4 GHz [25].

However, we calculated the pathloss exponent using LS-curve fitting with

the measured value of 500 points each CMs and frequency bands respectively. And then, we found that the pathloss exponent value ranged from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with propagation environments, such as an empty office, a concrete wall, a wood or metal door, or a glass window.

4.4 Conclusion

To propose the emission security limits, we set the target frequency bands from 100 MHz to 1000 MHz, firstly. Next, frequency correlation coefficients are calculated to find the representative frequencies at target frequency band for analysis pathloss characteristics on EMSEC-channel. The cross-correlation among the frequency tones is a little bit high from 0.6 to 0.9. We represented the nine representative frequencies as 200 MHz, 300 MHz, 400 MHz, 500 MHz, 600 MHz, 700 MHz, 800 MHz and 900 MHz on the basis of these results.

We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable TRA. TRA is defined as the sum of all types of radio attenuations such as free space loss and additional radiation pathloss in the environment.

We calculated the pathloss exponent using LS-curve fitting with the measured value of 500 points each CMs and frequency bands respectively. And then, we found that the pathloss exponent value ranged from 1.06 to 2.94 depending on frequency band and the CMs, which in turn differed with

propagation environments, such as an empty office, a concrete wall, a wood or metal door, or a glass window. CM3 and CM4 had a metal door and metal window frame between the TX and RX, respectively, in which the EMSEC-channel information was effectively shielded. We conjecture that CM3 and CM4 had relatively higher power attenuation than CM2 and CM5, which were composed of wood and concrete, respectively.

Chapter 5 Emission Security Limits for Compromising Emanations

5.1 Introduction

In this chapter, we present a periodic and aperiodic emission security limits using the measurement and analysis of electromagnetic emission security channel in chapter 4. Based on investigation about currently known security limits, suitable and actual security limits are proposed. These emission security limits can be used as the basis of the limited the leakage electromagnetic radiation of information appliance devices for authentication.

5.2 Parameters for Security Limits

In this section, we propose security limits on compromising emanation based on the measurement and analysis of the frequency correlation indoor EMSEC-channels, as described in Chapter 4.

Figure 5.1 shows the EMSEC system configuration at each stage for determination of emission security limits. EMSEC system' *SNR* is proportional to system gains such as antenna gain and signal processing gain, and inversely proportional to total radio attenuation in the radiation path and environmental noise strength [7, 25]. The *SNR* is defined as

$$SNR = \frac{E_{max} \cdot G_a \cdot G_p}{a_{total} \cdot E_{n,B} \cdot f_n}, \qquad (dB) \quad (5.1)$$

where, E_{max}= maximum field strength that the test standard permits

B = the impulse bandwidth used in the test

a_{total}= is defined by total radio attenuation(TRA) such as free space pathloss and additional radiation pathloss by the building walls

G_a = the gain of the best directional antenna that is feasible for use by the eavesdropper

G_p = the processing gain that can be achieved with techniques such as periodic averaging

$E_{n,B}$ = the field strength of natural and man-made radio noise at the location of the eavesdropping antenna within a bandwidth B

f_n = the noise factor of the eavesdropper's receiver

(5.1) can be expressed by the logarithm (dB) as following (5.2)

$$SNR = E_{max} + G_a + G_p - a_{total} - E_{n,B} - f_n, \qquad (dB) \quad (5.2)$$

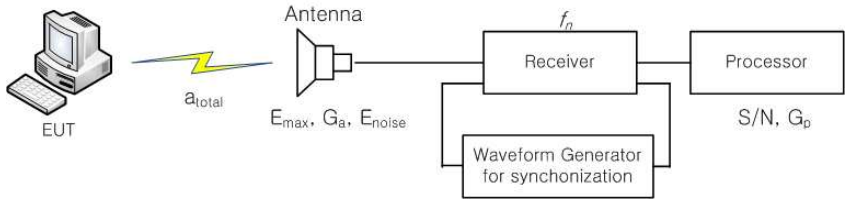


Figure 5.1 EMSEC's system configuration

This method consider that the minimal background noise that the eavesdropper faces even under good receiving conditions, the gain from antenna types that can be used covertly, and the gain from the use of suitable detection and signal processing methods for the signal of interest the closest distance between antenna and target device for which protection is needed. They achieved the signal-to-noise ratio that a radio-frequency eavesdropper under these conditions using (5.2).

Finally, we can obtain the emission limits level to derive each parameter to obtain the best signal-to-noise ratio from (5.2). Subsection 5.2.1~5.2.6 are presented the details of each parameter.

5.2.1. Total radio attenuation

The value a_{total} is defined by TRAs such as free space pathloss and additional radiation pathloss by the building walls. We assumed the maximum distance to be 10 m since the EMSEC system would not be closer than 10 m in indoor environments. Therefore, the TRA, a_{total} is defined at a representative frequency, f_r, receiver power amplitude k, and pathloss exponent n which are depends on channel environments as

$$a_{total} = PL(10, f_r) = 20 \cdot \log_{10} f_r + 10 \cdot \log_{10} k - 10 \cdot n. \quad (dB) \tag{5.3}$$

A comparison of the available literature on outdoor radio noise shows that rather limited data is available on indoor radio signal attenuations caused by building materials [7]. Previous work [1, 7, 24, 25] assumed that radio attenuations would have constant values. They mentioned that indoor ratio signal attenuation by building materials clear data are far less. They adjusted that the survey publications [32, 33] provide data for the frequency range of 900 MHz to 100 GHz, which is of particular interest to designers of mobile personal communicaiton systems and wireless networking applications [7]. However, this data shows only a few trends and mostly documents a significant variability between buildings. The survey [33] lists a number of alternative models that have been used to describe attenuation in buildings. Example values from published measurements mentioned in [33] include 1.4 dB for a cloth-covered office, 3 dB for wood and brick sliding, 7 dB for a 200 mm concrete block wall, 13 dB for another concrete wall, and 12 and 16 dB for floors in different buildings, where at 900 MHz, in addition to free sapce loss, attenuations of 10~25 dB have been reported. For the VHF frequency range, they found a study [34], which looked at 35 and 150 MHz signals from a far away station and found that signal levels inside buildings are in the order of 20~25 dB lower than outside in the street and that the building attenuation was in the range 5~45 dB in about 90 % of all measurements made with a sightly lower attenuation for 150 MHz. They want to ensure protection even for rooms whose attenuation by building materials is located in the lowest decile of the available statisics and therefore use total radio attenuation is 15 dB at 10 meter.

However, the radio attenuations have to be modelled as being normally distributed with a mean and variance determined through statistical evaluation of a large number of measurements in various environments. Accordingly, we measure and analyze the frequency correlation indoor EMSEC-channel under indoor environments. Based on these results, we found that the TRA in dB can be modelled as a random process that follows a Rician distribution at each channel. The cumulative distribution function (CDF) of the total radio attenuation with Rician fitting at CM2 at 400–500 MHz and CM4 at 900–1000 MHz is shown in Figure 5.2. The empirical CDF shows good agreement with the CDF of the Rician distribution.

Let *s* denote the direct-waves peak amplitude and σ denote the standard deviation of the overall total radio attenuation a_{total}, then the Rician *k*-factor is given as

$$k = \frac{s^2}{2\sigma^2}. \tag{5.4}$$

The Rician CDF is calculated as follows

$$C_{Rice}(a_{total}) = exp[-(k + \frac{a_{total}^{\ 2}}{2\sigma^2})]\sum_{m=0}^{\infty}(\frac{\sigma\sqrt{2k}}{a_{total}})^m I_m(\frac{a_{total}\sqrt{2k}}{\sigma}) \tag{5.5}$$

and $I_m()$ is a modified m-th order Bessel function of the first kind [31]. And Table 5.1 summarises the *s* and σ values of measured channels, the RMSE

of the measured results with Rician fitting result, and the 90% probability of TRA for each CM and frequency band.

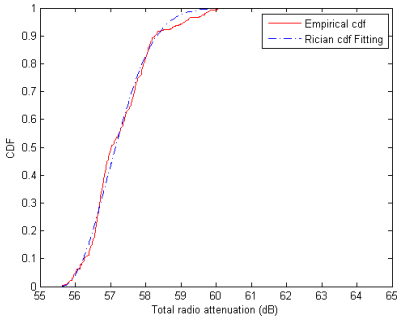
Table 5.1 Rician CDF parameters of indoor EMSEC-channel model

Frequency	CMs	s	σ	RMSE	TRA (dB)
100	CM2	0.77	1.18	0.06	41
–	CM3	0.84	1.25	0.02	43
200	CM4	2	2.17	0.05	48
MHz	CM5	2.6	2.44	0.04	29
200	CM2	0.03	1.05	0.06	33
–	CM3	0.51	1.09	0.17	42
300	CM4	1.64	0.90	0.03	48
MHz	CM5	0.66	1.30	0.04	24
300	CM2	0.40	1	0.06	32
–	CM3	0.70	1.20	0.03	42
400	CM4	1.86	2.07	0.05	47
MHz	CM5	1	0.87	0.03	24
400	CM2	0.23	0.71	0.02	31
–	CM3	2.73	1.59	0.06	45
500	CM4	1.46	0.86	0.05	50
MHz	CM5	0.39	0.67	0.04	25
500	CM2	0.94	1.53	0.049	30
–	CM3	2.36	1.21	0.024	51

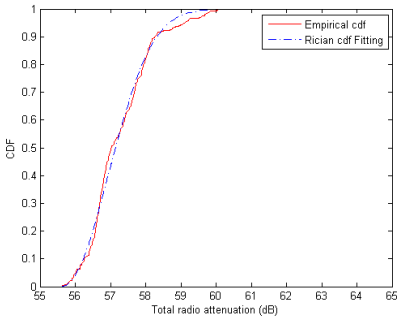
600 MHz	CM4	0.78	1.30	0.018	51
	CM5	0.59	0.70	0.021	24
600 – 700 MHz	CM2	3.47	2.79	0.042	36
	CM3	1.69	1.09	0.030	49
	CM4	3.01	1.89	0.063	51
	CM5	1.20	0.56	0.036	26
700 – 800 MHz	CM2	0.18	0.70	0.019	31
	CM3	0.99	1.89	0.032	51
	CM4	3.22	1.08	0.031	51
	CM5	0.66	1.08	0.032	29
800 – 900 MHz	CM2	1.92	1.03	0.063	29
	CM3	3.90	1.02	0.020	57
	CM4	2.05	2.02	0.016	52
	CM5	1.13	1.19	0.024	28
900 – 1000 MHz	CM2	1.1	1.01	0.03	34
	CM3	1	1.6	0.06	57
	CM4	0.99	1.05	0.02	57
	CM5	1.77	0.98	0.004	27

We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment : 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4,

and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.



(a)CM2 at 400–500 MHz (s = 0.23, σ = 0.71)



(b)CM4 at 900–1000 MHz (s = 0.99, σ = 1.05)

Figure 5.2 Rician CDF fitting of total radio attenuation

5.2.2. Radio noise

A standard survey-data reference for the noise levels to be expected in various environments throughout the radio spectrum exists in the form of

ITU-R Recommendation P.372 [35], which summarizes the results from numerous noise intensity measurements and categorizes their origin.

Environmental noise was the radio noise around the wireless information devices and eavesdroppers, and derived expressions presented in the ITU-R Recommendation P.372 [35]. Radio noise to the environment based on the recommendation of the noise can be expressed as follows:

$$E_{n,b}(dB\mu V) = F_a(dB) + 20\log f_{MHz} + 10\log B_{MHz} - 36.8, \qquad (dB) \quad (5.6)$$

where, F_a is external noise figure, f_{MHz} is frequency and B_{MHz} is receiver's BW. F_a is presented equation (5.7). External noise is shown by the following equation (5.7) on the recommendations

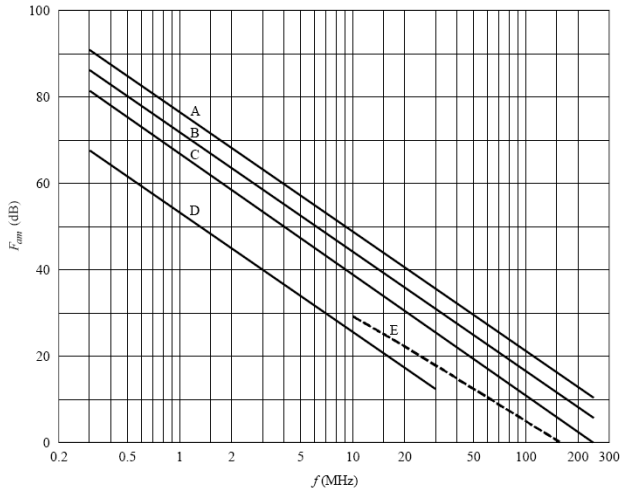
$$F_a = c - d \cdot \log(f) \qquad (dB) \quad (5.7)$$

where, c and d are constant values which are different by region and the value is categorized by commercial area, residential area, rural areas, not rural and cosmic noise in the from 0.3 MHz to 250MHz frequency band in Table 5.2 and Figure 5.3.

Table 5.2 Parameters c and d

Environment	***c***	***d***
Commertial area	76.8	27.7

Residential area	72.5	27.7
Rural areas	67.2	27.7
Not rural	53.6	28.6
Cosmic noise	52.0	23.0



A:commertial area, B: residential area, C: rural areas, D: not rural, E: cosmic noise

Figure 5.3 External noise figure corresponding to environment

5.2.3. Antenna gain

In the commercial market, the highest antenna gain in the 100–1000 MHz frequency band is commonly 17 *dBi* [36]; hence, we adopt an antenna gain, G_a, of 17 *dBi* for our target frequency bands to obtain rigorous emission security limits.

5.2.4. Signal processing gain

The advantage of signal processing, using various DSP to processes the digital signals that after digitized via AD converter signal of electromagnetic radiation that is received via the receiver shows the advantage to get through a method for improving the *SNR* of the signal.

The advantage of the signal processing, the signal of electromagnetic radiation that can be obtained through filtering, Correlation, and character recognition algorithms and averaging, generated from the information equipment such as a computer monitor, the same signal with a constant cycle to illustrate the form of periodic signals to be repeated. Averaging techniques is the most efficient method how to receive repeated signals of multiple periods continuously.

Received waveforms are mixed up noise component and signal component. Let us consider the case to match the phase of the signal to match with a plurality of cycles these received waveforms. Because the signal component is applied to the same phase, the voltage of the signal will be doubled. However, because it has a random phase to each other when it is assumed to be random noise, synthesis, noise component shows the effect of power is double the two signals having different phases. As a result, the signal voltage increased, power is increased, in the case of noise.

Thus, the advantages of the signal processing by these methods can be generalized as follows. We adopted an averaging technique as a post

processing method for image in order to improve the *SNR* of the reconstructed EMSEC-channel information. This method is a practical, highly effective, and widely used technique for increasing the *SNR* of a periodic signal, such as a signal generated by the image-refresh circuitry in VDUs [2, 7]. We used the common video resolution mode of 1280×1024 at 75 Hz, which is composed of 1,799,408 pixels [26]. G_p is defined as (5.8) [7]

$$G_p = 10 \cdot \log_{10} M, \qquad (dB) \tag{5.8}$$

where M indicates the number of the periodic signal applied to the correct phase. Since M is related to the available acquisition memory in the receiver as (5.9), we used high performance acquisition storage, which has a maximum memory of 512 MB and 12 bit resoultion, 2 byte is used for store. The maximum M is 213 and G_p is calculated about 23 dB using Equation (5.8).

$$M = \frac{512 \times 12bit \times 10^6}{1{,}799{,}408 \times 16bit} = 213 \tag{5.9}$$

As a result, the number of signal period which can be applied to the exact phase, is a primary parameter, the advantages of signal processing can be obtained by averaging technique method, when it was not applied to the correct phase in the course of the treatment is, it is possible to take advantage of the signal processing lower than this.

5.2.5. Minimum *SNR* for reconstruction

The final output of the reconstructed image after applying signal processing methods has been changed to a digital signal after the signal received by the antenna and receiver will have a certain amount of *SNR*, but if they will be recognized as the information.

Figure 5.4 shows the characteristics of the restoration image that is presented in the paper [7]. Vertical axis shows the *SNR* value, shown in 5 dB increments. In this example, must have a *SNR* of 10 dB or more, at least it is believed to be possible to recognize a correct character, and when you want to use a larger font and using such detection algorithm and character recognition than this is judged possible to character recognition in the signal lower *SNR*.

The paper of Markus, *SNR* of the restored image has been suggested that can be recognized as an information unless you 0 dB or more at least when you take into account the effect of improving a variety of multiple.

5.2.6 Receiver noise factor

A noise figure of receiver is the ratio between *SNR* at output and *SNR* at input on receiver. It is an index showing the effect of the noise by the receiver and a receiver having the lower noise figure is better.

We assume the attacker uses a receiver with a noise figure of f_n = 10 dB given for the Dynamic Sciences R-1250 and an impulse bandwidth of B = 50 MHz for same condition Kuhn's receiver noise figure [7].

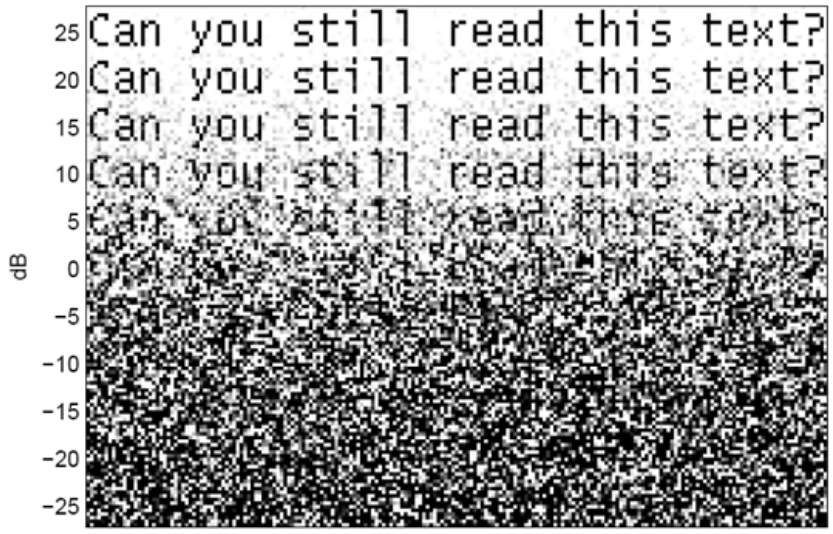


Figure 5.4 Video signal with varying *SNR*

5.2.7. Calculation of Emission Security Limit

Video display images are easily recovered by the periodic property of their EMSEC-channel information, whereas printer and fax images, which exhibit aperiodicity in their EMSEC-channel information, are reproduced by a single operation. From this point of view, the periodic emission security limit is considered to be the processing gain, G_p, when using the averaging image processing technique. However, it is difficult to obtain the processing gain for an aperiodic emission security limit. Hence, we apply a processing gain in order to divide periodic and aperiodic emission security limits. Emission security limits can be classified into confidentiality classes A and B. Class B

is for confidential equipment handling sensitive data; therefore, it requires stronger protection than class A [1].

Table 5.1 lists the TRA (a_{total}) from 100 MHz to 1000 MHz for each CM. a_{total} has a range from 24 dB at CM5 to 57 dB at CM3 and CM4. We calculated the emission security limits for class B using (5). E_{max} is 21 dBμV/m for class B at 200-300 MHz when the *SNR* is 0 dB, the receiver' s BW is 50 MHz, and the distance is 10 m. From (5.2), it is found that the emission security limits for class A are 45 dBμV/m on the same frequency band.

5.3 Proposed Emission Security Limits

In this subsection 5.2.7, E_{max} is 21 dBμV/m for class B at 200–300 MHz when the *SNR* is 0 dB, the receiver' s BW is 50 MHz, and the distance is 10 m. From (5.2), it is found that the emission security limits for class A are 45 dBμV/m on same frequency band. Because the general spectrum analyzers allow a maximum impulse BW of either 1 MHz or 5 MHz, measurements with a BW of 50 MHz are not possible using the commonly used spectrum analyzers. Therefore, the corresponding limit is 20 dB lower at a BW of 5 MHz [2]. We can therefore obtain the emission security limit for BW 5 MHz as 1 dBμV/m for class B and 25 dBμV/m for class A at 200–300 MHz .

Table 5.3 presents our calculated emission security limits using the frequency correlation indoor EMSEC-channel analysis at distance *d* of 10 m, a BW of 50 MHz and 5 MHz, respectively. We can ignore the ± 1 dB

interval of the calculated security limits to fall into several groups. For stricter emission security limits against eavesdropping, we selected a more rigid emission security limit by grouping.

Table 5.3 Calculated periodic emission security limits (unit : *dBμV/m*)

Frequency (MHz)	BW = 50 MHz		BW = 5 MHz	
	Class A	Class B	Class A	Class B
100-200	45	24	24	4
200–300	45	21	25	1
300–400	44	21	24	1
400–500	47	22	27	2
500–600	49	21	29	1
600–700	48	23	28	3
700–800	48	26	28	6
800–900	49	25	29	5
900–1000	55	25	35	5

Table 5.4 Proposed emission security limits (unit : *dBμV/m*)

Frequency (MHz)	Aperiodic EMSEC-channel information		Periodic EMSEC-channel information	
	Class A	Class B	Class A	Class B
100-200	47	27	24	4
200–400	47	24	24	1
400–600	51	24	28	1
600–700	51	26	28	3
700–900	51	28	28	5
900–1000	58	28	35	5

The periodic emission security limits for BW 5 MHz are 1, 1, 2, and 1 *dBμV/m* for class B in the 200–600 MHz, these can be grouped as 1 *dBμV/m*. In addition, the periodic emission security limits for BW 5 MHz are 27, 29, 28, 28, and 29 *dBμV/m* for class A in the 400–900 MHz range, these can be grouped as 28 *dBμV/m*. Similarly, the periodic emission security class limits for BW 5 MHz can be grouped 24 *dBμV/m* for class A in the 100~400 MHz. Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

Finally, we present our proposed periodic and aperiodic emission security limits in the target frequency bands using the frequency correlation indoor EMSEC-channel analysis at a BW of 5 MHz and distance *d* of 10 m in Table 5.4. In general, with existing EMC standards [4, 5], class B has a strict value 10 dB higher than class A without consideration of various channel environments. Class A and class B for the proposed emission security limits are influenced by the TRA, which is affected by the frequency and channel environment. Therefore, the difference in the emission security limits between class A and class B implies the difference between the maximum and minimum values of the TRA, which are affected by the channel environment and frequency band.

5.4 Comparison with Public Standards and Other Security Limits

5.4.1 CISPR22 and MIL-STD-461E

For comparison, we selected the CISPR22 class B standard [4], which is used globally as a radiated emission standard for IT equipment in commercial EMC standards, and the United States military EMC standard MIL-STD-461E/R102 [5] for mobile army and navy equipment radiation. Existing security limits [7, 25] and the civilian [4] and military [5] EMC standards are tunned to the same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits to prove their reliability and practicality. We have to take into account the different BW and antenna distances. To increase the impulse BW from 120 kHz for other EMC standards to 5 MHz for the proposed emission security limits, we have to raise the permitted field strength by 32 dB, in order to keep the equivalent spectral density constant. The limits have to be raised further by 20 dB to convert the measurement distance from 1 to 10 m [7].

The emission limits under the CISPR22 class B and class A standards are 62 *dBμV/m* and 72 *dBμV/m*, respectively, from 30 MHz to 230 MHz. For the CISPR22 class B and class A standards, the limits are 69 *dBμV/m* and 79 *dBμV/m* from 230 MHz to 1000 MHz, respectively. The MIL-STD-461E class B standard is 24 *dBμV/m* at 100 MHz, which linearly increases up to 32 *dBμV/m* at 1000 MHz. The MIL-STD-461E class A standard is 44 *dBμV/m* at

100 MHz, which linearly increases up to 52 *dBμV/m* at 1000 MHz at a distance of 10 m and a BW of 5 MHz.

Other measurement parameters of the compared limits such as the antenna gain, signal processing gain, both natural and man-made radio noise, and noise factor are used to determine the *SNR* for EMSEC system Eq. (4). Because the civil and military EMC standards [4, 5] consider the unintentional generation, propagation and reception of electromagnetic energy with reference to the unwanted effects to other IT devices, general EMC standards did not applied for these the measurement parameters because it does not take into account the *SNR*. In addition, other security limits [1, 7, 25] are applied by ITU-R P.372 [31] for natural and man-made noise factor as like the proposed security limits to consider the *SNR* and these security limits same as noise figure as our security limits.

Previous works and published EMC standards used the same security limit for all kinds of equipment in various environments. However, we proposed the emission security limits based on measurement and analysis of the EMSEC-channel in various real indoor environments. The proposed emission security limits are considered as the level of confidentiality and TRA based on the channel environment and frequency bands.

5.4.2 Security limits for Markus G. Kuhn

Most foreign countries classified for the leakage electromagnetic shielding

standards and criteria without disclosing. However, to present the related research in the field of academic methods and standards are often derived the leakage electromagnetic shielding standards. University of Cambridge, UK, Markus G. Kuhn presented these method his doctoral thesis and ITU-T K.84 is generated the test methods and guide against information leaks through unintentional EM emissions. In this section, these existing two security limits are explained

Markus method is presented by deriving the eavesdropper's the signal-to-noise ratio (*SNR*) that. Therefore, that method is to calculate the *SNR* of the obtained signal gain and the noise component from the target devices passing through antenna, receiver and signal processing device

To define stricter emission security limits than the EMC standards, for the worst case scenario we assumed that the *SNR* is less than 0 dB because of unreadable text for reconstruction [7], the receiver' s BW is 50 MHz, and the distance is 10 m. To protect the equipment against an EMSEC-channel attack, we calculated the maximum field strength, E_{max} which is the emission security limit, to satisfy $SNR \leq 0$ dB using the logarithmic equation (4).

In (5.2), E_{noise} and f_n are set to 27 dBμV/m and 10 dB, respectively, as given in [2]. In the commercial market, the highest antenna gain in the 100 MHz to 1000 MHz frequency bands is commonly 17 *dBi* [33]; hence, we adopt an antenna gain G_a of 17 *dBi* for our target frequency bands to obtain rigorous emission security limits. When in setting the standards for the Worst Case was mentioned represent the effect of 45 dB in 5 dB attenuation due to buildings in front of the building by at least 5 dB attenuation can be applied.

(5.2) assigned to each of these parameters was presented in front of the signal to restore requires at least 0 dB *SNR* final, you can get the upper level of electromagnetic radiation in Worst Case conditions for the protection of information leakage.

As a result, if the conditions set out above, the leakage electromagnetic wave generated by the information device to be released into the 1 *dBμV/m* or less, is the conclusion that can be protected against information leaks. The Kuhn' s security limit [7] is 1 *dBμV/m*, assuming a constant radio attenuation at a distance of 10 m and a receiver BW of 5 MHz in the VHF and UHF bands. In addition to, [25] proposes the security limit that is 49.5 *dBμV/m* from 100 MHz to 500, 50.7 *dBμV/m* from 500 MHz to 1000 MHz, and 56.8 *dBμV/m* at 1000 MHz. Because constant radio attenuation was not considered the influence of channel environment, the Kuhn' s emission security limit did not reflect the pathloss characteristics of the compromising emanation in a real environment.

5.4.3. ITU-T K.84 Guideline

A. The guiding concept

Whereas proposed method by Markus our is laid the foundation for computing the *SNR* with an emphasis on noise component that appears during signal transmission system, the provided method provided by NTT represents the shape of deriving a base shield on the basis of the minimum input level of the receiver. Also in this method, the parameters set the same system as

Figure 5.1, is considered are minimum receiver input voltage level and minimum *SNR* required to restore the signal.

B. Antenna factor

Antenna factor is a parameter showing the electromagnetic field generated around the antenna and is expressed by the following equation.

$$A_f(dB) = E(dB\mu V) - V(dB\mu V) \tag{5.10}$$

If the input impedance of the antenna is matched to 50Ω, with the gain of the antenna *G*, the antenna factor may be calculated as Equation (12) in general.

$$A_f = 20 \cdot \log_{10}(f[MHz]) - G - 29.79 \tag{5.11}$$

The most ideal antenna factor has a value of 0, which is a mode in which the output signal is generated by an electromagnetic field around without any loss. The antenna having the small antenna factor shows the high performance.

C. Minimum input voltage level

This parameter represents the sensitivity of the receiver and shows a minimum signal voltage level can be processed at the receiver. If the bandwidth is wider, the minimum input voltage level increases as fallen to its

characteristics sensitivity. The input voltage level of the signal has a form such as (5.12).

$$E_{\min} = V_{\min} + SNR + A_f \qquad (5.12)$$

Here, *SNR* is the strength ration between the signal required for signal reproduction and noise. In other words, performance is reduced to increase in noise so that a recognized signal noise is increased by the characteristic in response to the increase in bandwidth.

D. Minimum *SNR* for restoration

The NTT data has been presented classified into three types: a used receiver, is shown by dividing the *SNR* value that is required for signal recovery when using the receiver, respectively. Table 5.5 shows the required *SNR* for the each receiver.

Table 5.5 Examples of receiver and required *SNR*

Receiver	**Classification of Receiver**	**Minimum *SNR***
Receiver I	Amateur receiver	20 dB
Receiver II	General-purpose EMC receiver	15 dB
Receiver III	Special receiver for TEMPEST	0 dB

E. Maximum distance for restoration EMSEC signal

NTT document derived the maximum distance that can be restored the EMSEC signal.

(1) Antenna factor

They have selected the lowest antenna factor by investigating the Yagi antenna amateur radio for VHF bands. The selected antennas have the antenna factor from 2.2 dB at 144 MHz to 19.0 dB at 2.4 GHz.

(2) Minimum input voltage level

Checking the specifications of the receiver, minimum input voltage level was presented to -13 dBμV of 120 kHz receiver bandwidth in general. The reception bandwidth required at least 3 MHz to recover information from the received signal. The minimum input voltage level of the receiver is calculated (5.13).

$$-13+10\log_{10}(3\times10^{6}/1.2\times10^{5})=0.98\ dB\mu V \qquad (5.13)$$

(3) Calculation of limit level

Using the TEMPEST equipment, it is possible to restore the leak electromagnetic waves only *SNR* of 0 dB or more. It is assigned to derive equation (5.13) by obtained parameters , a limited level is obtained 3.18 dBμV at 144 MHz, 13.28 dBμV at 1.2 GHz

Compared with the class B and class A of VCCI, a Japanese EMI certification standards, the level is derived, if the EMSEC signal is radiated in a space surrounded by the reinforced wall, TEMPEST receiver as shown in Figure 5.5 it is determined that it is possible to restore and reception of signals up to about the 105 meter.

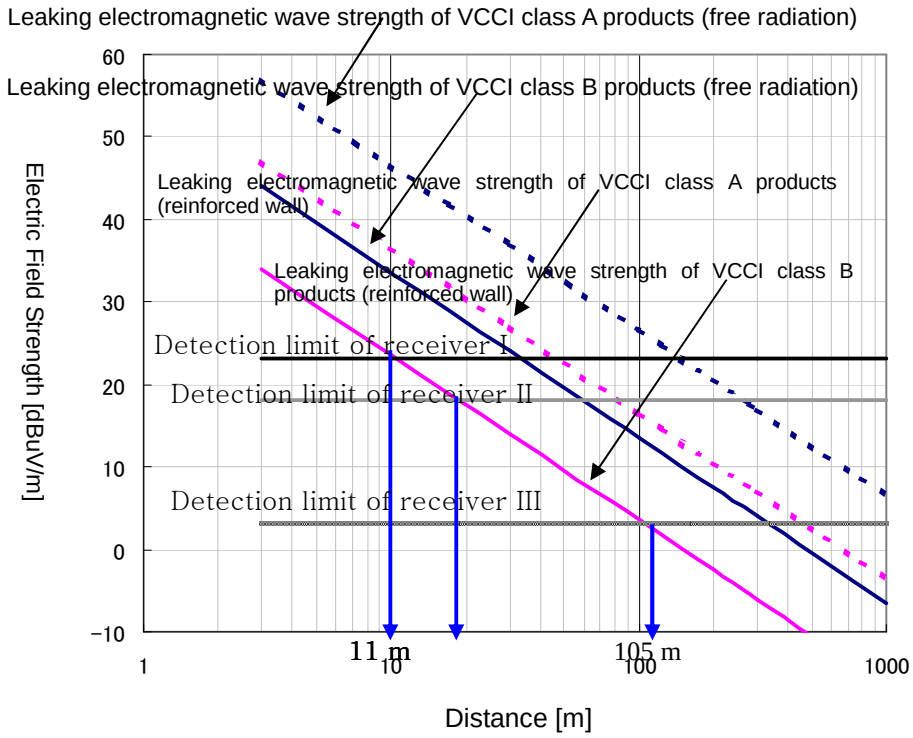


Figure 5.5 Relationship between possible electric field strength and distance for EMSEC

Fig. 5.6 shows the comparison between our proposed security limits and the other standards. The proposed periodic emission security limit for class B is

19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 0–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [25] is from 0.3 dB to 7.3 dB. However, Kuhn used the mimimum constant radio attenuation values to propose the security limits using the three survey documents [32,33, 34].

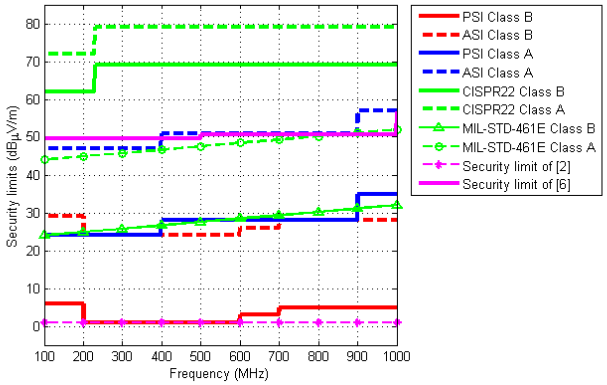


Figure 5.6 Comparison between our proposed security limits and other security limits and EMC standards

5.5 Conclusion

In this chapter, we present our proposed periodic and aperiodic emission security limits in the target frequency bands using the frequency correlation indoor EMSEC-channel analysis. In chapter 4, we measure and analyze the frequency correlation indoor EMSEC-channel under indoor environments. Based on these results, we found that the TRA in dB can be modelled as a random process that follows a Rician distribution at each channel. We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment: 29–41dB at CM2, a 42–57 dB at CM3, 47–57 dB at CM4, and 24–29 at CM5.

Emission security limits class A and class B are influenced by TRA which is affected by frequency and channel environment. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. And periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 900-1000 MHz, respectively. The difference with emission security limits of class A and class B implies the difference between the maximum and minimum values of the TRA which are affected by channel environments and frequency band. In addition, the differences with the PECI and AECI of emission security limits have the processing gain, 23 *dBi* owing to the redundancy caused by repetitive signals. So, that the PECI is easily leaked and

reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

For our proposed security limit's reliability and practicality, we compared the existing security limits, including the civilian and military EMC standards as same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits. The proposed periodic emission security limit for class B is 19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 2–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB only. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [6] is from 0.3 dB to 7.3 dB. However, Kuhn used the mimimum constant radio attenuation values to propose the security limits using the three survey documents [32,33, 34].

Chapter 6. Summary and further study

Radio wave is unintentionally emitted from information technology equipment. The important information can be reproduced by these received electromagnetic waves using the high sensitive antenna and receiver intentionally. This phenomenon is referred to as compromising emanations (CEs) or Electromagnetic emanation security (EMSEC).

While important documents related to these compromising emanations have been withheld from the public by military organizations. In addition, existing general EMC standards and security limits for compromising emanations are unsuitable for emission security purposes. For this reason, reasonable emission security limits for various electronic devices dealing with significant information are necessary. In our study, we focused on establishing the security limits for the compromising emanations in indoor environments.

Secondly, we represent how to build the EMSEC-system and to restore the signal leakage of electromagnetic waves on the basis of the signal characteristics of the electromagnetic wave leakage of printer and PC monitors that you saw in Chapter 2. The parameters that can improve the performance of signal recovery of the leakage electromagnetic wave, it can be given antenna sensitivity, RBW of the receiver, and signal processing gain. To adjust the signal processing gain, antenna which have the high antenna gain, and the use of wider RBW on receiver are improved hardware of EMSEC system.

Whereas, post-processing image restoration algorithm for a EMSEC system is a portion corresponding to the software of EMSEC system.

Techniques for increasing signal strength and noise reduction are particularly important when trying to measure compromising emanations because the magnitude of these signals can be extremely small. Averaging technique find to achieve maximum cross correlation between recorded electromagnetic leaked signals. That method is a practical, highly effective and widely used technique for increasing the signal-to-noise ratio (*SNR*) of a periodic signal, such as that generated by the image-refresh circuitry in a video display system. But, the printer and facsimile exhibit aperiodicity in their EMSEC-channel information during their operation state unlike video display systems. Since the aperiodic EMSEC-channel information of equipments such as printers and faxes is not involved in processing gain, the differences between periodic- and aperiodic-compromising emanations need to be considered in order to establish emission security limits. We reconstructed the EMSEC-channel information from VUDs and printer using the averaging technique and proposed the adaptive deringing filter.

Next, we perform the electromagnetic emanation security (EMSEC)-channel measurements in the 100–1000 MHz frequency bands. Second, we analyze the pathloss characteristics of the indoor EMSEC-channel based on these measurements. We find the frequency correlation pathloss characteristics of compromising emanations to determine the reasonable total radio attenuation (TRA). Also, the pathloss exponent value have a range from 1.06 to 2.94

depending on frequency band and the CMs, which in turn differed with propagation environments.

Through this EMSEC-channel analysis, we affirm that the total radio attenuation, which is one of the key parameters for determining the security limits for compromising emanations, follows the Rician distribution. However, previous work assumed that radio attenuations would have constant values. We found that the TRA does not show significant differences depending on the frequency bands and has the following range depending on the environment, 29–41dB at CM2, a 42–57 dB at CM3, a 47–57 dB at CM4, and 24–29 at CM5. In addition to, CM3 and CM4 have greater TRA than CM2 and CM5.

With these results, we propose that periodic and aperiodic emission security limits can be classified into two levels depending on the total radio attenuation and the extent of required confidentiality. Periodic emission security limits for class A is 24, 28, 35 $dB\mu V/m$ in the 100-400 MHz, 400-900 MHz and 900-1000 MHz, respectively. Similarly, periodic emission security limits for class B is 4, 1, 3, 5 $dB\mu V/m$ in the 100-200 MHz, 200-600 MHz, 600-700 MHz and 700-1000 MHz, respectively.

Aperiodic emission security limits are weaker than the processing gain G_p, 23 *dBi* than periodic emission security limits owing to the redundancy caused by repetitive signals. So, that the periodic EMSEC-channel information is easily leaked and reconstructed, which results in a potential risk. Thus, the periodic emission security limits must be stronger than the aperiodic emission security limits.

The proposed security limits are compared with other security limits and existing civil and military EMC standards as same measurement conditions such as BW of 5 MHz and distance d of 10 m, and VHF and UHF bands with the proposed security limits. The proposed periodic emission security limit for class B is 19–31 dB stricter than the MIL-STD-461E class B standard and 57-68 dB stricter than the CISPR22 class B standard. The proposed periodic emission security limit for class A is 9–28 dB stricter than the MIL-STD-461E class A standard and 37–55 dB stricter than the CISPR22 class A standard. In addition, the proposed aperiodic emission security limit for class B is similar to the MIL-STD-461E class B but differed slightly by 2–5 dB. The proposed aperiodic emission security limit for class A is similar to the MIL-STD-461E class A, with a difference of 0–6 dB only. Further, the proposed periodic emission security limit for class B is the same as the Kuhn' s emission security limit from 200 MHz to 600 MHz. And differenciation between aperiodic emission security limit for class A and security limit of [25] is from 0.3 dB to 7.3 dB.

Future works may include characterization and reconstruction of FAX, inkjet printer and other electronics. And it is need to EMSEC-channel analysis in more complex environments.

Bibliography

[1] *International Telecommunication Union*, "Test methods and guide against information leak through unintentional EM emission," in *ITU-T SG5*, *Rec. K.84*, Geneva, 2011.

[2] T. Tosaka, Y. Yamanaka, and K. Fukunaga, "Evaluation method of information in electromagnetic disturbance radiated from PC display using time varying stripe image," *IEICE*, 2010.

[3] *National Security Agency*, "Compromising emanations laboratory test requirements, Electromagnetics," in *NSTISSAM TEMPEST/1-92*, Dec. 1992.

[4] *International Electro-technical Commision*, "Information technology equipment, radio disturbance characteristics, limits and methods of measurement," in *IEC CISPR22 edition 6.0*, Sep. 2008.

[5] US Department of Defense, "Requirements for the control of electromagnetic interference characteristics of subsystems and equipment,", in *DOD MIL-STD-461E* Aug. 1999.

[6] R. M. Showers, "A comparison of military and civilian EMC standards," *IEEE Int. Symp. on Electromagn. Compat.*, pp.284-288, Aug. 1999.

[7] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," *Technical Report, UCAM-CL-TR-577*, Dec. 2003.

[8] Deborah Russell, G.T. Gangemi Sr. : Computer Security Basics. Chapter 10 : TEMPEST, O'Reilly & Associates, 1991.

[9] A. J. Mauriello, “Join a government program to unveil Tempest-spec mysteries”, *EDN*, Vo. 28, no. 13, pp. 191-195, June 23, 1983.

[10] Anton Kohling, “TEMPEST – an introduction and overview on compromising emanations, one aspect of information security”, *EMV*, Stuttgart, Feb. 1992.

[11] John Young, “How Old is TEMPEST?”, online response , Feb. 2000. http://cryptome.org/tempest-old.htm

[12] Wim van Eck, “Electromagnetic Radiation from Video Display Units : An Eavesdropping Risk?”, *Computer & Security*, vol. 4, pp. 269-286, 1985.

[13] W. Rankl, W. Effing, “Smart Card Handbook”, *John Wiley & Sons*, 2004.

[14] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis.” In Michael Wiener (Ed.), *Advances in Cryptology*. . *CRYPTO’99, LNCS* 1666, Springer, pp. 388.397, 1999.

[15] Suresh Chari et al., “Towards Sound Approaches to Counteract Power-Analysis Attacks.”, *Advances in Cryptology* . *CRYPTO’99, Proceedings, Lecture Notes in Computer Science* 1666, Springer-Verlag, pp. 398.412, 1999.

[16] T.S. Messerges, E.A. Dabbish, R.H. Sloan, “Examining smart-card security under the threat of power analysis attacks.”, *IEEE Tran. on Computers*, Vol. 51, No. 5, May 2002, pp. 541.552.

[17] Jean-Jacques Quisquater, David Samyde, “ElectroMagnetic Analysis (EMA): Measuresand Counter-Measures for Smard Cards.”, *Smart Card*

Programming and Security (E-smart2001), Cannes, France, LNCS 2140, September 2001, pp. 200.210.

[18] K. Gandolfi, C. Mourtel, F. Olivier, “Electromagnetic Analysis: Concrete Results.”, *CryptographicHardware and Embedded Systems* . *CHES* 2001, LNCS 2162, Springer, 2001, pp. 251.261.

[19] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi, “The EM Side-Channel(s).”, *4th International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS 2523, Springer, 2002, pp. 29–45.

[20] Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi, “Multi-channel Attacks.”, 5th International Workshop on Cryptographic Hardware and *Embedded Systems, LNCS* 2779, Springer, 2003, pp. 2–16.

[21] Suresh Chari, Josyula R. Rao, Pankaj Rohatgi, “Template Attacks.”, *4th International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS 2523, Springer, 2002, pp. 13–28.

[22] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanation of wired and wireless keyboards," *18th Int. Symp. USENIX*, pp.1–16, Mar. 2009.

[23] T. Tosaka, K. Taira, Y. Yamanaka, K. Fukunaga, A. Nishikata, and M. Hattori, "Reconstruction of printed image using electromagnetic disturbance from laser printer," *IEICE Trans. Commun.*, vol.E90-B, no.3, pp.711–715, Mar. 2007.

[24] D. G. Sun, W. Q. Huang, and Z. W. Zhao, "Modeling the radiated compromising emanation for digital channel," *IEEE Conf. on Robot., Autom. and Mechatronics*, pp.1–5, Dec. 2006.

[25] M. Zoyousefein, S. Hashemniaye, and A. Ghorbani, "Security limits for electromagnetic radiation from CRT displays," *2nd Int. Conf. on Comput. and Electr. Eng.*, pp.452–456, Dec. 2009.

[26] VESA and Industry Standards and Guidelines for Computer Display Monitor Timing, ver.1.0, rev.11, May, 2007.

[27] Michael Yuen, H.R. Wu, "A survey of hybrid MC/DPCM/DCT video coding distortions," *Signal Processing*, vol. 70, pp. 247-278, July 1998.

[28] *International Telecommunication Union*, "Examples for H.263 Encoder/Decoder Implementations," *in ITU-T Rec. H.263 Appendix III*, June 2000.

[29] A. Leon-Garcia, "Random Processes," in Probability and Random Processes for Electrical Engineering, *Addison-Wesley*, Reading, 1994.

[30] H. Arslan, Z. N. Chen, and M.-G. Di Benedetto, "Ultra Wideband Wireless Communication," pp.190, *John Wiley & Sons*, 2006.

[31] T. S. Rappaport, "Wireless Communications," pp.13–26, *Prentice Hall*, 2007.

[32] *International Telecommunication Union*, "Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz.", *ITU-R P.1238-7 Rec.*, Geneva, 2012.

[33] Homayoun Hashemi: The Indoor Radio Propagation Channel. *Proceedings of the IEEE*, Vol. 81, No. 7, July 1993, pp. 943–968.

[34] L. P. Rice: Radio Transmission into Buildings at 35 and 150 mc [MHz]. Bell System Technical Journal, Vol. 38, No. 1, January 1959, pp. 197–210.

[35] *International Telecommunication Union*, "Radio noise." *ITU-R SG3, Rec. P.372-7*, Geneva, 2001.

[36] Antenna Research Associate (ARA), "MWH SERIES antenna datasheets."

초 록

컴퓨터와 같은 정보통신기기를 사용하는 동안 비의도적으로 발생되는 전자파를 고성능의 수신기를 통해 수신하여 적절한 신호처리를 하게 되면 사용 중인 정보를 복원할 수 있다는 것이 여러 문서나 논문을 통해 많이 알려져 있다. 이러한 기술을 통한 기밀의 정보 누출을 방지하기 위해 미국을 비롯한 선진국을 중심으로 1950년대 중반부터 CE (Compromising emanation) 혹은 EMSEC (Electromagnetic emanation security) 로 일컬어지는 규제 기준을 제정하여 시행하고 있다. 가장 일반적으로 알려진 기준은 미국 NSA의 NACSIM 5100A와 NATO의 AMSG720B 등이 있으며, 그 내용의 일부를 제외하고는 실제 제한 기준레벨, 테스트 절차 등은 아직도 비밀로 취급되고 있다.

정보의 누출에 대한 보호레벨 수립을 위해 모니터 및 프린터 신호에 의한 전자파의 신호 주파수와 레벨을 정확히 측정함으로써 누출 가능성에 대한 평가가 이루어져야 하므로 2장에서는 모니터 및 프린터 신호 및 신호의 전송 및 처리 과정에서 자유공간으로 방사되는 전자파 신호의 특성을 분석하고, 신호레벨의 정확한 측정을 위해 필요한 조건들을 기술하였다. 탐지된 누설전자파 신호를 분석하여 3장에서는 그 신호 복원과정과 신호 이득을 높일 수 있는 후처리 과정으로 현재 가장 일반적으로 효과적인 *SNR* 이득을 얻을 수 있는 averaging technique 방법과 MPEG-4에서 이용하고 있는 후처리 과정중 하나인 deranging filter의 아이디어를 착안한 adaptive

deranging filter를 이용하여 모니터 및 프린터 신호에 대하여 복원 시스템과 복원영상 결과를 제시하였다. 실험결과, 후처리 이미지처리 기법으로 적응형 deranging 필터를 사용한 경우 후처리 이미지 처리를 하지 않은 복원 이미지와 비교 시 PSNR의 개선이 최소 2에서 최대 10만큼 개선됨을 알 수 있었다.

4장에서는 다양한 채널환경에서 측정된 데이터를 바탕으로 누설전자파 채널을 분석하고 주파수 상관성이 반영된 거리감쇄 수식을 제안했다. 이를 바탕으로 누설전자파 보호레벨 결정에 중요한 파라미터 중 하나인 총전파감쇠량(Total radio attenuation, TRA)이 주파수나 채널환경에 상관없이 상수값을 사용한 기존의 연구결과와는 다르게 총전파감쇠량이 채널과 주파수에 영향을 받는 값임을 밝히고 TRA의 확률분포값이 rician distribution을 따름을 확인했다.

5장에서는 후처리 신호처리 과정을 지난 누설전자파 복원영상의 *SNR*은 최소입력전압, 안테나 이득 및 신호처리 이득에 비례하고 총전파감쇠량, 배경노이즈 및 수신기 잡음레벨에 반비례함을 바탕으로 누설전자파 신호 특성과 신호의 중요도에 따라 class A와 class B로 나누어 주기신호와 비주기 신호에 대한 누설전자파 보호레벨을 제안했다. Class A의 주기성 누설전자파 방사보호레벨은 100-400 MHz에서는 24 $dB\mu V/m$, 400-900 MHz에서는 28 $dB\mu V/m$, 900-1000 MHz에서는 35 $dB\mu V/m$ 값을 각각 제안한다. 유사하게 Class B의 주기성 누설전자파 방사보호레벨은 100-200 MHz에서는 4 $dB\mu V/m$, 200-600 MHz에서는 1 $dB\mu V/m$, 600-7000 MHz에서는 3 $dB\mu V/m$, 700-1000 MHz에서는 5 $dB\mu V/m$ 값을 각각 제안한다.

주기성 누설전자파 방사보호레벨과 비주기성 방사보호레벨 간의 차이는 신호처리 이득인 약 23 dB 만큼의 차이가 발생되며 이는 주기성을 가지는 누설전자파 신호가 신호복원이 쉽기 때문에 강인한 보호레벨이 필요함을 말한다. 한편, class A 보호레벨과 class B 보호레벨과의 차이는 채널환경과 주파수, 신호의 보안정도에 의한 값의 차이임을 알 수 있다.

본 논문의 마지막은 우리가 제안한 누설전자파 방사보호레벨의 신뢰성을 확인하기 위하여 기존의 표준레벨인 CISPR EMC 기준값과 군에서 사용하고 있는 MIL-STD-461E 값 및 기존의 Kuhn의 방사보호레벨 및 ITU-T K.84의 방법을 함께 비교하였다.

주요어 : 누설전자파, 채널모델링, 주파수 상관관계, Rician 분포

학번 : 2006-30856