

I Can See What You Are Seeing: A Trial of Intercepting Display Image Using Electromagnetic Emanations from VGA Cable

Submitted by

Wu Jinzhou

In partial fulfilment of the
requirements for the Degree of
Bachelor of Engineering (Computer Engineering)
National University of Singapore

B.Eng. Dissertation

**I Can See What You Are Seeing: A Trial of Intercepting Display Image
Using Electromagnetic Emanations from VGA Cable**

By

Wu Jinzhou

Department of Computer Science

School of Computing

National University of Singapore

2013/2014

Project No: H004890

Advisor: Assoc. Prof. Hugh Anderson Assoc. Prof. Chang Ee-Chien

Deliverables:

Report: 1 Volume

Program: 1 Diskette

Data: 1 Diskette

Abstract

VGA cable and display unit are typical mediums for information transmission and output in a computer system. Since VGA cable is made by metal wires and carries display signal, it eventually emits electromagnetic waves. These emanations reveal display image and may cause private and sensitive information leakage. This report describes the experiments and analysis of the interception of personal computer's display image using emanation of electromagnetic wave from VGA cable. In the experiment, a modern full HD flat LCD screen connected to a personal computer via VGA cable is used as the target display, the interception is performed under normal office/home environment condition. In our work, we have (1) studied the computer display monitor timing and identified the sync information, (2) intercept the electromagnetic emanations from VGA cable, (3) processed the intercepted data and restored the display image on the target screen and (4) analyzed the image reconstruction results by repeating step (2) at various distance. We have fully or partially restored the display image at the distance from less than 1 cm up to 30 cm away from the signal source. Both observation results and analysis results suggest that the bright text on the dark background is more secure than the dark text on the bright background in against of interception under experimental settings.

Subject Descriptors:

H.3.3 Information Search and Retrieval

K.6.5 Security and Protection

Keywords:

Electromagnetic wave, Compromising emanations, Side-channel attack, TEMPEST on VGA cable, Information security

Software and Hardware:

OS X 10.9, Windows 8, GNU Radio Companion 3.7.2.1 with UHD 003.005.004, Xcode 5.02, Ettus USRP B100, HP 2309m 23 inch Diagonal Full HD LCD Monitor, Personal Computer, VGA Cable, Wire Loops

Acknowledgement

I would like to express my deep gratitude to Professor Hugh Anderson and Professor Chang Ee-Chien, my project supervisors, for their patient guidance, enthusiastic encouragement and useful critiques of this project work.

I would like to express my very great appreciation to Professor Hugh Anderson for his valuable and constructive suggestions during the planning and development of the project. Advices given by him have been great helpful through out the project duration. His willingness to give his time so generously has been very much appreciated.

I would also like to express my grateful thanks Professor Chang Ee-Chien, for his encouraging and monitoring in keeping my progress on schedule. His valuable comments and sharing of knowledge made this project work possible.

Table of Contents

Title	i
Abstract	ii
Acknowledgement	iii
1 Introduction	1
1.1 Background	1
1.1.1 TEMPESTS and Compromising Emanation	1
1.1.2 Two Types of Electromagnetic Emanations	2
1.1.3 Computer Displays Under Electromagnetic Eavesdropping	3
1.2 Software-defined Radio	4
2 Equipment and Technical Discussion	6
2.1 The Equipment	6
2.1.1 USRP B100	6
2.1.2 HP Pavilion 2309m Monitor	6
2.2 Technical Discussion	7
2.2.1 Video-signal Timing and Spectra	7
2.2.2 Sampling Rate and Down-sampling	10
2.2.3 Background Noise and Signal Interception	11
3 Data Interception	13
3.1 Experimental Setup	13
3.2 GNU Radio Function Blocks and Data Capture	15
4 Data processing and Image Reconstruction	17
4.1 Sync Reconstruction	18
4.1.1 Noise Reduction	18
4.1.2 Frame Extraction	20
4.1.3 Line Extraction	23
4.2 Image Reconstruction	26
5 Experiment Result and Threat Analysis	28
5.1 Experiment Result and Discussion	28
5.2 Threat Analysis	30
5.2.1 Observation and Analysis	30
5.2.2 Conjecture and Verification	32
6 Conclusions and Recommendations	34
6.1 Summary and Conclusion	34
6.2 Limitations and Recommendations	35
References	iv
Appendix – Data Used in Statistics	v

Chapter 1: Introduction

Digital computers and electronic devices have been in our daily life since the past half century, as the consequence, many fields of business and industry have become strongly dependent on the mobility, reliability, and confidentiality of digital processed information. These digital equipment transmit energy in many forms, such as electrical currents, magnetic force, heat, electromagnetic waves, and mechanical vibrations. Most energy consumed will be used to form cyphers for the purpose of communication or lost as dissipation. However, some of the dissipations are correlated in various ways to processed data and can form unintended information leaks. This gives alternative opportunities for ulterior outsiders to get unauthorized access to processed confidential information.

1.1 Background

1.1.1 TEMPESTS and Compromising Emanation

Side-channel cryptanalysis has been used successfully to attack many cryptographic implementations¹. The term "TEMPEST" coined in the late 1960s and early 1970s was a codename for the U.S. National Security Agency operation to secure electronic communications equipment from potential eavesdroppers. Now, "TEMPEST" is often used broadly for referring to the type of Side-channel attack based on investigations and studies of compromising emanations.

Compromising emanations are defined as unintentional intelligence-bearing signals, which, if intercepted and analyzed, may disclose the information, transmitted, received, handled, or otherwise processed by any information-processing equipment. Compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or by mishap unintentionally emitted by any number of sources within equipment or systems. This energy may relate to the original pre-encrypted or non-encrypted message, or information being processed, in such a way that can lead to sensitive information disclosure.

¹ P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. Advances in Cryptology-Crypto '96, Springer.com, Lecture Notes in Computer Science # 1109, pp 104–113.

The compromising signals can, and do, exist in several forms such as magnetic- and/or electric field radiation, line conduction, or acoustic emissions². Laboratory and field tests have established that such compromising emanations can be propagated through space and along nearby conductors. The interception/propagation ranges and analysis of such emanations are affected by a variety of factors, e.g., the functional design of the information processing equipment; system/equipment installation; and, environmental conditions related to physical security and ambient noise.

1.1.2 Two Types of Electromagnetic Emanations

Electromagnetic emanations arise as a consequence of current flows within the control, I/O, data processing or other parts of a device. Each current carrying component of the device not only produces its own emanations based on its physical and electrical characteristics but also affects the emanations from other components due to coupling and circuit geometry. According to the study from IBM Watson Research Center³, electromagnetic emanations can be generally classified as direct emanations or unintentional emanations.

Direct emanations are result from intentional current flows. Usually, components at the higher frequencies prove more useful to the attacker due to overwhelming noise and interference prevalent in the lower frequency bands. In complex circuits, isolating direct emanations can be difficult and may require use of tiny field probes positioned very close the signal source and/or special filters to minimize interference from other signal sources⁴⁵.

Unintentional Emanations are created by electrical and electromagnetic coupling between circuit components. Such couplings provide a rich source of compromising emanations to the attacker. These emanations manifest themselves as modulations of carrier signals, one

² Public version of NACSIM 5000 Tempest Fundamentals, <http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm>

³ Dakshi Agrawal Bruce Archambeault Josyula R. Rao Pankaj Rohatgi The EM Side-Channel(s): Attacks and Assessment Methodologies, Springer.com, Lecture Notes in Computer Science Volume 2523, 2003, pp 29- 45

⁴ K. Gandolfi, C. Mourtlet and F. Olivier. Electromagnetic Attacks: Concrete Results. In the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2001 (CHES 2001), LNCS 2162 Paris, France, May 2001, pp 251-261

⁵ Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In Smart Card Programming and Security (E-smart 2001), Cannes, France, LNCS 2140, pp.200-210, September 2001.

strong source of carrier signals is the harmonic-rich “square-wave” clock signal⁶ propagated throughout the device. Some of the ways modulation occurs, which include amplitude modulation and angle modulation. Amplitude Modulated (AM) signals are generated and emanated by the non-linear coupling between a carrier signal and a data signal. The data signal can be extracted by using a receiver tuned to the carrier frequency and followed by performing AM demodulation. Angle Modulated Signals (FM or Phase modulation) are also generated by circuit coupling. In the ideal condition, signal generation circuits should be completely decoupled from data processing circuits, however, this is rarely achieved in practice. As the consequence, if these circuits draw upon limited energy source, the generated signal, very often, is angle modulated by the data signal. The data signal is then recoverable by performing angle demodulation of the generated signal.

1.1.3 Computer Displays Under Electromagnetic Eavesdropping

Many studies have demonstrated the feasibility of electromagnetic eavesdropping attacks based on timing and power by collecting the AM signal leakage. The first electromagnetic eavesdropping of computer displays was demonstrated to the public by van Eck in 1985⁷. In the experiment, the leaked signal from cathode ray tube (CRT) video display unit (VDU) was captured three hundred meters away by using a directional antenna and TV receiver, and the video synchronization was restored by using a variable oscillator and a frequency divider circuit.

Study shows that electromagnetic eavesdropping of computer displays is not restricted to cathode-ray tubes. Modern flat-panel and laptop displays are also vulnerable to electromagnetic eavesdropping. A proof of concept system was created by Markus G. Kuhn at the University of Cambridge in 2004, which managed to reproduce the display of an LCD screen at 10 meters and through 3 plasterboard walls.

According to Kuhn's report⁸, there are two main differences between CRT displays and flat

⁶ L. Goubin and J. Patarin. DES and Differential Power Analysis. Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES '99, LNCS 1717, August 12–13, 1999, Worcester, MA, pages 158–172.

⁷ Van Eck W. Electromagnetic radiation from video display units: an eavesdropping risk? Computers and Security, 1985, 4(4): 269–286

⁸ Markus G. Kuhn Electromagnetic Eavesdropping Risks of Flat-Panel Displays, (4th Workshop on Privacy Enhancing Technologies proceedings, Springer-Verlag, LNCS 3424).

panel displays (FPD) when considering the electromagnetic eavesdropping risk. First, FPDs lack deflection coils, which make them “low radiation” devices compared to CRTs in the frequencies below 400 kHz. What’s more, the field strengths of LCDs are limited by a Swedish ergonomic standard⁹. Second, LCDs operate with low voltages and – unlike CRTs – do not amplify the video signal by a factor of about 100 to drive a control grid that modulates an electron beam.

The two differences between CRTs make FPDs thought to be safer under the eavesdropping, however, Kuhn’s report shows it is just other way. The experiments reported that some types of flat-panel display do pose a realistic eavesdropping risk and even easier to receive than those of modern CRTs. By using a super- heterodyne AM receiver that multiplies the input signal with a sine wave of adjustable frequency, the frequency band of interest can be shift to a fixed intermediate frequency where it can then be filtered easily to the required bandwidth. The video information, which converted with specially written software into raster images, can be recorded and restored by a computer controlled digital storage oscilloscope with 8-bit resolution, 16 MB acquisition memory, and up to 1 GHz sampling frequency that directly connected to the output of the AM demodulator.

Kuhn’s study finally suggest that the video cable used to connect the display panel with the graphics controller turned out to be the primary source of the leaking signal. What’s more, with some modern video interfaces, it is quite easy to configure the display of text in a way that maximizes the leaking signal strength, which makes emanations from video interfaces used with flat-panel displays emit significantly stronger and better to decode signals than CRTs.

1.2 Software-defined Radio

Electromagnetic emanations from video cable leads display information leakage, the leaked data information can be intercepted and reconstructed by various methods, the traditional way of intercepting electromagnetic emanations is by using the integrated hardware circuit with different functional components, a new way to do the same work is by using the

⁹ TCO’99 – Mandatory and recommended requirements for CRT-type Visual Display Units (VDUs). Swedish Confederation of Professional Employees (TCO), 1999. <http://www.tcodevelopment.com/>

software-defined radio (SDR).

In traditional way, electromagnetic emanation is captured by using broadband antenna receiver, filter, amplifier, analog-to-digital converter and other equipment. After the data signal being intercepted, the original information can be restored by processing the digital signals through correlated reconstruction technology. Since the frequency, modulation, and other parameters of electromagnetic emanations are usually unknown, experienced operators are needed to adjust the intermediate frequency (IF) and bandwidth of receiver. In addition, the performance of information interception will be limited by the receiver's capability while high performance broadband receivers can be very costly. Thus, the interception based on traditional method is not only expensive but also difficult to realize.

In 1992, Joseph Mitola III introduced the concept of software-defined radio. The core idea is to construct an open, standardized, and modular hardware platform in which the A/D and D/A converter are attached to antenna, and, using software to transform the stream of data from the converter to any other form the application requires. Using software to perform signal processing instead of using hardware increases the system flexibility and reduces the cost.

Based on the idea of using software-defined radio, in this project, we have built the hardware platform on the Ettus Universal Software Radio Peripheral (USRP), a software-defined radio, to perform an electromagnetic emanation interception on the VGA cable connect between a personal computer and a LCD display at various distance. The intercepted electromagnetic emanation is recorded and encoded by GNU Radio, an open-source software development toolkit that provides various signal-processing blocks to handle signal acquisition.

Chapter 2: Equipment and Technical Discussion

This section introduces the experiment preparation, the equipment will be used and the theatrical foundations. Ettus USRP is the software-defined radio that used to intercept the electromagnetic emanation form VGA cable and HP Pavilion 2309m Monitor is the target monitor that connects to a PC via the intercepted VGA cable. Two theoretical foundations - the Nyquist sampling theory and Fourier analysis - combined with basic engineering knowledge about inductance have been used in the experiment theoretical preparation.

2.1 The Equipment

2.1.1 USRP B100

The Ettus Research USRP B100 (Figure 3.1) is an entry-level software-defined radio. The hardware provides a maximum analog to digital sampling rate of 64 MS/s with 12-bit resolution,

and up to 16 MS/s of signal streaming through the USB 2.0 host interface. In the experiment the device is used to receive the electromagnetic emanation form VGA cable.



Figure 3.1: USRP B100

2.1.2 HP Pavilion 2309m Monitor

The HP Pavilion 2309m (Figure 3.2) is a 23-inch wide-screen monitor with liquid crystal display (LCD) and thin-film transistor (TFT) screen. The screen has a 1920x1080@60Hz factory-set resolution with horizontal scan range from 24 KHz to 94 KHz and vertical scan range from 48 Hz to 76 Hz. In the experiment, this display is used as the target screen that connects to a PC via the intercepted VGA cable.



Figure 3.2: The HP Pavilion 2309m

2.2 Technical Discussion

2.2.1 Video-signal Timing and Spectra

Most modern computer video despoils are raster-san devices. Similar as in an old CRT display, the graphic signal is transmitted and update as a sequence of scan lines that filled up the entire display area periodically with a constant velocity. The pixel luminosities in the scan line are the functions of the graphic-signal voltage. In the color VGA graphic signal format, each pixel color is a combination of the 3 primary colors R (Red intensity), G (Green intensity) and B (Blue intensity) whereas RGB signals take values in a continuous (analog) voltage range from +0 V (absolutely dark) to +0.7 V (maximum brightness). Each of these 3 signals controls a screen's liquid crystal bright a basic color (R, G or B) in a pixel. Any color is the visual mixture of different levels of brightness of the 3 primary colors.

An important characteristic of the video signal is pixel clock frequency f_p , which is – in the case of a CRT – the reciprocal of the time in which the electron beam travels from the center of one pixel to the center of its right neighbor. The pixel clock is an integer multiple of both the horizontal and vertical deflection frequency, that is the rate of line sync multiplies by the rate of frame sync. It is noteworthy that the actual image displayed on the screen is only a portion of the frame, while the specification of "1920x1080@60 Hz" means "the number of visible (addressable) pixels in one scan line is 1920 and the number of visible (addressable) lines in one frame is 1080 where the frame refreshes at a rate of 60 Hz". One line contains some "(imaginary) invisible pixels" (horizontal blacking) to transmit line (horizontal) synchronization pulses and one frame contains some "(imaginary) invisible lines" (vertical blacking) to transmit frame (vertical) synchronization pulses.

In order to grand a unified factory adjustment of the image geometry in displays over the wide range of video timings used in personal computers industry, the Video Electronics Standards Association (VESA) has standardized a collection of exact timing parameters, which most PC monitor use today.

The target monitor (HP Pavilion 2309m Monitor) used in the experiment operates in the

graphic mode of 1920x1080@60 Hz. According to the VESA standards¹⁰, it has a pixel rate of 148.5 MHz, line rate of 67.500 KHz and frame rate of 60 Hz. The detailed timing parameters are illustrated in Figure 3.3.

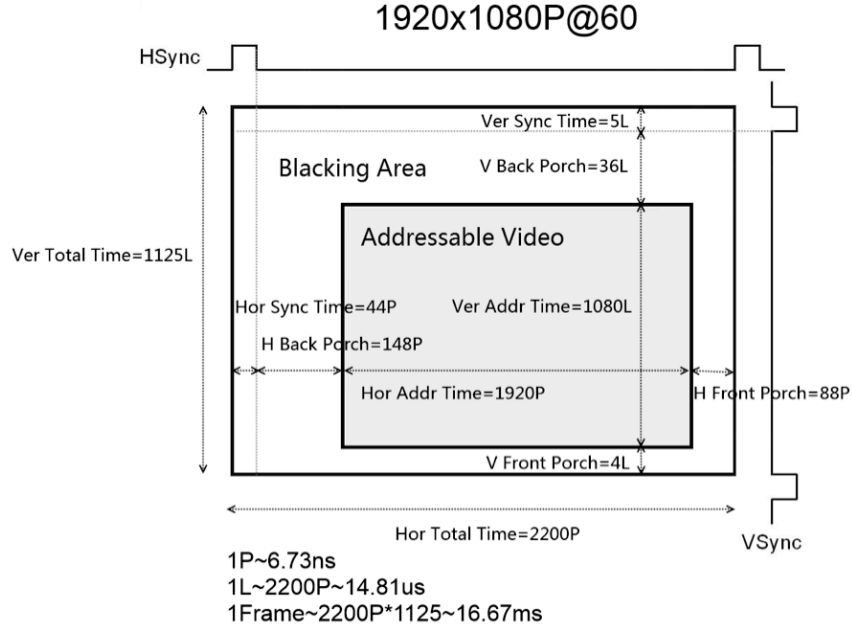


Figure 3.3: The VESA standards of monitor resolution “1920x1080@60 Hz”.

As shown in Figure 3.3, when the target monitor is operating under 1920x1080@60 Hz resolution mode, the horizontal blacking takes 12.7% of total horizontal time and vertical blacking takes 4.0% of total vertical time. There are 2200 pixels in one line and 1125 lines in one frame. The color control signal is only triggered in addressable video range.

The pixel signal generated by the graphic card from one primary color control channel of RGB with pixel clock frequency f_p , period $T_p = \frac{1}{f_p}$, and pixel values A_n ($n \in \mathbb{Z}$) can be represented as a stream of non-return-to-zero (NRZ) line code with expression:

$$s_p(t) = \sum_{n=-\infty}^{\infty} A_n \cdot g(t - nT_p) \quad (3.1)$$

Where A_n is any real number between 0 and 0.7 and $g(t)$ is the periodic unit pulse function with magnitude equals to 1 and period equals to T_p . An illustration of equation (3.1) is shown in Figure 3.4:

¹⁰ VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1.0, Revision 12p, Draft 3 10/17/08, Page 86 of 100

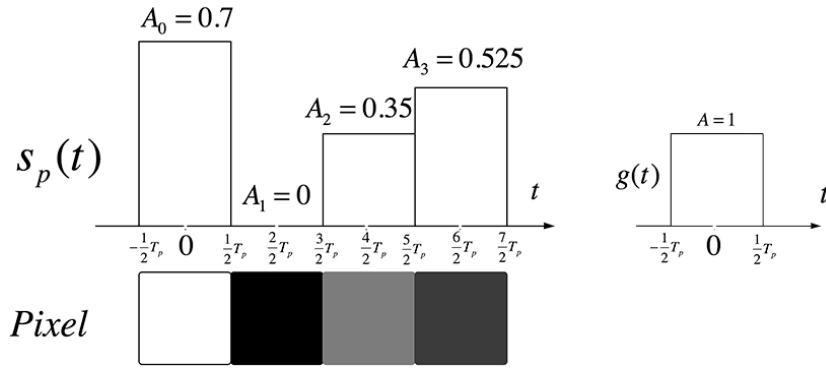


Figure 3.4: An illustration of pixel signal as a train of NRZ line code

The frequency spectra of the pixel signal can be obtained by applying the Fourier transfer to the time domain signal $s_p(t)$

$$S_p(f) = \mathcal{F}\{s_p(t)\} = \sum_{n=-\infty}^{\infty} A_n \int_{-\infty}^{\infty} g(t - nT_p) e^{-j2\pi ft} dt = G(f) \sum_{n=-\infty}^{\infty} A_n e^{-j2\pi f(nT_p)} \quad (3.2)$$

Where

$$G(f) = T_p \cdot \text{sinc}(f \cdot T_p) \quad (3.3)$$

We obtained in (3.3) the Fourier transformed video signal has copies of the original spectrum in the frequency range $-\frac{f_p}{2}$ to $\frac{f_p}{2}$ repeated throughout the spectrum with a repetition distance f_p . The illustration of plot of $S_p(f)$ show in Figure 3.5 therefore should be a main lobe followed by many minor lobes. Each lobe has a bandwidth of f_p and center-to-center distance of f_p .

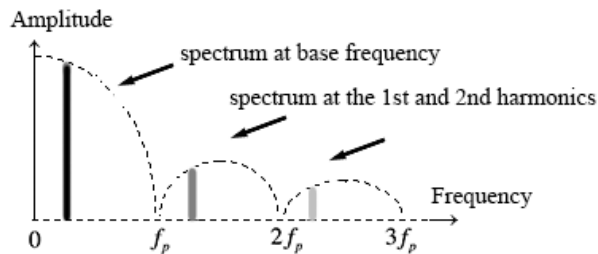


Figure 3.5 The spectra of video signal: The spectrum of the signal repeats in harmonics and decays in strength.

The above properties show the main characteristic of the electromagnetic emanation from the digital device. This information is of great importance in TEMPEST testing, signal receiving, information reconstruction and risk prevention.

2.2.2 Sampling Rate and Down-sampling

According to Nyquist's sampling theorem, the full information content of a digitally generated video signal with pixel clock frequency f_p can be reconstructed from samples whose sampling frequency is greater than $2f_p$. This theory indicates that with the increasing of the screen resolution, the sampling rate required to restore the full pixel information will increase rapidly, as increase screen resolution usually means increase the addressable video range in both horizontal and vertical direction. The target monitor used in this experiment has a native screen resolution of 1920x1080@60 Hz and a pixel rate of 148.5 MHz. According to the sampling theory, the minimum sampling rate required to restore the full content of the video signal is 297 MHz. The software-defined radio, USRP B100, however, provides a maximum sampling rate of only 64 MHz.

A down-sampling ratio needed to be decided to reduce the sampling rate. Two factors should be taken into consideration: the best achievable resolution and sample data streaming rate limitation.

USRP B100 has a maximum analog to digital sampling rate of 64 MHz. It streams the sampled data at a maximum transfer rate of 16 MS/s to a host computer via USB 2.0 interface. Theoretically, when the sampling rate is less than $2f_p$, the higher sampling rate provides the better result; using a sampling rate of 64 MHz will give a best achievable resolution of the original video signal. However, the real bottleneck of obtaining the sampled data is not the limitation of sampling rate, but the limitation of the transfer rate of the sampled data from USRP to the host computer. The sampled data transfer rate is supported up to only 16 MS/s in USRP, the 64 MHz sampling rate is practically not achievable. On another side, software platform (also the hardware driver) of USRP, the GNU Radio, forms ADC sampled signal into complex float 32-bit binary number before it being transmitted, as the result, one sampled data will be converted into a 64-bit binary number (with a value range of $[-1.0, 1.0]$). If take the transfer rate limitation into consideration, use 16 MHz sampling rate, the data transferred from USRP to the host computer, via USB 2.0 interface, in 1 second, will be $16 \text{ MS} \times 64 \text{ bit/S} = 1024 \text{ Mbit} = 128 \text{ MB}$, which is more than two times of the theoretical maximum data transfer rate (60 MB/s) of USB 2.0 interface. Although the host computer has a USB 2.0 interface whose

performance better than the theoretical value, the 128 MB/s data transfer rate is still too high for practice. Consequently, the sampling rate needs to be further decreased. Based on several tests and trials, the best sampling rate is found to be 10.667 MHz (10.667 MHz is the actual sampling rate of USRP when a required sampling rate is set to be 10 MHz). Under this sampling rate, the data transfer rate from USRP to the host computer, via USB 2.0 interface is $10.667 \text{ MS/s} \times 64 \text{ bit/S} = 682.6880 \text{ Mbit/s} = 85.336 \text{ MB/s}$, which is achievable for practice.

The theoretical sampling rate to restore the full information of the video signal is 297 MHz and the practical achievable sampling rate is 10.667 MHz, Known the actual achievable sampling rate, the down-sampling ratio can be figured out:

$$\text{Down – sampling Ratio} = \frac{\text{achievable rate}}{\text{theoretical rate}} = \frac{10.667 \text{ MHz}}{297 \text{ MHz}} = 0.0359 \quad (3.4)$$

The best achievable resolution for image reconstruction also can be calculated:

$$\text{Image Resolution Ratio} = \frac{\text{hor}}{\text{hor} \cdot \text{DSR} \times 2} = \frac{2200 \text{ pixel}}{2200 \text{ pixel} \times 0.0359 \times 2} = 13.93 \quad (3.5)$$

In Equation (3.5), *hor* is the total horizontal pixel and *DSR* is the down-sampling ratio obtained from Equation (3.4). The result from (3.5) suggests that with a sampling rate of 10.667 MHz, one sample data point is obtained for every 13.93 pixel time.

2.2.3 Background Noise and Signal Interception

The data interception experiment is performed in a normal office/home environment condition where the electromagnetic emanation signals are dominated by background noise. It is in practice not feasible to eavesdrop electromagnetic signal in this condition without a directional antenna – since outside special shielded chambers, waveforms picked up by receiver will be dominated by the many radio broadcast services and numerous other sources of radio noise that populate the spectrum from below 10 kHz to above 10 GHz.

A selectively amplify of the emanated video signal from VGA cable is necessary if a

directional antenna is not available. I used this approach to amplify the electromagnetic emanation as shown in Figure 3.6. By attaching a wire coil to the VGA cable (more specifically, the red-color control channel in the cable), the intended signal was amplified to a clearly recognizable level against the background noise without using a shielded chamber or a directional antenna.

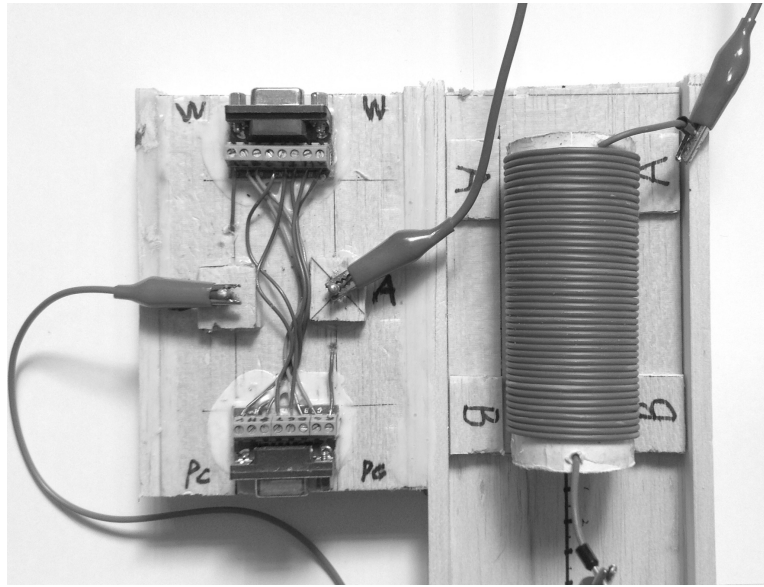


Figure 3.6: A wire coil is attached to the red-color control channel of the VGA cable

In Figure 3.6, the coil attached to the VGA cable is placed on a wood guide that is used to mark the separation distance (with accuracy of 1cm) from itself to the receiver. The receiver is made by another wire coil and connected to the USRP.

As the coil is attached to red-color control channel, this setting can only detect the signal from red color. As the consequence, this brings some limitations to the experiment. Firstly, the image displayed on the target screen must contain red-color component. Which means, if the image is composed by only green and blue color it won't be detectable since the red control channel is not being used. Secondly, the sync signal is not being detected. Both horizontal sync signal and vertical sync signal has its exclusive control channel in the VGA cable and they are not transmitted with the color signal. Missing synchronization may bring visual artifacts to the reconstructed image include repeating (out of vertical sync) and tearing (out of horizontal sync). However, it is possible to infer the horizontal sync signal and vertical sync signal from the color control channel by using certain sync algorithms. Experiment result shows that a reconstruction of the target screen image with out detecting the sync signal is achievable in a small separation distance range.

Chapter 3: Data Interception

This chapter describes the hardware connections and the software platform that used in the experiment. A personal computer, VGA cable and the target monitor are together formed the experiment subjects. USRP B100, host computer, and the GNU Radio are together formed the experiment detection equipment. The NUS logo is chosen as the target image that displayed on the target screen. Two wire coils at various separation distances are used in the experiment, one is attached to the VGA cable and another one is connected to the USRP. The compromising video signal is first amplified by the coil attached to the VGA cable and subsequently collected by the coil connected to the USRP. The GNU Radio runs on the host computer provides the hardware driver of USRP and records the sampled video signal data to host computer.

3.1 Experimental Setup

The experimental setup is illustrated in Figure 3.7:

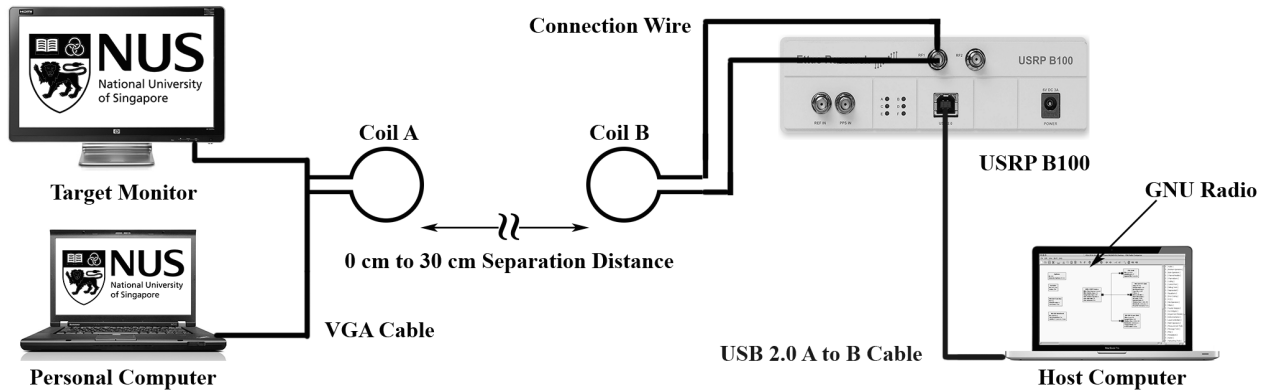


Figure 3.7 An illustration of system setup

The target display (HP Pavilion 2309m) which operates in its native resolution (1920x1080@60 Hz) is connected to a personal computer via VGA cable, a white background NUS logo is chosen as the target image displayed on that screen. Coil A is attached to the red-color control channel of the VGA cable to amplify the electromagnetic emanation of the video signal. Coil B receives the emanation at an adjustable separation distance (from 0 cm to 30 cm) to coil A and connected to the USRP B100's antenna connector with ordinary electrical wires. The USRP B100 samples the received signal at a

rate of 10.667 MHz, converts the sampled data to 32-bit complex binary number with values in range of $[-1.0, 1.0]$ and streams this converted data to host computer via USB 2.0 A to B cable. The host computer runs the GNU Radio, which drives USRP, defines the sampling rate, and provides record function and other signal processing options.

The target image, NUS logo (Figure 3.8), has a background of white color, text of blue color, and coat of arm of orange with blue color. These three colors, white, blue or orange makes the red-color control channel either fully turned on or (almost) fully turned off. As the consequence, if we remove green-color-channel and blue-color-channel to view this image in red-color-channel only, it appears to be purely black and white (i.e. no gray components). A visualized explanation is shown in Figure 3.9A-3.9D:



Figure 3.8: The target image displayed on the monitor

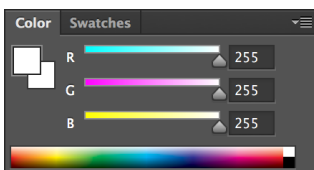


Figure 3.9A: RGB components of white

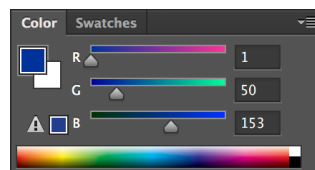


Figure 3.9B: RGB components of blue

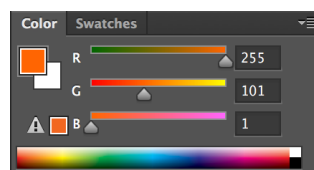


Figure 3.9C: RGB components of orange



Figure 3.9D: view the target image in red-channel only

Figure 3.9A,B, and C shows the RGB components of the three colors are used in the target image. Most computer monitor has an 8-bit color depth, which displaying the image information in such that each color control channel is represent by a value form 0 to 255. A value of 0 indicates the channel is completely turned off; conversely, a value of 255 indicates the channel is completely turned on. In the target image, the white color and orange color both has a red-channel value of 255, which means the red-component turned on and the blue color has a red-channel value of 1, which means the red-channel is (almost) turned off. Figure 3.9D illustrated the case that view the target image on red-channel only.

3.2 GNU Radio Function Blocks and Data Capture

GNU Radio is a free and open-source software development toolkit that provides signal-processing blocks to implement software radios. GNU Radio has filters, channel codes, synchronization elements, equalizers, demodulators, encoders, decoders, and many other function blocks that are typically found in radio systems. In this experiment, GNU Radio runs on the host computer and works together with USRP B100. In this experiment, four main tasks are carried out in GNU Radio function blocks. Firstly, it provides hardware driver to USRP, it will detect the motherboard and daughter boards automatically and initiate the hardware when the signal source is defined to USRP. Secondly, it defines the sampling rate of USRP; this is done by the sampling rate value in the USRP source function block. Thirdly it plots the sampled data in real time, the FFT plot and scope plot functions are allow us to see the spectra (plot in frequency domain) and the waveform (plot in time domain) of the sampled data in real-time. Lastly, it defines the sample data type, receives the converted sample data from USRP and stores it on host computer. In this experiment, the sampled data file is encoded in complex float 32-bit binary data type and mapped to values rang of $[-0.1, 0.1]$. A screen captured in Figure 3.10 shows the UI interface of functions blocks on GNU Radio that used in this experiment to form a radio system.

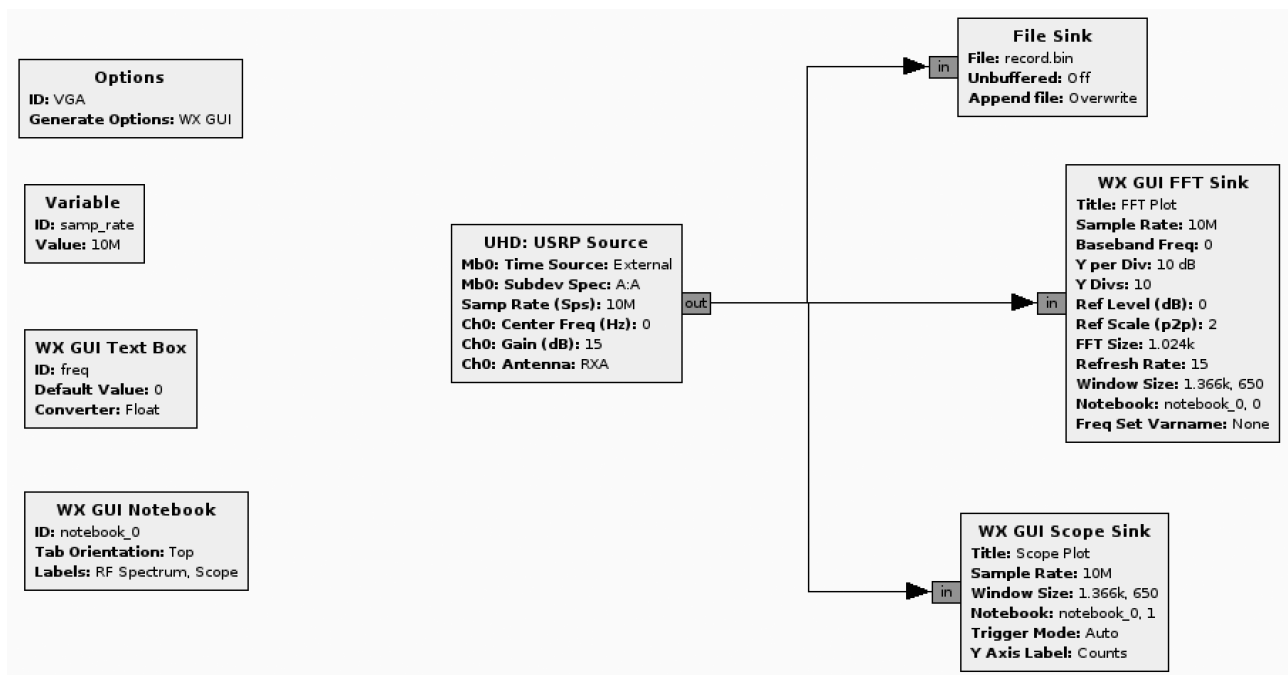


Figure 3.10: GNU Radio function blocks

“UHD: USRP Source” block is the function block that loads the USRP driver, defines USRP sampling rate and sample output type (not shown in Figure 3.10, but it can be set by changing the block properties). The time source option tells where the motherboard should sync its time and clock references when the sink blocks and source blocks reference different devices. Subdevice specification tells the motherboard's subdevice specification. Each motherboard should have its own subdevice specification in the same string format. If this option is left blank, the driver will try to select the first subdevice the system. Sample rate defines the number of samples per second of USRP. The driver will try its best to match the requested sample rate. If the requested rate is not possible, an error will be print at runtime. The center frequency is the overall frequency of the RF chain a zero value gives the largest frequency range that support by the hardware.

“File Sink” block provides the functions to write stream sample data to the file with the type defined in the “UHD: USRP Source” block.

“WX GUI FFT Sink” block plots the sampled signal frequency plectrum in real time. It provides grid view, allows user to zoom, scale and define the center frequency on the plot control window.

“WX GUI Scope Sink” block plots the sampled signal waveform in real time. It provides grid view, allows user to zoom, scale and define the start time on the plot control window.

The sampled data is streamed from USRP to the host computer via USB 2.0 interface, under a sampling rate of 10.667 MHz, with the data type set to be complex float 32-bit binary, 80 MB data are transferred in second. The received data can be opened by a text editor, which shown in Figure 3.11:

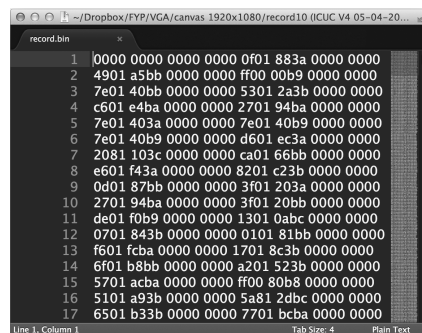


Figure 3.11: The sample of video signal is formed to complex float 32-bit binary numbers in range of $[-1.0, 1.0]$.

Chapter 4: Data processing and Image Reconstruction

After the electromagnetic emanations from VGA cable been intercepted and recorded, the next step is to process with the data and try to reconstruct the image displayed on the target screen. I have separated the image reconstruction procedure into four major steps. The first three steps are meant for sync reconstruction, and the last step is meant for image restoration. First of all, noise reduction should be performed to the sample data. The intercepted signal is mixed with both red-color control channel signal and background noise, since both horizontal sync and vertical sync pulses are not directly detected, therefore a "clean" video signal is needed to restore the image sync information, a noise reduction algorithm is implemented to "clean up" the background noise form the sample data before the it being further processed. Followed by noised deduction, the second step is frame extraction. In order to restore the vertical sync, the frame start point is need to be decided, a algorithm is designed to allocate the frame start point and extract one single frame data out of the large amount of samples. After the single frame data is obtained, the third step is to extract line data form frame. A line sync correction parameter is calculated to correct the cumulate deflection error in deciding the line start point and tries to make the reconstructed image stay in sync. After the line is extracted, the last step is to reconstruction the displayed image on target screen. A drawing function implemented by using open GL framework is implement to draw the frame data line by line, the reconstructed image has a same pixel size as the target screen, with a resolution ratio found in Equation (3.5).

We have already figured out the down-sampling ratio in Equation (3.4) To have a visualized understanding of the relation between the sample data points and the pixel timing, an illustration of mapping sample data points to the pixel timing for a horizontal line is shown in Figure 4.1:

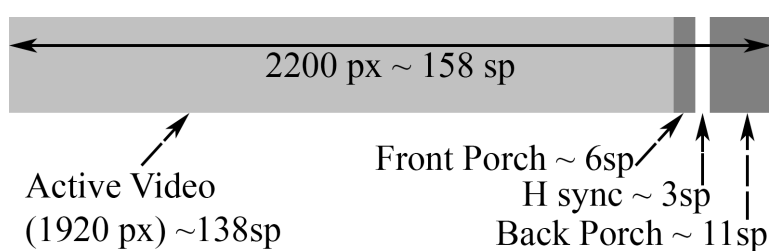


Figure 4.1: Map sample point to pixel timing

Known the sampling frequency and display timing standard, it can be shown from calculation that the video signal information for one line pixel is sampled into 158 data

points. If we choose the active video start point as the start point of the line signal, the first 138 sample data points will represent the signal from addressable (active) video, the following 20 sample data points will represent the signal from blacking area. In the blacking area, the first 6 sample data points represent the front porch, followed by 3 points to represent the horizontal sync signal and the last 11 sample data points represent the back porch signal.

Knowing the relation between the display timing and the sampled data sequence is important. For a sample data from red-color control channel signal, if the pattern of the sample data point sequence is clear, it is possible to infer the horizontal and vertical sync pulses and reconstruct the displayed image with correct sync without detecting the sync pluses from the VGA cable.

4.1 Sync Reconstruction

4.1.1 Noise Reduction

In the sample file, the video signal is mixed with background noise, therefore to identify the frame start point, a noise deduction need to be performed.

To reduce the noise, the first thing is to define the noise level. There are many ways to figure out the noise level the most convenient way is record a noise sample use the existing experimental setting. Reference to Figure 3.7, without attach Coil A to VGA cable, turn on USRP and host computer, run GNU Radio, we can easily get a sample of environment noise. After the sample of environment noise is obtained, we can extract the real part of the complex float 32-bit binary number from the sample file and plot it out.

A sample of noise record in 10 frames' time (0.16666667 second) duration is extracted and plot out as shown in Figure 4.2. According to the static from the plot, the total 1777770 sample data points are fall in range of $[-0.013245, 0.0160222]$, from which 881826 data points are positive and 88153 data points are negative. The summation of the total positive number is 1769.85 and the summation of the total negative number is -1790.73. Theoretically in a "good" noisy environment, the chance of obtaining a positive value and the change of obtaining a negative value should be same. However, in my testing environment, according to the statistic results as shown in Table 4.1, there are more

negative sample values than positive values. This indicates that, if defined in my testing environment, the lower bound of the noise level, in magnitude, should be greater than the upper bound of the noise level.

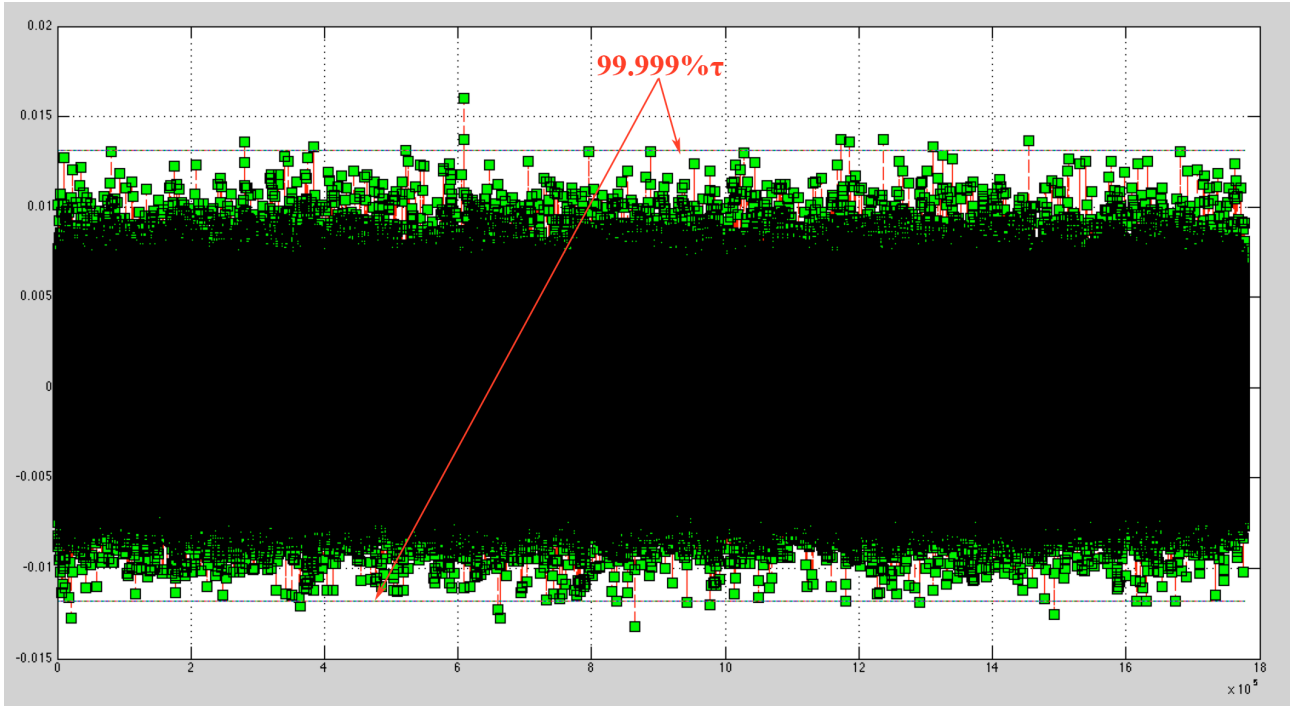


Figure 4.2: A noise record in a duration of 10 frames' time (0.16666667 second)

	Absolute Value	Positive Value	Negative Value
Summation	3560.57	1769.85	-1790.73
Maximum (*)	0.0160222	0.0160222	-0.013245
Minimum (*)	0	3.05185e-05	-3.05185e-05
Average	0.00200283	0.00200702	-0.00201624
Median	0.00173955	0.00173955	-0.00177007
99.999% τ	0.0127873	0.013123	-0.0118412

Note (*): The Maximum and Minimum are indicate the distance from zero

Table 4.1: The detail statics of a sample of the noise record in a duration of 10 frames' time (0.16666667 second)

We choose the 99.999% τ as the effective range of the sample data points do define the noise level, as shown in Figure 4.1, 99.999% τ range drops 32 data points out of consideration, which in numerically equivalent to drop 3.2 data points outliers in one frame time duration, make the 99.999% data points fall in to a rage of $[-0.013245, 0.0160222]$.

Known the noise margins, a quick way to remove it from the sample data is to set all values between $[0.0160222, -0.013245]$ to zero. As the consequence, the data points represent the (addressable) video information are preserved while data points represent the horizontal and vertical blackings are almost completely removed. The start point of a frame thus can be easily obtained form the denoised sample.

An illustration of the noise reduction effect can be shown: In a test environment with noise level of $[-0.035, 0.035]$, a sample of video signal contains information of 3 frames has been recorded and shown in Figure 4.3A. The difference of before and after noise reduction of the sample file is compared in Figure 4.3B and Figure 4.3C:

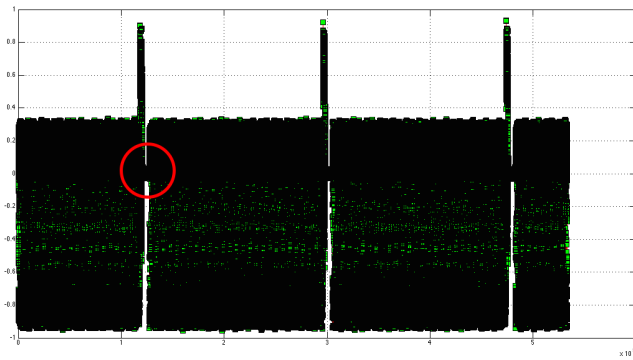


Figure 4.3A: A sample data which contains 3 frames' video information

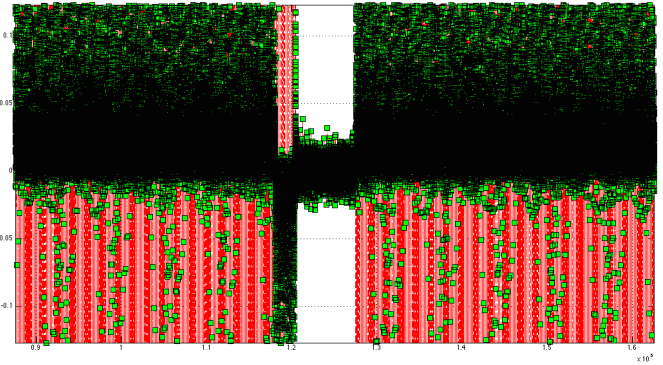


Figure 4.3B: sample data before noise reduction

Figure 4.3B and Figure 4.3C indicate the blacking areas between frames which are the zoomed in views of the circled portion in Figure 4.3A. It can be seen in Figure 4.3C, the noise is almost completely removed so the end of the first frame and the start of the second frame can be easily observed from the plot.

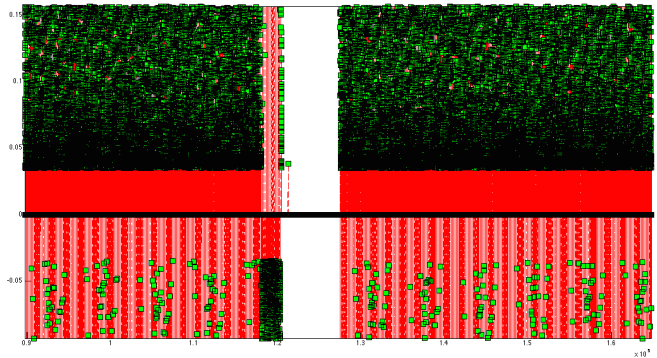


Figure 4.3C: sample data after noise reduction

4.1.2 Frame Extraction

After the noise is removed from the sample file, the video frame data is clearly spaced at the distance of blacking in the data plot and the start point of the frame can be found by two

size-fixed sliding windows which unit are one.

Reference to Figure 3.3, according to the VESA standards, a computer monitor operates in resolution of 1920x1080@60 Hz has a vertical addressable area of 1080 lines and a blanking area of 45 lines. Reference to Figure 4.1, from the mapping between the sample data points to the pixel timing, it is known that one line of video information is represent by 158 data points. If we use window W_1 to indicate the data points that in blanking area and windows W_2 to indicate the data points that in addressable area, it is easy to find that W_1 has a size of 7110 ($158 \times 45 = 7110$) and W_2 has a size of 170640 ($158 \times 1080 = 170640$). W_1 and W_2 together cover the entire data points of one frame. If we link W_1 and W_2 together and slide them from the beginning of the sample data to the end of the sample data at the speed of one sample per time. At the time we find that 99.999% or greater of the data points in W_1 are zero, the start point of W_2 will point to the start point of addressable video of the frame and the end point of W_2 will point to the end point of addressable video of the frame. The illustration of the “sliding-window” is shown in Figure 4.4:

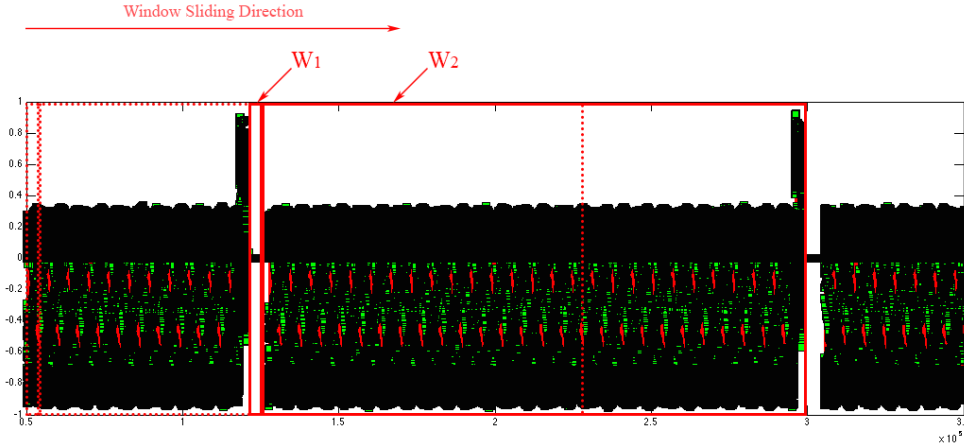


Figure 4.4: An illustration of “Sliding-window”

Known the frame start point, we can extract the frame information out by reading the original sample data. The reason to use the original sample data instead of using the denoised data is because the noise reduction process suppresses the signals in both horizontal blanking and vertical blanking, the line sync pulse in the horizontal blanking may also been eliminated, while we want to preserve it for line information processing.

While applying the “sliding-windows” algorithm, it is possible that the two windows are reached to the end of the sample data before a frame start point could be identified, this

problems can be caused by two reasons.

The first, and the most common reason is the noise level is not well defined. Since the noise level is defined from a separate sample of environment noise other than the sample data contains video information that is being processed, the noise level may be different. It is possible that before the video signal being intercepted, the environment has a lower noise level, when performing the video signal intercepting, the environment noise has increased, as the defined noise level is less than the actual, the noise reduction process will fail to set the 99.999% noise data points to zero, and when the two windows start to slide, W_1 will not detect a status that matches the stopping requirement, which leads to the windows sliding to the end of the sample data. It is also possible that the environment noise level is not changed but the 99.999% τ is not good enough to describe the effective noise level, sample data that contains the video information may have more than 3 outliers per frame, which causes the W_1 fail to detect a stop status and slide to the end of the sample data. To solve the problem caused by the first reason, just increase the noise margin and redo the noise reductions that are described in section 4.1.1.

Increasing noise margin can solve the problem in most cases, however, it won't solve the problem that is caused by another reason, which is the window size of W_1 is set too large. This reason sounds "unreasonable" since the monitor used in the experiment follows the VESA display timing standards, and the window size of W_1 is calculated based on that standards, the size of W_1 should be precisely accurate. Even if there can be errors in hardware design that made the monitor's display timing is not exactly followed the VESA's standards, the improper window size of W_1 which causes one test case fail should cause all test cases fail. About 200 times of video data interceptions are performed with different pictures displayed on the target screen at various distances from the VGA cable during the program testing, increasing noise margin solved the problem in almost all cases that made the frame data of the addressable video failed to allocate, only two failed test cases could not be solved by increasing noise margin. After the noise margin is doubled from the origin, the frame information still could not be extracted. After I reduced the window size W_1 to 98% of its original size, the frame start point can be allocated without increasing noise margin. The physical cause of the problem is not known yet, but according to my guess, it may have two causes. The first possible cause is the monitors' displaying timing is changed due to

unstable power source or the increase/decrease of the room temperature. The second possible cause is the USRP's sampling rate is changed during data interception. Any of the two assumptions are form my personal guess, to prove/disprove them, more data should be collected, and more experiments should be performed.

4.1.3 Line Extraction

The line data can be obtained after the frame data being extracted. Reference to section 4.1.2, by applying the "sliding-windows" algorithm, the position of the first element in W_2 points to the start position of the frame in the original sample data. Reference to Figure 4.1, by mapping the sample data points to the display timing, we have already know that 158 continuous sample data points represent one line information. The data of lines can be simply extracted form the start point of the frame by dreading every continuous 158 data point. This extraction is fast but prefect, the deflection and tearing may occur on the constructed images.

Further adjustments need to be done to eliminate the deflection and tearing before the image being reconstructed. Calculate a deflection correction factor and infer line sync signal form the line data will make the start point of each line dynamically adjustable and the restored image stay in sync as good as possible.

The image deflection is caused by the accumulated errors of the line data length mapping. When we mapping the sample data point to the signal, we count the number of data points to represent a line in an integer, however, 158 is not an accurate value. Numerically, use the float number to represent the total number of data points in one line should be 157.9733338. ($Line\ Time \times Sampling\ Rate = 14.81 \times 10^{-6} \times 10.6666667 \times 10^6 = 157.9733338$) Using 158 data points to represent a line causes one extra data point counted into a line sample per 37.5 lines. The addressable video area of the target screen has 1920 lines that leads total 51.199 extra data points counted in to the last line which is equivalent to 32.41% deflation (pixels are shifted to right) in the reconstructed image. To reduce the deflation is easy, just set back one data points (make the start point of the line left shift one) for every 38 line extraction.

The image tearing is caused by the lost of sample data in one line. The reason behind this this problem is not understood yet. What already known is the line color/contrast and the separation distance of the VGA cable to the receiver have relevance to the sample data losing. This data losing will become more significant if (1) a line is divided into large portions and each portion has different color or contrast or (2) the line is in a pure color (i.e. the extreme case of (1)) or (3) the separation distance of the VGA cable (Coil A in Figure 3.7) to the USRP receiver (Coil B in Figure 3.7) increases.

A trial to fix this problem is to infer the horizontal sync pulse form the line data. If the horizontal sync pulse is found, the end of the current line or the start of the next line can be easily identified. To do this, I need first to find and characterize the sync pulse. A much simpler image has been generated and displayed on the target screen. As shown in Figure 4.5A, a picture of 1920x1080 size with a background and two white vertical lines is used. The two vertical lines each has a width of 75 pixels and separate at a distance of 75 pixels. Before the image signal was intercepted, I made a prediction on the extracted line data form the previous knowledge, the illustration is shown in Figure 4.5B: the first 6 (75 px / 1920 $px \times 158$ $sp = 6$ sp) sample data points will repersent the pixels in the first white segment followed by 6 sample data points represent the pixels in the black segment and another 6 data point represent the pixels in the second white segment. After the second white segment, the rest portion of the addressable video and blacking are exactly same as shown in Figure 4.1. When started to perform the data interception, instead of separating the VGA cable (Coil A in Figure 3.7) from the USRP receiver (Coil B in Figure 3.7) at distance, the red-color control channel was directly connected to the USRP's signal source. I obtained a sample file of the "two-vertical-line" image by directly collecting the voltage signals form the red-color control channel of the VGA cable. After the sample file was process and the line data was extracted out, one extracted line data was plotted and shown in Figure 4.5C. In the active video range, the plotted data is exactly matches the prediction: three 6 sampled data points represent the video signal form three white/black segment on the original image respectively, the rest 120 data points represent the black back ground of the original that is after the second vertical line in the addressable video range. However, according to the plot, for the blacking area, the experiment result is different as predicted. A noticeable difference is on the plot, the inferred horizontal sync pulse is directly followed the active video signal, which makes the front porch merged together with the back porch. Since the real horizontal

sync pulse signal that transmitted in VAG cable is not detected, it can't make the conclusion that the real horizontal sync signal is shifted. To make it easier to get a direct visual comparison between the predicted result and the experiment result, an overlapped figure of Figure 4.5B and Figure 4.5C is generated and shown as Figure 4.5D



Figure 4.5A: Image displayed on target monitor

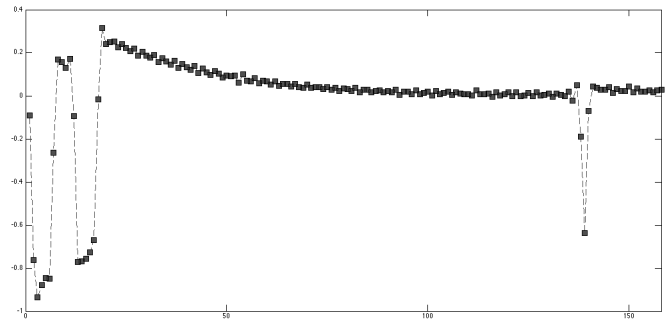


Figure 4.5C: Experiment line data plot

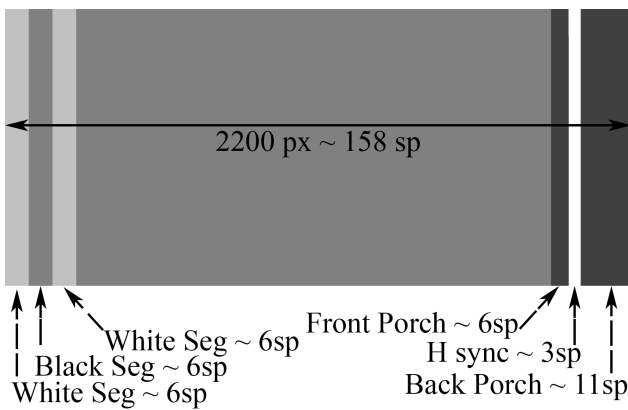


Figure 4.5B: Predicted line data plot

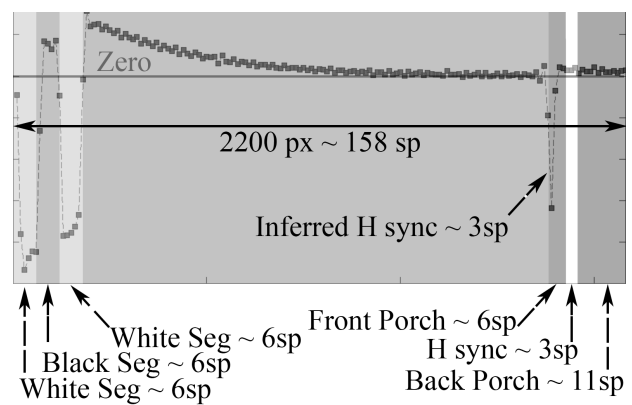


Figure 4.5D: A overlapped figure of Figure 4.5B and Figure 4.5C for visual comparison

Some characteristics of the sampled signal can be observed from Figure 4.5C, B, and D. firstly, the positive sample data points represent the dark pixels which have a red-channel component from 0 to 127 and the negative sample data points represent the bright pixels which have a red-channel component from 128 to 255. Secondly, the signal strength decays with along horizontal direction, at the end of the addressable video range, the signal is almost decreased to zero (fall below noise level). Thirdly, signal from bright color has a stronger pulse strength compared with the dark color. Lastly, the inferred horizontal sync pulse is directly following the addressable video signal, it formed by 3 sample data points under the sampling frequency of 10.667 MHz and it's a negative going pulse.

Known the characters of the sync pulse is important, it helps to identify the length of the

line single in the sample data file. If a line signal sample has a sync-pulse to sync-pulse distance greater than 158, it may subject to addressable-signal-sample losing, in another hand, if a line signal sample has a sync-pulse to sync-pulse distance greater than 158, it may be the mixture of two (or more) lines, and the mixed lines are subject to blacking-signal-sample losing.

If a line is extracted and the sync signal is not found at the end of the addressable video signal, it will be marked as a “bad line” and a dynamic adjustment is needed to restore the sync. A tried method is reallocate the start point of the next line: shift the calculated start point to right or left along the time line until find the sync pulse of next or previous line. However, this method is subjected to certain limitation. The first limitation is the algorithm will not distinguish the difference between the difference between the white pixel and the sync, its possible to be that a line is missing blacking-signal-sample while there is a white color segment in the addressable area, the algorithm therefor will treat the single from a white color segment as a sync pulse, and reallocate the start point of the next line followed the wrong “sync signal”. The second limitation is the algorithm will fail to detect the sync pulse if the separation distance from the VGA able to the receiver is large (8 cm in the experiment) the signal decreases rapidly while the separation distance increases and which make the sync pulse too weak that to be distinguishable from the noise.

4.2 Image Reconstruction

The reconstructed image is generate by using the extracted line data that obtained in section 4.1.3, OpenGL framework is used in the software application to construct the image line by line. Each reconstructed line is joint by 138 line segment that from the addressable signal rage of the line data. Since data is from only red-color control channel, the reconstructed image is in gray scale color with a rage of 0 to 255.

To find a reference contrast level of the image, a pure white and a pure black images have been put on the target screen and been intercepted at a VGA cable to receiver separation distance less than 0.5cm. The 99% τ of the negative values in the intercepted data of the white image is used to define the peak value of white color in the reconstructed image. accordingly the 99% τ of the positive values in the intercepted data of the black image is

used to define the peak value of black color in the reconstructed image. Any values of the line data from any intercepted image is roofed to the peak value of black color and floored to the peak value of white color. The peak value of white color to zero (exclusive) is mapped to 255 to 128 in gray scale and zero (inclusive) to the peak value of black color is mapped to 0 to 127 in gray scale. An example of a reconstructed image of Figure 3.8 use contrast level of contrast level of $[-0.0438856, 0.011536]$ is shown as Figure 4.6

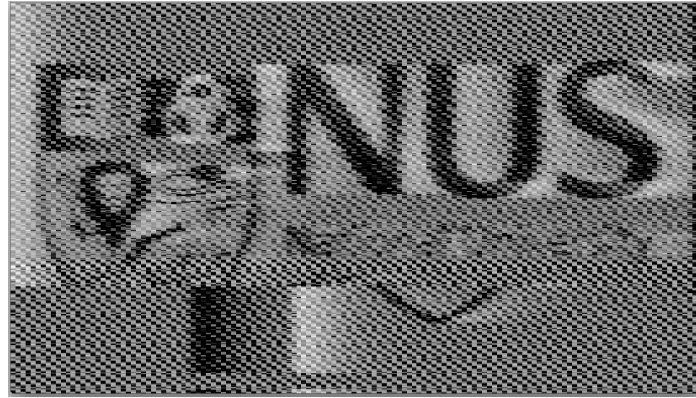


Figure 4.6: A reconstruction of NUS logo (Figure 3.8)

Figure 4.6 is a restored image from the NUS logo (Figure 3.8) that displayed on the target screen. This interception is performed at 4cm away from the VGA cable in an unshielded second-floor living room. From the reconstructed image, we can see the main part of the logo (the coat of arms and the text “NUS”) is full restored and the sync is relatively stable, the segments that joint together to form the line bring the “patchwork effect” to the reconstructed image. We also can “see” the signal strength decay from the restored image: the original image has a purely white color background, but in the reconstructed image, the white color is concentrated around at the start portion of the line which matched the value of the sample data of the line. This result suggests how the color control in VGA cable works: it send a positive/negative pulse when the line start with a dark/bright pixel, if the line is in a pure color, the signal strength will decay along the horizontal displacement from maximum high/low value to zero, if the line contains other color, the signal will first decay along the horizontal displacement until reach to pixels with different color, afterwards, another positive/negative pulse is send to represent the new color, which also decays along the horizontal displacement before reaches the pixels have a different color.

Chapter 5: Experiment Result and Threat Analysis

The VGA cable connected to the target screen was intercepted at a various separation distance from 0 cm to 30 cm. Two groups of experiment, the experimental group and control group, were performed at the same time. Experimental group was performed with the image of Figure 3.8 displayed on the target screen while the control group was performed with the color-inverted image of Figure 3.8 displayed on the target screen. 16 data samples were obtained from the experiment group and 11 data sample were obtained from the control group. All data samples are processed and reconstructed with a same contrast level of $[-0.0438856, 0.011536]$, which references from a purely white and a purely black picture by using the method described in section 4.2. The direct observation of the reconstructed images from the two groups suggests that experiment group has a better quality of restored image. Analysis results of the signal strength decay ration and the noise to signal ratio agrees with the observation. A conjecture that under the testing environment, bright text/image on the dark background is more secure than the dark text/image on the bright background in against of interception is raised and corresponding verification experiment is performed.

5.1 Experiment Result and Discussion

The measurements took place in an unshielded second-floor living room with a noise level of $[-0.013245, 0.0160222]$. Table 5.1 illustrate the quality and readability that an eavesdropper can achieve from signal the source of experiment group and control group at receiver with separation distance ranging from 0 cm (separation distance less than 0.5 cm) to 20 cm. It is clear to see that with the separation distance increases, the quality of the reconstructed image decreases rapidly. This is reflected in three aspects: the image grays, the resolution decreases, and sync stability reduces, with the separation growths. The first problem, image grayish, is caused by the signal strength drop. With the increasing in separation distance, the signal strength drops exponentially, signal collected at far distance is much weaker than the signal collected near to the source, and this decay should reflect on the sampled data. Since all the images are reconstructed using a same reference of contrast levels from the sample data of white/black pictures, the weaker the signal compares to the







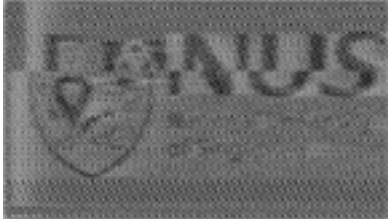



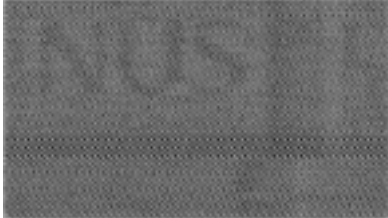


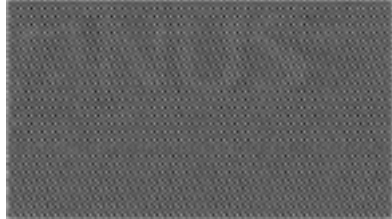
	Experiment Group	Control Group
Original Image		
Separation Distance: 0 cm		
Separation Distance: 4 cm		
Separation Distance: 8 cm		
Separation Distance: 12 cm		
Separation Distance: 16 cm		
Separation Distance: 20 cm		

Table 5.1: Reconstructed images from the sample data

reference, the lower the contrast will be, since the zero is set to gray in the contrast level mapping, the lowering in contrast bringing grayish to the reconstructed image. The second problem, image resolution decrease, is caused by the increasing of the noise to signal ratio. With the signal strength decreases along the separation distance, the noise to signal ratio increase rapidly. When reach to certain distance, the signal will be overwhelmed by the background noise. The reconstructed image losing resolution because the noise reconstructed with the signal, the stronger the noise compare to the signal, the blurrier the reconstructed image will be. The third problem, losing sync, is caused by the disoriented line data, as discussed in section 4.1.3, the increase of the separation distance will lead line data losing, the further, the severe data missing will be. As the consequence, the tearing effect of the reconstructed image will increases with the separation distance growing.

5.2 Threat Analysis

5.2.1 Observation and Analysis

As discussed in the section 5.1, the reconstructed images from both experiment group and control group are subject to be grayish, blurring and desynchrony with the incensement of the signal source to receiver distance.

However, a careful observation shows that for the same separation distance, the quality of the restored images in experiment group and control group are different, images in experiment seems have a better visual quality compared with the images in the control group. The first observation is the image in the experiment group looks more "stable": the images from control group lost horizontal synchronization at the beginning, while the images from experiment group remains a relatively stable line sync until the separation distance is greater than 8 cm. The second observation is the image is more "clear" in the experiment group at a separation distance larger than 12 cm: compare the restored portion of the original image, the text "NUS" looks more clear in the images from experiment group than it in control group and this become very significant when the separation distance increases to 20 cm.

To understand the cause of visual difference in the quality of the reconstructed images, an

examination on the data that used to generate these reconstructed images is necessary. Statistics base on the sample data from the experiment group that used to generate the reconstructed image. The plot of signal strength vs. separation distance and the noise to signal ratio vs. separation distance are shown in the Figure 5.1A,B,C, and D.

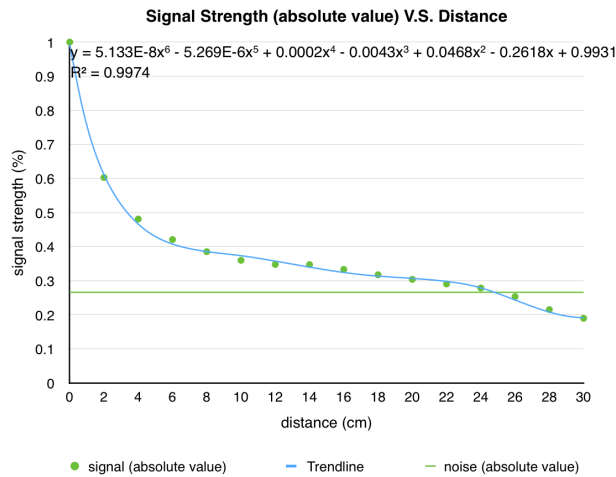


Figure 5.1A: Signal Strength (in absolute value) VS. Separation Distance

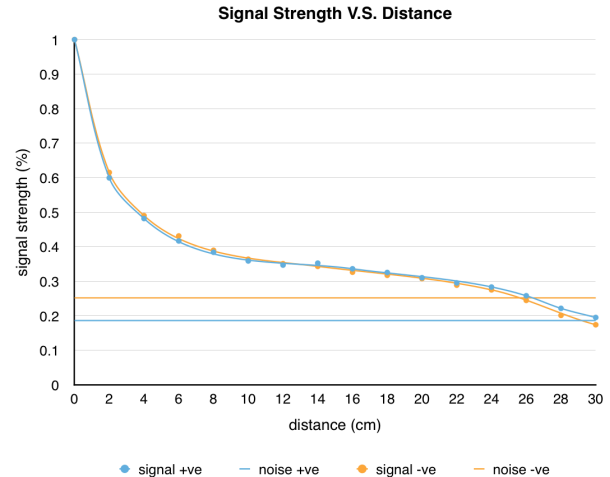


Figure 5.1B: Signal Strength (in both positive and negative values) VS. Separation Distance

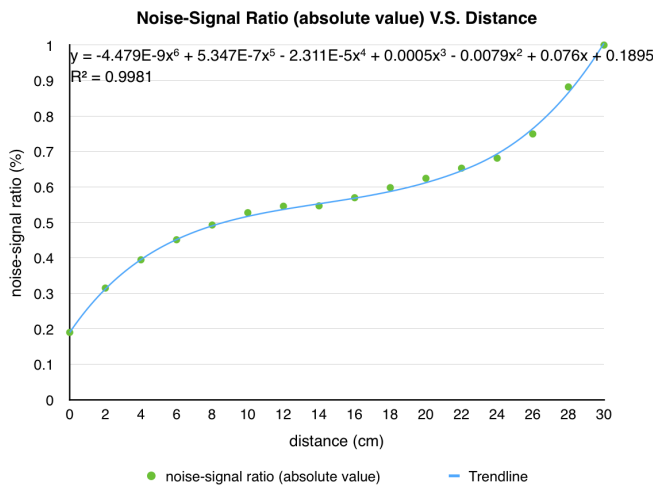


Figure 5.1C: Noise To Signal Ratio (in absolute value) VS. Separation Distance

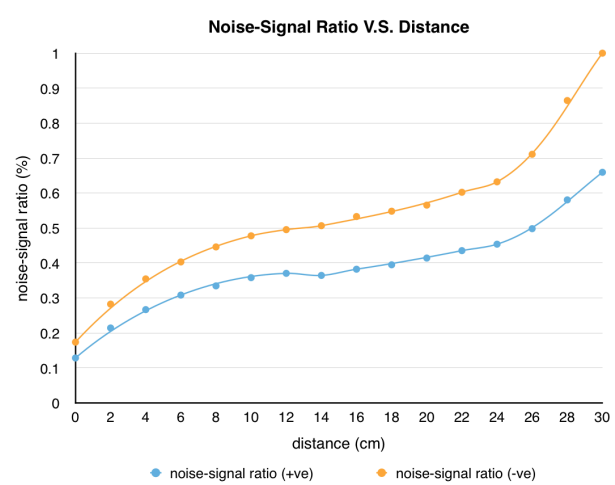


Figure 5.1D: Noise To Signal Ratio (in both positive and negative values) VS. Separation Distance

According to the experiment results, the reconstructed image at the separation distance of 30 cm is totally visual-unrecognizable, the plot in Figure 5.1C and Figure 5.1D are using the normalized result to this this separation distance i.e. normalize the noise to signal ratio to 100% at the separation of 30 cm.

From Figure 5.1A and Figure 5.1C, It's clear to see, in general, the signal strength decays rapidly while noise to signal ration increases vastly with the separation distance increases.

However, according to Figure 5.1B and Figure 5.1D that the signal represent bright color (the "signal -ve" in the plot) and the signal represent dark color (the "signal +ve" in the plot) have different relative noise levels (this is discussed in section 4.1.1, the experiment environment has a noise level of $[-0.013245, 0.0160222]$, which the lower bound is smaller than upper bound compared in magnitude) that causes the noise to signal ratio increases at different rate when the separation distance increases. For example, if we look at the signal strength and the noise to signal ratio at the separation distance of 24 cm: Figure 5.1B shows at the separation distance of 24 cm, the signal represent bright color and the signal represent dark color almost have a same percentage signal strength deduction (at a value about 30% of the strength measured at the separation of 0 cm) while the signal represent white color is closer to its relative noise level and the signal represent black color is further to its relative noise level. The same result also reflected in Figure 5.1D, at the separation distance of 24 cm, the signal represent bright color has a relative noise ratio of more than 60% while the signal represent dark color has a relative noise ratio of less than 50%.

All in all, from what has been discussed above, both the direct observation and the statistic results of the sample data suggest that under the experiment environment, signal represent dark color has a better noise resistivity.

5.2.2 Conjecture and Verification

According to both observation and statics result obtained in section 5.2.1, we may reasonably arise the conjecture that the bright text on the dark background is more secure than the dark text on the bright background in against of display image interception under experimental settings.

To verify the conjecture, another controlled experiment is performed under the same experiment settings. A image of black color text on the white background is used in the experiment group and a image of white color text on black background is used in the control group, the separation distance form the signal source to the receiver is various in rage of 10 cm to 20 cm. The experiment result is listed in the table 5.2.

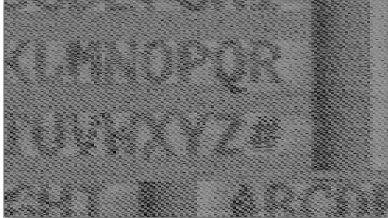

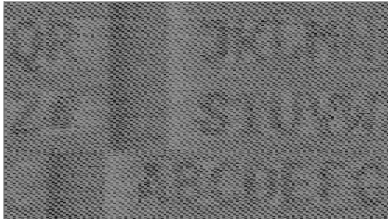
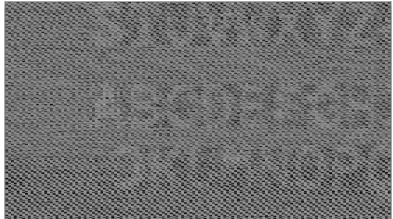
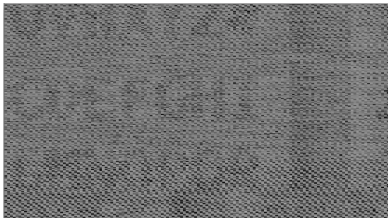
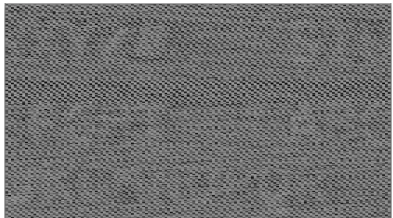

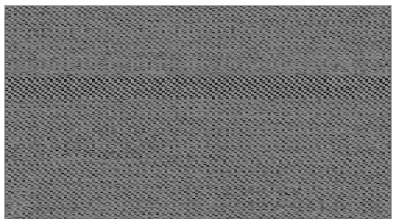
	Experiment Group	Control Group
Original Image	ABCDEFGHI JKLMNOPQR STUVWXYZ#	ABCDEFGHI JKLMNOPQR STUVWXYZ#
Separation Distance: 10 cm		
Separation Distance: 14 cm		
Separation Distance: 18 cm		
Separation Distance: 22 cm		

Table 5.2 : Reconstructed images from the sample data

From the reconstructed image list in table 5.2, it can be seen that at a separation distance above 14 cm, the text in images from the control group is more difficult to recognize compared with it in the images in the experiment group. At the separation distance of 22 cm, the text on the image from the experiment group is still faintly visible while the text on the image from the control group is completely invisible.

The result of the verification experiment supports the conjecture that bright text on the dark background is more secure than the dark text on the bright background in against of display image interception under experimental settings.

Chapter 6: Conclusions and Recommendations

Compromising emanations remain an area with many security questions. In realistic overall threat models of applications that depend on information security, compromising emanations no doubt play a relatively minor role at present. The vast majority of practical vulnerabilities can be exploited using comparatively simple and purely software-based techniques. Nevertheless, compromising emanations are an important field of research. Compared to the large number of minor and highly theoretical vulnerabilities of cryptographic primitives and protocols discussed in much of the current computer security literature, compromising emanations are a risk of practical interest that has so far remained mostly undocumented. Even the most basic concepts of compromising emanations are not even mentioned in textbooks at the moment, except perhaps for the occasional reference to classified military documents on the subject. Entire new classes of vulnerabilities, such as, for example, the diffuse optical emission risks, are still being discovered. Many others, such as RF emanations from devices that are illuminated by an external carrier wave, have been speculated about, but no experimental data has been published so far.

6.1 Summary and Conclusion

This report demonstrated the experiment and discussed the analysis result of the interception of personal computer's display image using emanation of electromagnetic wave form VGA cable. Under normal office/Home environment condition.

In the report, we have firstly studied the computer display monitor timing and identified the video signal synchronization. In addition, we have demonstrated the experiment of intercept the electromagnetic emanations from VGA cable and discussed the algorithms to process the intercepted data and reconstruct the display image on the target screen. Further more, we have analyzed the image reconstruction results by repeating the interception experiments at various distance. Finally, we have made a threat analysis and concluded that the bright text on the dark background is more secure than the dark text on the bright background in against of interception under the experimental settings form the results of analysis and verification experiments.

6.2 Limitations and Recommendations

There limitations in the demonstrated experiment are reflected in both hardware settings and software-algorithm implementations. On the hardware side, the restrictions in the sampling and data transferring rate constraint the maximum resolution in the image reconstruction, the lacking of a proper antenna limit the signal receiving distance in small range. On the software side, the line extraction algorithm is not good enough to restore the sync when the signal sample is collected at a large distance of separation. The image reconstruction speed is also not fast enough to reconstruct the display image in real-time. Some improvement can be made in future works: Firstly, it is possible to transfer the sampled data to a FPGA processing board other than the host computer, the sample data can be read and processed at the same time, therefore, the target display image is restored on real-time. Secondly, it is possible to develop a image filter to improve the quality of the restored image, some trials has already been made (not mentioned in the report), and results shows that certain filtering method can improve the reconstructed image quality under the experiment setting. Finally, it is will be good if a directional antenna is used in the future work, a good antenna suppresses background noises and picks up the video electromagnetic emanation signal at a much further distance.

References

- [1] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. Advances in Cryptology-Crypto '96, Springer.com, Lecture Notes in Computer Science # 1109, pp 104–113.
- [2] Public version of NACSIM 5000 Tempest Fundamentals,
<http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm>
- [3] Dakshi Agrawal Bruce Archambeault Josyula R. Rao Pankaj Rohatgi The EM Side–Channel(s):Attacks and Assessment Methodologies, Springer.com, Lecture Notes in Computer Science Volume 2523, 2003, pp 29- 45
- [4] K. Gandolfi, C. Mourtel and F. Olivier. Electromagnetic Attacks: Concrete Results. In the Proceedings
of the Workshop on Cryptographic Hardware and Embedded Systems 2001 (CHES 2001), LNCS 2162 Paris, France, May 2001, pp 251–261
- [5] Jean–Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In Smart Card Programming and Security (E-smart 2001), Cannes, France, LNCS 2140, pp.200-210, September 2001.
- [6] L. Goubin and J. Patarin. DES and Differential Power Analysis. Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES '99, LNCS 1717, August 12–13, 1999, Worcester, MA, pages 158–172.
- [7] Van Eck W. Electromagnetic radiation from video display units: an eavesdropping risk? Computers and Security, 1985, 4(4): 269–286
- [8] Markus G. Kuhn Electromagnetic Eavesdropping Risks of Flat-Panel Displays, (4th Workshop on Privacy Enhancing Technologies proceedings, Springer-Verlag, LNCS 3424).
- [9] TCO'99 – Mandatory and recommended requirements for CRT-type Visual Display Units (VDUs). Swedish Confederation of Professional Employees (TCO), 1999.
<http://www.tcodevelopment.com/>
- [10] VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1.0, Revision 12p, Draft 3 10/17/08, Page 86 of 100

Appendix – Data Used in Statistics

Table 1: Statistics for noise

distance	net sum	Sum (abs)	Mean (abs)	99.999% τ (abs)	p	n	p/n ratio	Mean (+ve)	99.999% τ (+ve)	Mean (-ve)	99.999% τ (-ve)
0	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
2	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
4	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
6	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
8	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
10	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
12	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
14	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
16	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
18	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
20	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
22	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
24	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
26	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
28	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412
30	-20.8827	3560.57	0.00200283	0.0127873	881826	888153	0.992876	0.00200702	0.013123	-0.00201624	-0.0118412

*NOTE: The noise is assumed to be constant at various separation distance

Table 2: Statistics for “NUS logo” (Figure 3.8)

distance	net sum	Sum (abs)	Mean (abs)	99.999% τ (abs)	p	n	p/n ratio	Mean (+ve)	99.999% τ (+ve)	Mean (-ve)	99.999% τ (-ve)
0	-17.4088	18507.1	0.0104103	0.0480972	856148	918509	0.932106	0.0107982	0.0484329	-0.010084	-0.0470901
2	-21.779	10575.2	0.00594856	0.0289926	873448	901111	0.969301	0.00604123	0.0290231	-0.00587994	-0.0289621
4	-29.4866	8788.75	0.00494369	0.023133	885011	889606	0.994835	0.00494868	0.0233161	-0.00495626	-0.023072
6	-25.6691	7314.05	0.00411417	0.0202338	881784	891545	0.989052	0.00413275	0.0201727	-0.00411629	-0.0202948
8	-24.4506	6897.07	0.00387962	0.0185247	882052	890955	0.990007	0.00389581	0.0185858	-0.00388433	-0.0183416
10	-23.7085	7138.96	0.00401569	0.017304	882916	890583	0.991391	0.00402941	0.017365	-0.00402134	-0.0171209
12	-17.8816	7161.25	0.00402822	0.0167241	884894	889033	0.995344	0.00403628	0.0167852	-0.00403761	-0.0165105
14	-11.6034	6242.95	0.00351167	0.0166936	883213	889448	0.99299	0.00352766	0.0170598	-0.00351597	-0.0161443
16	-23.4843	6285.88	0.00353582	0.0160222	883016	889866	0.992302	0.00354603	0.0162664	-0.00354512	-0.0153508
18	-21.3431	6375.14	0.00358603	0.0152593	883908	889426	0.993796	0.00359415	0.0157475	-0.00359585	-0.0149235
20	-21.7474	5405.65	0.00304069	0.0146184	881932	889532	0.991456	0.00305233	0.0150151	-0.0030507	-0.0144658
22	-20.2502	3760.49	0.00211529	0.0139775	876978	889032	0.986441	0.00213246	0.0142827	-0.00212633	-0.0135807
24	-18.1679	5183.39	0.00291567	0.0133976	883306	888589	0.994055	0.0029238	0.0137028	-0.00292687	-0.0129398
26	-17.9919	4716.63	0.00265311	0.0121769	883149	888813	0.993627	0.00266016	0.0124821	-0.00266345	-0.0115055
28	-13.7995	3430.15	0.00192947	0.0103458	880879	888800	0.991088	0.00193917	0.010712	-0.00193742	-0.00946074
30	-25.515	2522.85	0.00141911	0.00912503	874203	891692	0.980387	0.00142835	0.00943022	-0.00142895	-0.00817896

Table 3: Statistics for Signal Strength (in absolute value) Decay

distance	signal_ABS	noise_ABS	nsr_ABS
0	1	0.265863709321956	0.265863709321956
2	0.602791846510816	0.265863709321956	0.441053924104771
4	0.480963548813652	0.265863709321956	0.55277309471318
6	0.420685611636436	0.265863709321956	0.631977186687621
8	0.385151318579876	0.265863709321956	0.690283783273142
10	0.359771462787855	0.265863709321956	0.738979426722143
12	0.347714627878546	0.265863709321956	0.764603177450504
14	0.34708049533029	0.265863709321956	0.766000143767669
16	0.333121262776212	0.265863709321956	0.798098887793185
18	0.317259632577364	0.265863709321956	0.838000432523116
20	0.303934532571543	0.265863709321956	0.874740053631038
22	0.290609432565721	0.265863709321956	0.914848864246109
24	0.278552597656412	0.265863709321956	0.954447065145997
26	0.253172741864391	0.265863709321956	1.05012770081055
28	0.215101918614805	0.265863709321956	1.2359894836552
30	0.189720607436608	0.265863709321956	1.40134333804929

Table 4: Statistics for Signal Strength (+ve and -ve) Decay

distance	signal (+ve)	noise (+ve)	signal (-ve)	noise (-ve)	nsr (+ve)	nsr (-ve)
0	1	0.185866162878998	1	0.251458374477863	0.185866162878998	0.251458374477863
2	0.599243489446224	0.185866162878998	0.615035856793678	0.251458374477863	0.310168013758083	0.408851568083807
4	0.481410363616467	0.185866162878998	0.489954364080773	0.251458374477863	0.386086750361434	0.513228155339806
6	0.416508200004542	0.185866162878998	0.430978061206071	0.251458374477863	0.446248508137346	0.583459802510989
8	0.383743281942646	0.185866162878998	0.389500128477111	0.251458374477863	0.484350271718314	0.645592532821565
10	0.358537275281885	0.185866162878998	0.363577482315816	0.251458374477863	0.518401225459385	0.691622519844168
12	0.346566073887791	0.185866162878998	0.350615097440863	0.251458374477863	0.536308014209079	0.717192089882198
14	0.352235773616694	0.185866162878998	0.342838515951336	0.251458374477863	0.527675428791793	0.733460106663033
16	0.335854346941852	0.185866162878998	0.32598784033162	0.251458374477863	0.553413003498144	0.771373478906637
18	0.325140555283702	0.185866162878998	0.316913746201431	0.251458374477863	0.57164866042878	0.793459979227394
20	0.310018603057013	0.185866162878998	0.307194081133826	0.251458374477863	0.599532289502049	0.818565167498516
22	0.294896650830324	0.185866162878998	0.288398198347423	0.251458374477863	0.630275597758282	0.871913818875318
24	0.28292338472402	0.185866162878998	0.274788118946445	0.251458374477863	0.656948746249104	0.915099151455202
26	0.257719442775469	0.185866162878998	0.244329487514361	0.251458374477863	0.721195734700268	1.02917734996306
28	0.22117197194469	0.185866162878998	0.200907197054158	0.251458374477863	0.840369424953533	1.25161456714803
30	0.194706903778217	0.185866162878998	0.173687462969924	0.251458374477863	0.954594620284809	1.44776352983753

Table 5: Statistics for Noise-Signal Ratio

distance	nsr (abs)	nsr (+ve)	nsr (-ve)	nsr (abs) normalized	nsr(+ve) normalized	nsr (-ve) normalized
0	0.265863709321956	0.185866162878998	0.251458374477863	0.189720607436609	0.128381575477216	0.173687462969924
2	0.441053924104771	0.310168013758083	0.408851568083807	0.314736518973809	0.214239416427965	0.282402173875515
4	0.55277309471318	0.386086750361434	0.513228155339806	0.394459430251159	0.266678046797298	0.354497226074897
6	0.631977186687621	0.446248508137346	0.583459802510989	0.450979549071359	0.308233008319684	0.40300766698859
8	0.690283783273142	0.484350271718314	0.645592532821565	0.492587194394513	0.334550678847856	0.445924019714749
10	0.738979426722143	0.518401225459385	0.691622519844168	0.527336453999077	0.358070371835904	0.477717876980768
12	0.764603177450504	0.536308014209079	0.717192089882198	0.545621588007728	0.370438958542673	0.495379304079225
14	0.766000143767669	0.527675428791793	0.733460106663033	0.546618464561271	0.364476254524114	0.506615957334789
16	0.798098887793185	0.553413003498144	0.771373478906637	0.569524160227687	0.382253725896969	0.532803502097612
18	0.838000432523116	0.57164866042878	0.793459979227394	0.597997942238507	0.39484946860965	0.54805910141723
20	0.874740053631038	0.599532289502049	0.818565167498516	0.62421537240738	0.414109263803136	0.565399770493166
22	0.914848864246109	0.630275597758282	0.871913818875318	0.652837059560011	0.435344298132038	0.602248779517996
24	0.954447065145997	0.656948746249104	0.915099151455202	0.681094375111966	0.453767989529912	0.63207777554522
26	1.05012770081055	0.721195734700268	1.02917734996306	0.749372171899256	0.498144703770236	0.710873929859634
28	1.2359894836552	0.840369424953533	1.25161456714803	0.882003325020785	0.580460418869538	0.864515883535544
30	1.40134333804929	0.954594620284809	1.44776352983753	1	0.659358106908478	1