TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.1, January 2014, pp. 269 ~ 274
DOI: http://dx.doi.org/10.11591/telkomnika.v12i1.3966

Analysis of the Relationship between Hamming Distance and the Electromagnetic Information Leakage

Zhang Jiemin*[1], Liu Jinming[2], Sun Haimeng[3], Mao Jian[4]
[124]Computer Engineering College, Jimei University (JMU)
No.183 Yinjiang Rd, 361021 Jimei, Xiamen, Fujian, China, Ph./Fax: +86-592-6182451/6181601
[3]Chengyi College, Jimei University (JMU)
No.185 Yinjiang Rd, 361021 Jimei, Xiamen, Fujian, China, Ph./Fax: +86-592-6182996/6182998
Corresponding author, e-mail: zhangjm@jmu.edu.cn[1], liu_jinming@126.com[2], haimes@163.com[3], myjeans@sina.com[4]

Abstract

Electromagnetic information leak as a potential data security risk is more and more serious. Discussing the relationship between compromising emanations and Hamming distance is directed to preventing or reducing the electromagnetic information leakage. The paper presents the model of electromagnetic information leak, then the hierarchical protection strategy based on the model is proposed, that is anti-radiation, anti-intercept and anti-reconstruction. Analyzing the causes of electromagnetic information leak through the touch screen case, the paper describes the electromagnetic radiation intensity is correlated to the transition's Hamming distance. The paper presents the anti-intercept method, which is reducing the Hamming distance of the sensitive data or keep Hamming distance constant in order to reducing or preventing the electromagnetic information leakage. The anti-intercept method is available showed as the touch screen case.

Keywords*: Electromagnetic information leakage*, *hierarchical protection strategy*, *Hamming distance*, *data security*, *anti-intercept*

1. Introduction

The safety of the information is more and more important, however the attack is becoming more and more serious. Electromagnetic radiation as a potential computer security risk is ignored while the people pay more attention to the network attack or virus.

As early as 1985, the concept of electromagnetic information leakage was brought firstly to the attention of the broader public by Van Eck [1], [2], who showed that the screen content of a cathode-ray tube (CRT) display can be reconstructed at a distance using a TV set whose sync pulse generators are replaced with manually controlled oscillators.

In fact, the compromising emanations was discovered not only from video displays, but also from CPU, mainbard, keyboard, printer, lines as power line, data wire, control line and so on [3], even though the different components call for the different approaches to intercept and reconstruct the original data [4].

With the wide application of computer technology, network technology and modern communications technology in the various business, meanwhile with the advancement of intercept techniques and reconstruct techniques, electromagnetic information leakage is very grave. It has become an major way to obtain confidential information using electromagnetic information leakage both here and abroad. All these developments make it necessary to reevaluate the emission-security risks identified now.

It is presented in the paper that electromagnetic information leak is correlated to the transition's Hamming distance. Study on the relationship between compromising emanations and Hamming distance is directed to preventing or reducing the electromagnetic information leakage.

2. The Model of Electromagnetic Information Leak

All electrical and electronic equipment produces electromagnetic radiation. The electromagnetic signals propagate along electrically conductive pathways called conducted

Received June 22, 2013; Revised August 14, 2013; Accepted September 16, 2013

emissions or through space called radiated emissions. Both the conducted emissions and the radiated emissions will result in electromagnetic interference (EMI) and electromagnetic leak. Electromagnetic leak is more severe rather than merely EMI. If these emissions are intercepted and analyzed they could reveal confidential data that the signals contain. A receiving device can intercept these signals without being detected even when located some distance away access to the original equipment is not required. Electromagnetic radiation of the computer results in electromagnetic information leak.

According to the electromagnetic radiation theory and information theory, it may be considered that electromagnetic information leak system is composed of three parts that are leak source (information source), electromagnetic radiation (information channel), interception equipment (information sink), showed as Figure1.

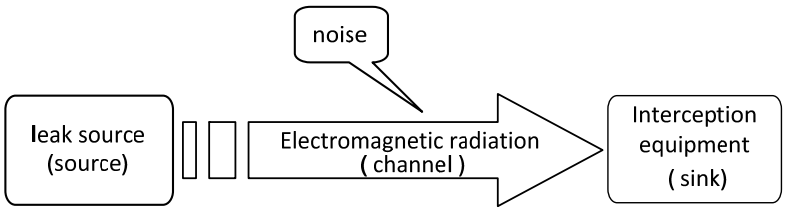

Figure 1. Model of electromagnetic information leak

The research of electromagnetic information leak is based upon the model in this paper. According the model, The three aspects of the source, channel and sink should be considered to protect from electromagnetic information leakage. Thus the hierarchical protection strategy is taken into account, that is anti-radiation, anti-intercept and anti-reconstruction, showed as Figure 2.

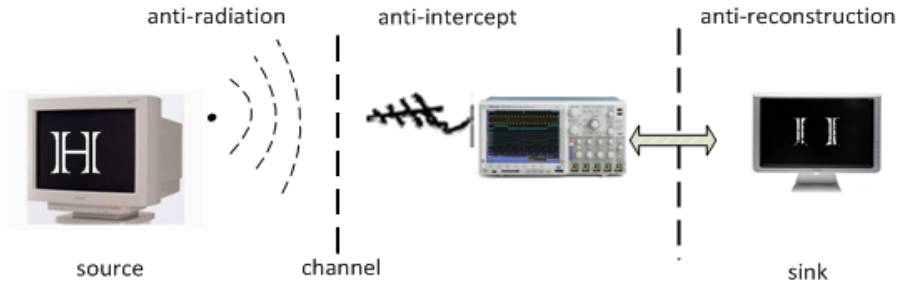

Figure 2. Hierarchical protection model

anti-radiation: try to inhibit or block electromagnetic radiation in order to hold the leakage as less as possible.

anti-intercept: try to make intercept more difficult in order to keep from capture as far as possible.

anti-reconstruction: try to make reconstruction more difficult in order to keep from reproduction as far as possible.

The Hamming distance of data processed in a computer have a certain relationship with electromagnetic radiation intensity. It is possible to make intercept more difficult by adjusting the Hamming distance of data so that prevent or reduce the electromagnetic information leakage.

3. Analyzing the Causes of Electromagnetic Information Leak

The construction of information equipment results in the cause why electromagnetic radiation is associated with information leak. Most chips made for digital information devices are

designed in CMOS technology, so these logic family has become dominant in very large scale integrated circuits (VLSI), including inverter, NOR gate, NAND gate and so on. CMOS inverters are the basic building-block of all digital CMOS logic. The inverter can be looked upon as a push-pull switch: A "In" grounded cuts off the one transistor, pulling "Out" high. A high "In" does the inverse, cuts off the another transistor , pulling "Out" to ground, showed as Figure 3.

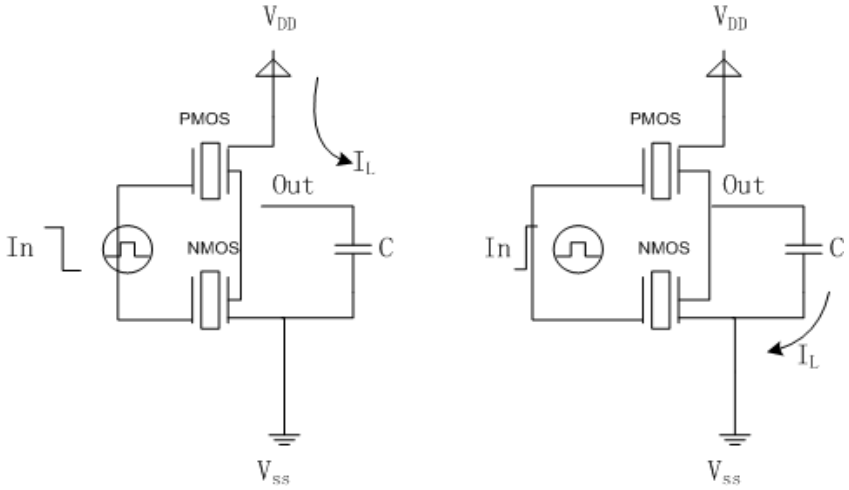

Figure 3. Elementary CMOS gate

There are three kinds of current while CMOS gate works that are the static current, dynamic short-circuit current and dynamic current as the capacitor C charging and discharging. Power consumption or electromagnetic radiation intensity is mainly caused by dynamic current because of static current only contributes less 15% [5], [6].

In particular, the dynamic short-circuit current results in the impulse. During a transition from "0" to "1" or vice-versa, the device's n and p transistors are on for a short period of time. This results in a short current pulse from V_{dd} to V_{ss}. This sudden current pulse causes a sudden variation of the electromagnetic field surrounding the chip which can be monitored by some inductive equipments.

According to above analysis, in the case of inverse no matter "0→1" or " 1→0" happened, electromagnetic information leak is there. Meanwhile the data "1" has the higher power consumption than the data "0". Thus the power curve is correlated to the transition's Hamming distance. This explains why the electromagnetic radiation curve is correlated to the transition's Hamming distance and why electromagnetic information leakage when data flips.

Hamming distance is the number of different code value of corresponds to bits between any two codeword in a data encoding set, as in (1).

$$H(x, y) = \sum x[i] \square y[i] \quad (1)$$

Here is i=0,1,..n-1; x, y is n bits of code; $\oplus$ is exclusive or operator; H (x, y) is the difference for x and y take 0 or 1 values, if x and y are binary codes.

The more the number of bits changed is, the more the power consumption is, and the higher the electromagnetic radiation intensity is. The power consumption model can be build based on Hamming distance, and then the electromagnetic radiation model can be build based on Hamming distance [7], [8], as in (2).

$$C = a* H(D \oplus R) + b \quad (2)$$

In (2), C is the electromagnetic radiation; D is the original data, R is the result data; H is Hamming weight; $\oplus$ is operator XOR. Then H(D $\oplus$ R)is the Hamming distance of D and R.

Let a = 1 and b = 0, then C is expressed simply as in (3).

$$C = H(D \oplus R) \quad (3)$$

The formula represents a series of changes in the relationship "Hamming distance of data→power consumption→electromagnetic radiation".

Based on the analysis above, the power consumption is different while the information equipments process the data of "0" or "1", leading to changes in intensity of electromagnetic radiation and in electromagnetic signal. In particular, a bit of data transitions from "0" to "1" or vice-versa results in a short current pulse from V_{dd} to V_{ss}, then electromagnetic information leakage can be captured through the method of DPA (Differential Power Analysis) [5]-[8] or EA (Electromagnetic Analysis) [7] etc.

If reducing the Hamming distance of the sensitive data or keeping Hamming distance constant, it will reduce the variation of electromagnetic wave radiated or keep the changes of electromagnetic signal constant, then the interception is more difficult. So intercepting the electromagnetic wave with information becomes more hardly.

4. Adjusting the Hamming Distance to Anti-Intercept

Touch screen monitors are widely used as an input device in an automatic teller machine (ATM), a cash dispenser (CD), a door and gate access control terminal, mobile [9], and so on. In the operation, the operator inputs often the certificate code by touching the numeric and character button image. The touched button image then changes the color at one time to inform the operator the input button key. The change of color of the touched button image is widely general in the flow of input button key operations on touch screen monitors.

The standard color scheme of the touch screen monitors is showed as Figure 4.

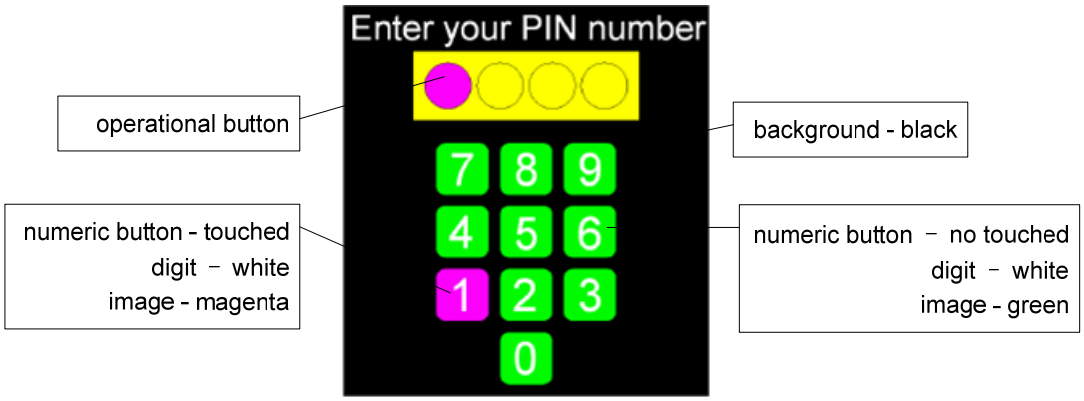

Figure 4. Standard color scheme of a touch screen monitor

The image that touch screen monitors display can be reconstructed on a personal computer with intercepting electromagnetic radiation [10]-[12]. If the change of color of the touched button image can be distinguished in the reconstructed display image, the information of input button key operations on touch screen monitors leaks from the electromagnetic radiation [13].

The color change means that the data changes, it means the Hamming distance of data is not 0 before and after touch the numeric button. There are changes in electromagnetic radiation. Table 1 shows a touch screen standard color scheme and data encoding. The calculations for the standard color scheme are summarized in Table 2 before and after touch the numeric button.

Table 1. Standard color scheme and data encoding

Numeric button	No touched	Touched
background color	black [00H : 00H : 00H]	black [00H : 00H : 00H]
image color	green [00H: FFH : 00H]	magenta [FFH : 00H : FFH]
digit color	white [FFH : FFH: FFH]	white [FFH : FFH: FFH]

Table 2. Hamming distance for standard color scheme before and after touch the numeric button

Numeric button	No touched	Touched
color change of image	[00H: 00H : 00H] →[00H :FFH : 00H]	[00H :00H :00H] →[FFH :00H :FFH]
Hamming distance for image	8	16
color change of digit edge	[00H :FFH :00H] → [FFH :FFH:FFH]	[FFH :00H :FFH]→ [FFH :FFH:FFH]
Hamming distance for digit edge	16	8

The reason for the information leak of input button key operations on touch screen monitors is investigated in Table 2.

Select cyan color ([00H : FFH : FFH]) as a different image color for touch button, called anti-intercept color scheme showed as Figure 5, so that the Hamming distance of data is 0 before and after touch the numeric button.

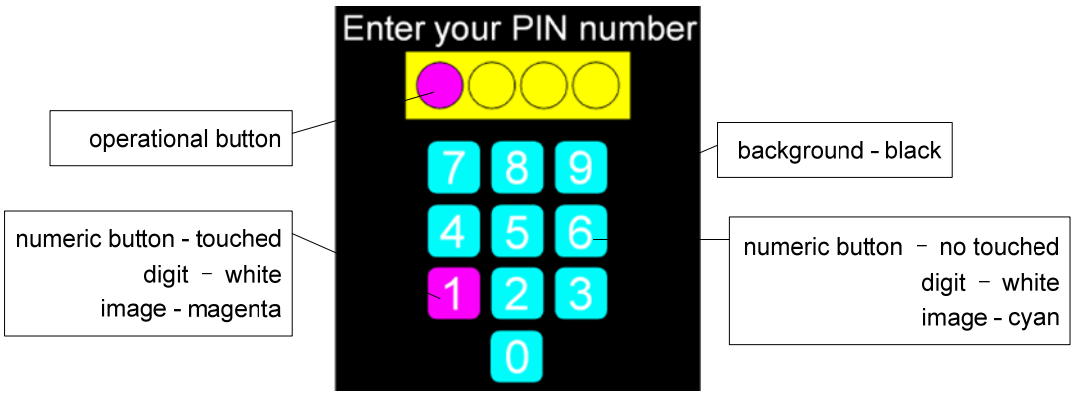

Figure 5. Anti-intercept color scheme of a touch screen monitor

The calculations for the anti-intercept color scheme are summarized in Table 3 before and after touch the numeric button.

Table 3. Hamming distance for anti-intercept color scheme before and after touch the numeric button

Numeric button	No touched	Touched
color change of image	[00H : 00H : 00H] →[00H : FFH : FFH]	[00H:00H :00H] →[FFH :00H :FFH]
Hamming distance for image	16	16
color change of digit edge	[00H : FFH : FFH] → [FFH :FFH:FFH]	[FFH:00H :FFH]→ [FFH :FFH:FFH]
Hamming distance for digit edge	8	8

Compare the anti-intercept color scheme with the standard color scheme, showed as Table 4, Either the Hamming distance for image or the Hamming distance for digit is constant before and after touch the numeric button for the anti-intercept color scheme, it is 16 or 8 respectively.

Table 4. Hamming distance for anti-intercept color scheme and standard color scheme

Numeric button	Standard Image	Standard Digit edge	Anti-intercept Image	Anti-intercept Digit edge
no touched	8	16	16	8
touched	16	8	16	8
difference	-8	8	0	0

5. Conclusion

Because that the Hamming distance is constant, the electromagnetic radiation variation maintains constant before and after touch a numeric button. It result in that can't determine whether a numeric button is touched thereby protecting the password security. The anti-intercept color scheme used in practical application, it is really difficult to capture and reconstruct original data using electromagnetic radiation.

So adjusting the Hamming distance of data to make the electromagnetic radiation variation is constant, can effectively prevent the electromagnetic information leakage, protect the confidential data security. Adjusting the Hamming distance of data to make the electromagnetic radiation variation is less, can effectively attenuate the electromagnetic information leakage, protect the confidential data from attack.

References

[1] Markus G Kuhn. Compromising emanations: eavesdropping risks of computer displays. *University of Cambridge Computer Laboratory Technical Report.* 2003; UCAM-CL-TR: 577-581.

[2] Van Eck W. Electromagnetic radiation from video display units: An eavesdropping risk?. *Computers and Security*. 1985; 4(4): 269-286.

[3] CHU Jie, DING Guoliang, DENG Gaoming, ZHAO Qiang. Design and Realization of Differential Power Analysis for DES, Department of Computer Engineering. *Journal of Chinese Computer Systems*. 2007; 1(28):11-14.

[4] Timo Kasper, David Oswald, and Christof Paar. EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. *Horst Görtz Institute for IT Security Ruhr University Bochum, Germany, HY Youm and M Yung (Eds.)*: WISA 2009: LNCS 5932: 79-93.

[5] DING Guoliang, CHANG Xiaolong, CHENG Jiawen, WU Cuixi. The Electromagnetic Information Leakage Evaluation on Basic CMOS Gate. *Microelectronics & Computer*. 2011; 28(5): 67-70.

[6] ZHANG Jingjing, LI Renfa, LI Lang, ZENG Qingguang. Research and realization of simulation of DES differential power analysis attack. *Computer Englneering and Applications*. 2010; 46(33): 82-84.

[7] Karine Gandol, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results, Hardware and Embedded Systems. *Computer Science*. 2001; Lecture Notes (2162): 251-262.

[8] LU Chang, PAN Xiong. Research on the selection function in diferential power analysis. *Information Technology.* 2012; 3: 108-110.

[9] Emy Setyaningsih, Catur Iswahyudi. Image Encryption on Mobile Phone Using Super Encryption Algorithm. *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2012; 10(4): 837-845.

[10] Hidenori Sekiguchi, Shinji Seto. Measurement of Radiated Computer RGB signals. *Progress In Electromagnetics Research C.* 2009; 7(C): 1-12.

[11] Hidenori Sekiguchi, Shinji Seto. Measurement of Computer RGB signals in Conducted Emission on Power Leads. *Progress In Electromagnetics Research*. 2009; 7(C): 51-64.

[12] Hidenori Sekiguchi. Information leakage of input operation on touch screen monitors caused by electromagnetic noise. *IEEE 978-1-4244-6307-72010*.

[13] Deris Stiawan, Mohd Yazid Idris, Abdul Hanan Abdullah. Attack and Vulnerability Penetration Testing: FreeBSD. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(2): 399-408.