The Search and Reconstruction of Compromising Emanations of Laser Printers in Three Media

Cihan Ulaş*‡, Ulaş Aşık*, Cantürk Karadeniz*

* TEMPEST Test Laboratory, TÜBİTAK BİLGEM, Gebze Kocaeli.

‡ Cihan Ulaş; TÜBİTAK BİLGEM, Gebze Kocaeli

Tel: +90 262 648 1882, Fax: +90 262 648 1100, e-mail: cihan.ulas@tubitak.gov.tr

Abstract- In this paper, the emissions of a laser printer, which may process classified information, are investigated in the media of electromagnetic radiation (ER), Power Line Conductors (PLC), and Signal Line Conductors (SLC). First, the candidate frequency points of Compromising Emanations (CE) are examined in the frequency domain. Second, the emitted signal is AM-demodulated with the proper bandwidth, and then sampled by a high storage oscilloscope in these frequency points. Third, the collected data is converted to 2D image by applying signal and image processing techniques. In addition, this study introduces some practical measurement methods to reveal the possible CEs of laser printers. Finally, the procedure of the image reconstruction of CEs of the laser printer data is explained in detail.

Keywords- Compromising Emanations; Information Leakages; Printers; TEMPEST; Electromagnetic Radiation; Power and Signal Line Conductors.

1. Introduction

Electronic equipment naturally emits electromagnetic (EM) waves during its regular operation. Unintentional intelligence bearing signals may disclose the processed information which might be transmitted, received, or processed by any information processing equipment. If the information is classified as confidential, a serious information security weakness is occurred. There have been many studies on the subject of Compromising Emanations (CE) and information leakages caused by the information technology equipment such as computers displays, keyboards, and printers.

Harold Joseph Highland mentioned about the computer security risk of electromagnetic radiation in 1967 [1]; however, the first detailed open publication about compromising emanation risks was released by a Swedish government committee in 1984 [2]. Wim van Eck reconstructed Cathode Ray Tubes (CRT) screen information and displayed on a television monitor by using commercial equipment in 1985 [3]. Moreover, information leakages of other computer units and peripherals, such as keyboard and printers have been studied in the literature.

Keyboards are mostly used as input devices for confidential data such as passwords and text documents entry. Measurements and analyses on CE of keyboards were started with Han in early 1990s [4]. Vuagnoux et al. used an effective method to deal with the keyboards emissions and recovered keyboard entry from a distance around 20 meters with 95% success [5]. Zhang studied on compromising mechanism of the keyboards and compared the emanations among various keyboard types [6]. Kuhn studied on many researches in the field of CE of CRT displays, laptop displays, and flat panel displays. Kuhn reconstructed a CRT display image from three meters away [7]. Then laptop displays and flat panel displays are studied, and target display images are reconstructed successfully [8, 9].

Printers are also used as output devices for computer systems. Acoustic emanations of printers were studied in 1991, and the letters “W” and “J” were distinguished successfully

[10]. An attack method has been presented which is based on the recording of the sound of a dot matrix printer processing English text [11]. Up to %72 of the printed words were recovered and the attack achieved recognition rate up to 95 % with the assumption of the knowledge about the text. Tosaka et al. studied the CE of laser printers, and they measured the magnetic field of a laser printer in the near field and achieved to reconstruct the printed image [12]. Przesmycki used some special Test Patterns (TP) to improve to the measurements of CE of monochromatic laser printers [13]. He presented the oscillograms of three lines that placed on different places of white sheet.

In this paper, CE of a laser printer is investigated in the media of power line conductors, signal line conductors, and electric radiation (ER). While the most of the studies focuses on the measurements of CE in the media of ER, in this study, it is also shown that the risk of information leakages in the media of power and signal lines (like USB) cannot be ruled out. In addition, we introduce a practical approach of searching CE using a conventional spectrum analyzer. In this approach, it is shown that the configuration of resolution bandwidth, frequency span and the sweep time has to be applied properly. Moreover, to be able to analyze and detect the CE frequency points more conveniently, new image patterns are proposed in addition to ones introduced by Przesmycki [13].

In the next section, the emission measurement setups in ER, PLC, and SLC are given. In Section 3, the approach for the searching CE and the evaluation of the TP are discussed. The image reconstruction method from the CE of the printer emissions is explained section 4. Finally, the paper is concluded in Section 5.

2. Emission Measurement Setup

Visual assessment of emissions is really difficult in the case of a laser printer. The video signal is sent at a specific time in the printing process and activation time is limited. The same is true for the laser exposure system. Another difficulty is the noise produced by the sub-system used at the printing process, which could mask the CE.

The method used in this study is based on the study descripted in [13], which consist of using a spectrum analyzer and an oscilloscope. If the settings of wideband receiver system are not appropriate, detection of CE is almost impossible. Signal detection process consists in scanning the whole frequency range of the measurement setup and searching for any variation in the emanation that is related to the TP. When relation is determined, emanation is demodulated according to its amplitude modulation (AM) as descripted in [13] and [5]. The spectrum analyzer is used to identify the data-related emanations and a spectrum analyzer and an oscilloscope are used together to decide whether the relation is a compromising emanation or not. In this way, the number of frequency points to be investigated is reduced significantly.

Tests are conducted in a Fully Anechoic Room (FAR) as shown in Fig. 1 and Fig. 2. The method is also compared with the method proposed by Przesmycki [13] in the media of Electric Radiation (ER). A personal computer used to send TP and the measurement system is located in the control room. The laser printer is placed on a table in the FAR as shown in Fig. 1 and Fig. 2. FSET 22 is used as spectrum analyzer and the video output of the receiver is connected to the high storage oscilloscope. Here, the video output provides the AM-demodulated data, which is then sampled by the oscilloscope.

Searches are also performed for CE conducted on power line and signal line over 100 kHz to 1 GHz. General line-conduction measurement setup is shown in Fig. 1. While SLC measurements are performed using only current probe, PLC measurements are performed using either a current probe or a Power Line Impedance Stabilization Network (PLISN). In PLC measurements, both PLISN and current probe are used to differentiate emanations from the power cable and power leads.

ER measurements are performed over the frequency range 10 kHz to 2 GHz. In ER measurements, three types of antenna is utilized,

which are rod antenna in the frequency range of 10 kHz - 30 MHz, biconical antenna in the frequency range of 30 MHz - 300 MHz, and log periodic antenna in the frequency range of 300 MHz - 2 GHz.

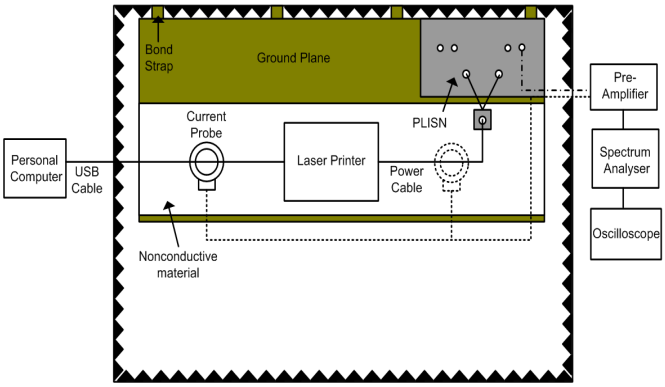


Fig. 1. Measurement setup of the laser printer's power leads and USB cable in the Fully Anechoic Room (FAR).

In all measurements with biconical and log periodic antennas, they are polarized vertically and horizontally and positioned 1 meter away from the front edge of the setup boundary and 1 meter above the floor as shown in Fig. 2.

In the experiments, the same pattern is printed multiple times to ensure the emanations from the laser printer to be an unchanging input signal. Analysis with the swept spectrum analyzer needs time ranging 5 milliseconds to several seconds to sweep across the frequency span. This approach is based on the assumption that the input signal is not changed significantly in the time it takes

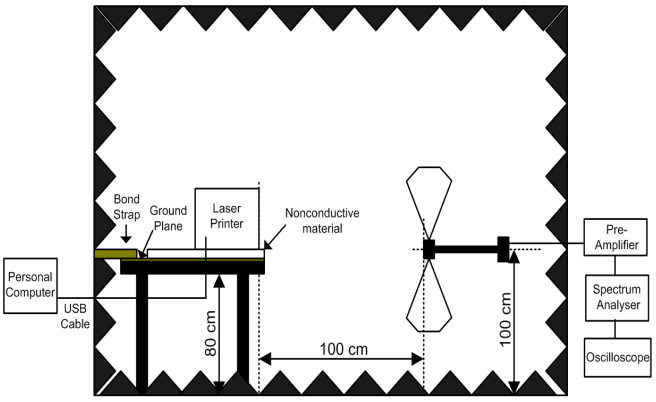


Fig. 2. Measurement setup for ER tests and antenna position in the FAR.

to complete a sweep of the analyzer. We determined that 10 pages per pattern are adequate to assure the emanations as a static input signal.

Another way to improve the input signal quality is to use appropriate TP whose characteristics could be easily detected from the emanations by visual assessment. TP shall be simple but at the same time shall be complex enough to be noticeable in the noisy spectrum. The TP (IV, V, and VI) used in this study are shown in Fig. 3. The emissions from printing Pattern I are used as reference to distinguish data-related emissions from the other patterns in every measurement as in [13].

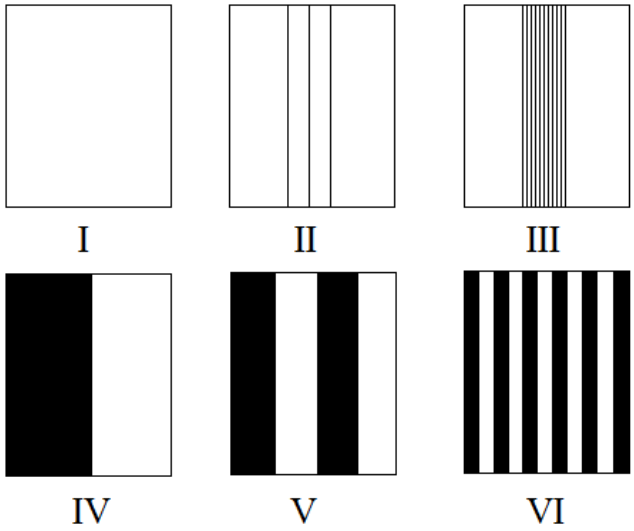


Fig. 3. Test patterns used in this study.

3. The Approach for Searching CE and the Evaluation of Test Patterns

In this section, we describe our approach to capture the data-related emanations and to evaluate whether the data-related emanation is a compromising emanation or not. The method is used in ER, PLC, and SLC media, and the obtained results are given. The analyses carried out in frequency domain are explained in this section.

The print speed of current laser printers is nearly 30 pages per minute. It means that it is necessary to sweep frequency span multiple times in 2 seconds to catch the CE. Sweep time (ST) is the most critical parameter in the all setting of the analyzer because of an absent of a

mechanism to trigger the analyzer as in the case of laser printer tests. The ST is dependent on the resolution bandwidth (RBW), frequency span, and the design of the spectrum analyzer. For a near-Gaussian-shaped analog RBW filters, the relation between ST, span, and the RBW can be obtained through Equations (1-3).

$$t_p = \frac{RBW}{Span} ST \tag{1}$$

where t_p is the time in pass band. This time can be approximated to rise time t_r of the filter which is inversely proportional to the bandwidth of the filter as

$$t_r = k \frac{1}{RBW}. \tag{2}$$

If the terms t_p and t_r are equalized and solved for ST, the following relation is obtained.

$$ST = k \frac{Span}{RBW^2} \tag{3}$$

where k is the constant of proportionality.

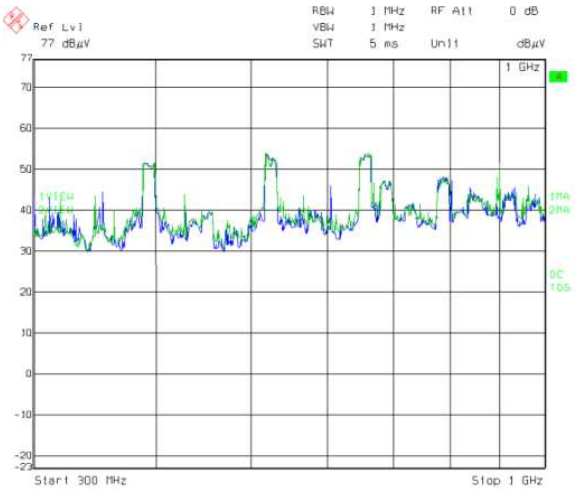
There is a tradeoff among frequency selectivity, which can be improved by reducing RBW, signal-to-noise ratio (SNR), frequency span and measurement speed as seen in Equation 3. As RBW is narrowed at a fixed frequency span, the displayed average noise level of the spectrum analyzer is lowered. SNR and the selectivity are improved but the sweep time and trace update rate are degraded. For modulated signals, it is important to set the RBW wide enough to include the sidebands of the signal to make the measurement accurate. The optimum choice of the spectrum analyzer setting depends heavily on the characteristics of the signals of interest. In this study, we try to determine the most suitable spectrum analyzer setting to capture the CE from the laser printer.

In the first study, we set RBW to 500 kHz as in [13] and sweep the 300 MHz – 1 GHz frequency band. Pattern I and Pattern II are used for the test as [13]. Fig. 4(b) gives the measurement results. As seen from the figure that there is no apparent frequency points or bands to be evaluated as the data-related emanation. We change RBW value and repeat the measurements to find a narrower frequency range to start with. Measurement results are presented in Fig. 4. At first step we chose RBW as 1 MHz. Emissions related to Pattern I and Pattern II are become more similar than the emissions measured when we set RBW to 500 kHz as seen in Fig. 4(a). Assigning the data-related emanation is become more difficult as we increase RBW value. We decide to use RBW values lower than 500 kHz.

The measurement results as RBW is set to 100 kHz and 50 kHz are presented respectively in Fig. 4(c) and Fig. 4(d). There is no improvement on determining the date-related emanation between the measurement results as RBW is set to 100 kHz and 500 kHz as seen in Fig. 4(c) and Fig. 4(b). Emissions related to Pattern I and Pattern II could only be distinguishable when RBW is set to 50 kHz as seen in Fig. 4(d).

The proposed minimum value for RBW is 50 kHz because lower values make the sweep time of 300 MHz – 1GHz frequency span longer than print time of one page. As we examine Fig. 4(d), pattern emissions are explicitly differentiated from each other in following sub-bands: 400 MHz – 435 MHz, 460 MHz – 620 MHz and 820 MHz – 880 MHz.

(a)



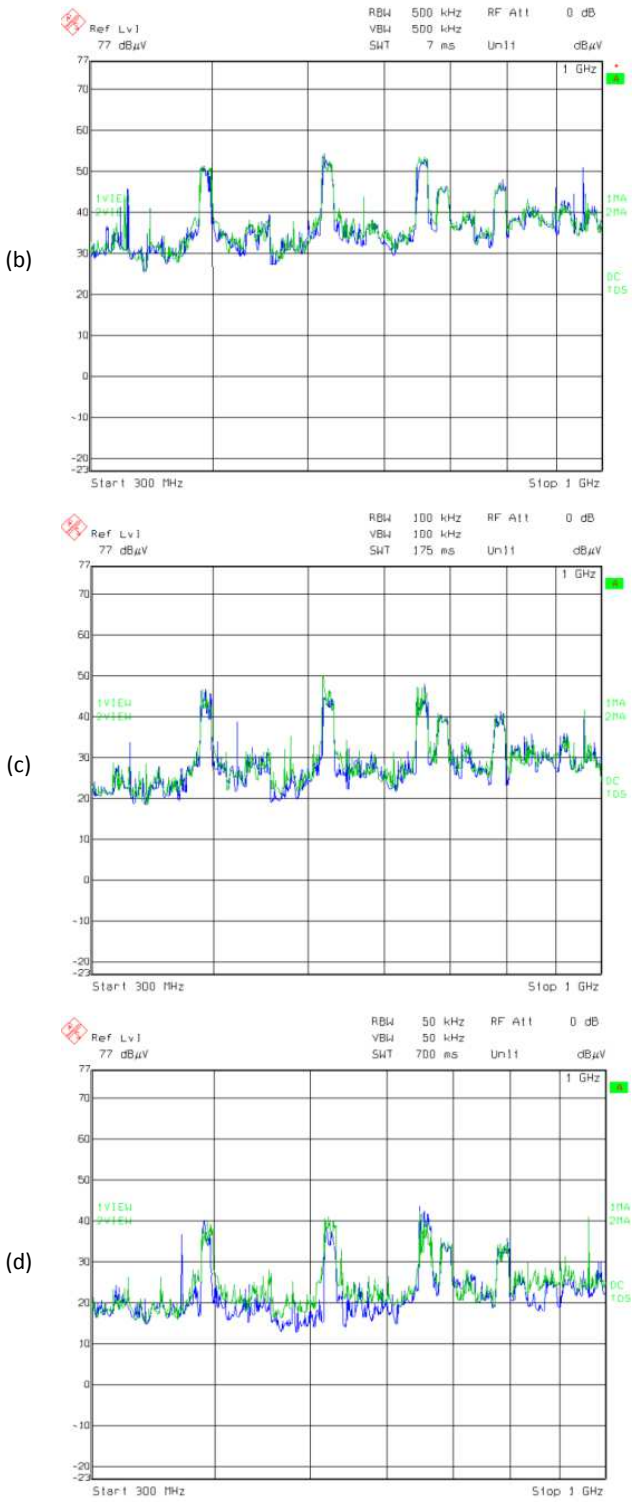
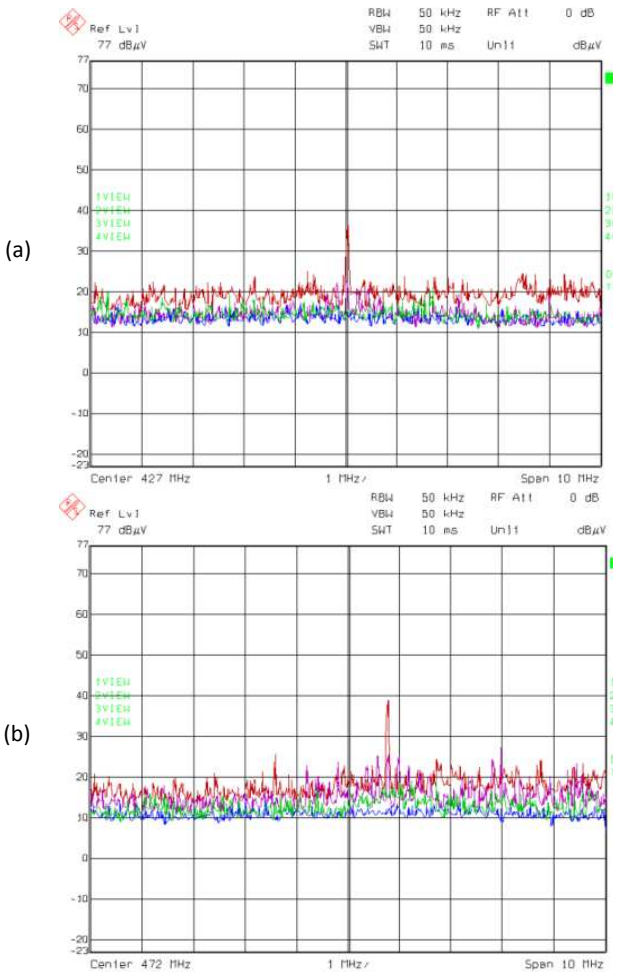


Fig. 4. ER test results while printing patterns, Blue: Pattern I, Green: Pattern II; (a) RBW = 1 MHz. (b) RBW = 500 kHz. (c) RBW = 100 kHz. (d) RBW = 50 kHz.

In the second study, it is made searches in the sub-bands listed above to capture the emanations related to the video signal. We choose the span value between multiples of 5 MHz to cover the sub-bands properly. In order to determine the optimum span value, 5MHz, 10 MHz, and 50 MHz span is investigated in the following.

It is started with 10 MHz span value and the results are given in Fig. 5. Emanations related to empty page and Pattern II are almost the same in all sub-bands. The difference between empty page and Pattern III is negligible in all span steps. Possibly, the number of lines and the thickness of each line at Pattern II and Pattern III would not be enough to radiate the data-related emanations that would pass the noise level at 50 kHz RBW.

Test patterns IV, V, VI are compared with test patterns I, II, III. Although the difference among empty page and test patterns I, II, III are not distinguishable, for the proposed patterns the emission difference is around 15 dB in all the data-related frequency points as shown in Fig. 5.



(c)

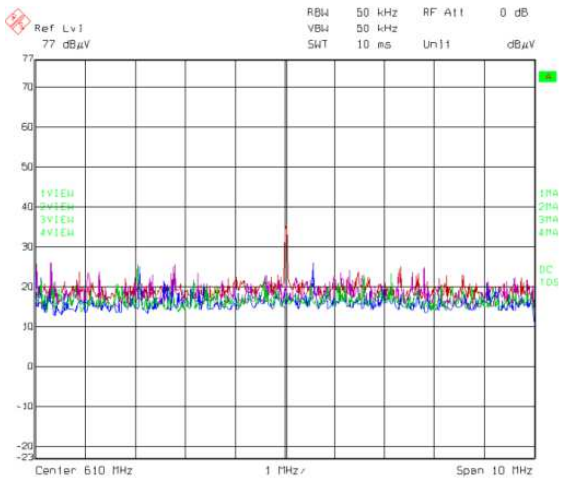


Fig. 5. ER correlated to TP. Blue: Pattern I, Green: Pattern II, Magenta: Pattern III, Red: Same for Pattern IV, V, and VI. Center Freq: (a) 437 MHz, (b) 472 MHz, (c) 610 MHz.

Pattern VI is the most suitable candidate for searching the data-related frequency points in oscilloscope to decide whether it is a compromising emanation or not since it can be identified under the high level noise due its high frequency content. Therefore, in the rest of the study, Pattern VI is used. For this particular case, while the emissions in 400 MHz – 435 MHz and 460 MHz – 620 MHz subbands contains the data-related emanations, in 820 MHz – 880 MHz sub-band, any data-related emanation frequency point isn't found. This difference might be result from the laser assembly system that is not used while printing empty pages.

In the second step, we repeat the tests with empty page and Pattern III by setting RBW to 5 kHz. Maximum frequency span is set to 5 MHz due to the limit on the print time.

The results are presented in Fig. 6. SNR is improved as 10 dB and peaks related to Test Pattern (TP) become visible. In some sub-bands improving SNR as 10 dB is not enough to make peaks visible. We narrow the span and decrease the RBW. This approach increases the search time of the whole frequency band. On the other hand, Pattern VI allows us to increase the RBW and frequency span as shown in Fig. 7. Although the radiations related to Pattern III aren't visible as given in Fig. 6, the radiation related to Pattern VI improves the SNR without lowering the RBW.

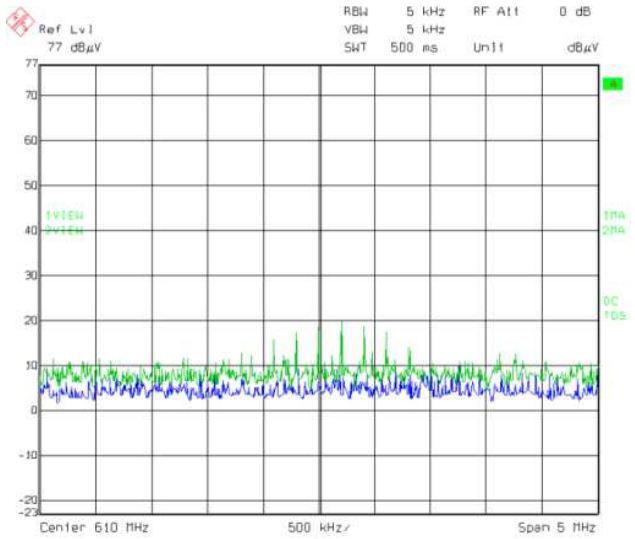


Fig. 6. ER correlated to test patterns; Blue: Pattern I, Green: Pattern III.

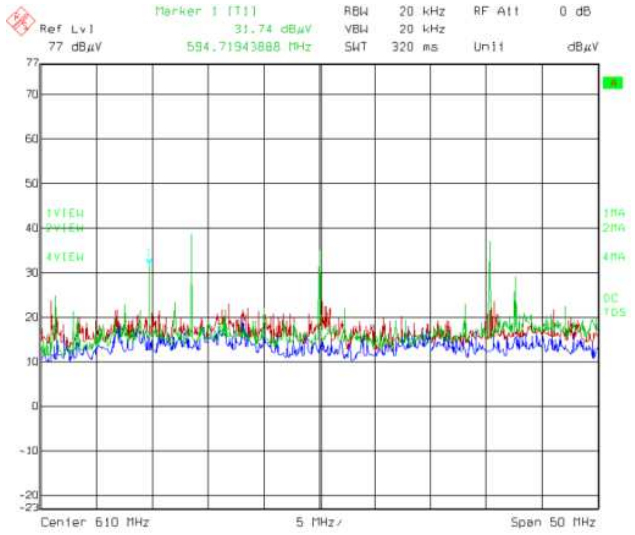


Fig. 7. ER correlated to test patterns; Blue: Pattern I, Green: Pattern VI, Red: Pattern III.

High RBW allows us to increase the frequency span; thus, the search time of the whole frequency band is decreased significantly.

In the experimental tests, it is observed that the span width larger than 50 MHz makes it difficult to decide whether an emanation is data-related or not because the number of peaks increases. As the number of peaks increases, the number of tests increases to determine whether an emanation at the peak point is data-related or not. We set RBW to 20 kHz to improve SNR. RBW values lower than 20 kHz with 50 MHz span makes sweep time longer than print-time of one page.

In the third study, we aim to determine whether sweeping the whole band as in the first study or sweeping the whole band by dividing into sub-bands. We divide 300 MHz – 1 GHz band into 50 MHz sub-bands and set RBW to 20 kHz. We find the data-related emanation points in the 700 MHz – 750 MHz sub-band which is not explicit in Fig. 4(d). Therefore, it is considered that the best way to search of the data-related emanations of laser printers is to divide the test frequency range into sub-bands and to use RBW as minimum as possible.

In the next section, the details of the data reconstruction from electromagnetic emanations are explained.

4. Reconstruction of the Printer Data

The method proposed in the preceding section provides us the CE in the analyzed frequency points. However, to be able to obtain and certify a human readable document, the AM-demodulated data in these frequencies are sampled with a high storage oscilloscope, and the document printed is reconstructed by applying signal processing techniques.

First, in order to understand the structure of printer data, which is directly obtained from the video signal sent to the laser scanner system with a probe, its representation in one dimensional (1D) space is investigated. Second, the row frequency used to convert 1D data to 2D image is calculated. The similar procedure in the second step is carried out for the AM-demodulated data, and the reconstructed image is shown on a computer screen as an image. In the following section the sampled data is analyzed.

4.1. Representation of the 1D Printer Data

The time domain representation of a 1D printer data obtained from the video signal of the formatter output is given in Fig. 8(a). To be able to capture one image page, one has to collect about 1 second data. For this reason, the data signal is sampled with 10 MHz by an oscilloscope, which provides 10 Million Sample (MS) points. The data printed is a text with the font of Times New Roman and 72 pt. The corresponding frequency domain representation of the printed data is shown in Fig. 8 (b).

As seen from the frequency content, the most of the power accumulated in the first 1 MHz band. The reason is that the 72 pt. text fills almost only the 1 MHz spectrum. Thus, it can also be said that for this particular case, it is sufficient to use 2 MHz sampling frequency to reduce the sample points to 2MS. This 1D data has to be converted to 2D data in order to obtain the printed document image. Therefore, one needs a row frequency (or horizontal synchronization) for the conversion, and this information is not known by an attacker in advance. However, a simple and effective computation method to find row frequency is introduced in the next section.

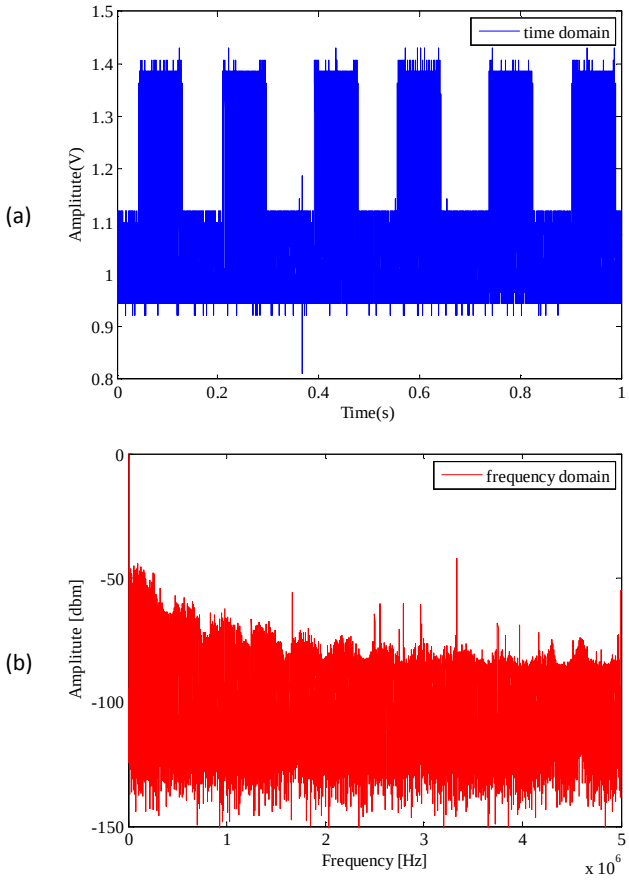


Fig. 8. Printer data singal representation. (a) in time domain. (b) in frequency domain. The sampling frequency is 10 MHz.

4.2. Extraction of the Row Frequency

To be able to reconstruct the printed data and raster it in 2D, one has to know the row

frequency. The terminology of the row frequency is borrowed from video raster concept of the Video Display Units (VDU). The row frequency of a VDU, also known as horizontal frequency, can be obtained by the VESA standards if one knows or guests the resolution of VDU. Unfortunately, apart from the producer, one cannot know the row frequency of the printer since it is not declared in anywhere. However, this row frequency actually is hidden in the 1D data and can be obtained from the frequency spectrum by looking at the low frequencies. Mostly, the first powerful spike after the DC component provides the row frequency. In some cases, the first component can be weaker but by looking at other spike frequencies, it is seen that the other consecutive spike frequencies are the multiple of the main component. For the example given in Fig. 8, we obtain the row frequency as 2407 Hz for the given data as shown in Fig. 9. The other spike frequencies are 4814 Hz, 7221 Hz, and 9628 Hz, respectively.

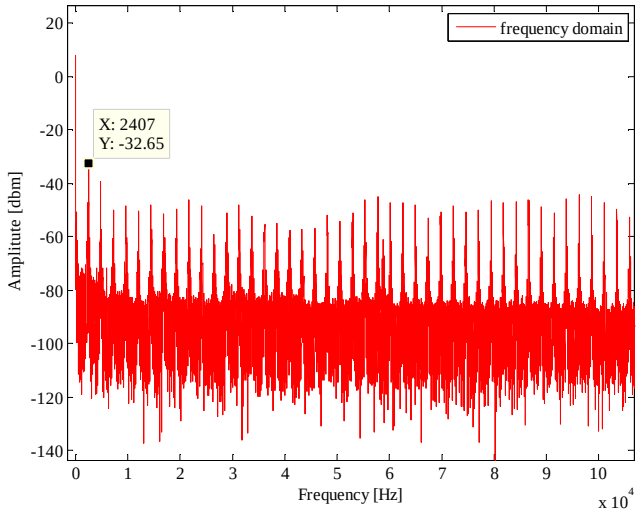


Fig. 9. Extracting the row frequency from the frequency spectrum.

4.3. Data Reconstruction from the Emissions

The similar procedure of finding the row frequency for the ideal data is applied also for the emissions obtained by the receiver systems. The AM-demodulated data is sampled by an oscilloscope and stored. Then this data is analyzed in the frequency domain to find the row frequency. Similarly, we focus on the first part of the spectrum and measure the row frequency. As shown in Fig. 10, the reconstructed image, the printed document, can be easily read. The row frequency is actually a real number, and the reason of obtaining a rotated image is that the row frequency is rounded to an integer value to be able convert 1D array to 2D image matrix.

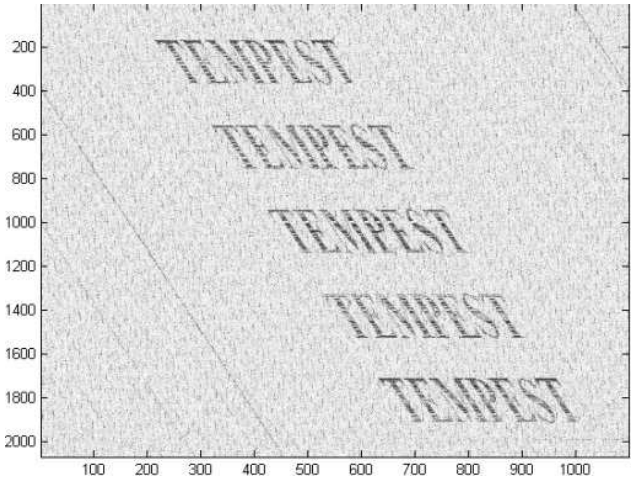


Fig. 10. Reconstructed image from the emission.

5. Conclusion

In this study, the CE of a laser printer are analyzed in different media. The emissions obtained from the electric radiation, power cable and signal line conductors like USB cable is investigated, and a measurement method to reveal the possible information leakages is proposed. Finally, the procedure of the image reconstruction of CE of the laser printer data is explained in detail. The experimental results show the vulnerability of the commercial laser printers in terms of emission security.

Acknowledgements

This work was supported in part by the Scientific and Technological Research Council of Turkey (TUBITAK) under the project TEMPEST Tests.

References

[1] H. Highland and V. Fåk, "Electromagnetic radiation revisited, part II," *Computers & Security*, vol. 5, pp. 181-184, 1986.

[2] K. Beckman, "Leaking Computers – information on compromising emanations," presented at the National Council for Crime Prevention, Stockholm, Sweden, 1984.
[3] W. Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," *Computers & Security*, vol. 4, pp. 269-286, 1985.
[4] H. Fang, "Electromagnetic Information Leakage and its Protection of Computer," presented at the Science Press, Beijing, 1993.
[5] M. Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," in *USENIX Security Symposium*, 2009, pp. 1-16.
[6] J. Zhang, "Information Recover Based on Compromising Electromagnetic Emanations of Keyboard," *Beijing: Desertation of Beijing Jiaotong University*, 2010.
[7] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," *University of Cambridge Computer Laboratory, Technical Report, UCAM-CL-TR-577*, 2003.
[8] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in *Privacy Enhancing Technologies*, 2005, pp. 88-107.
[9] M. G. Kuhn, "Eavesdropping attacks on computer displays," presented at the Information Security Summit, 2006.
[10] R. Briol, "How to keep your data confidential," in *Electromagnetic Security for Information Protection*, 1991.
[11] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers," presented at the Proceedings of the 19th USENIX conference on Security, Washington, DC, 2010.
[12] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, and M. Hattori, "Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer," in *Electromagnetic Compatibility, 2006. EMC-Zurich 2006. 17th International Zurich Symposium on*, 2006, pp. 630-633.
[13] R. Przesmycki, "Measurement and Analysis of Compromising Emanation for Laser Printer," in *PIERS Proceedings*, 2014.