

Development of an Automatic TEMPEST Test and Analysis System

Cihan Ulaş, Serhat Şahin, Emir Memişoğlu
TUBITAK BILGEM, Gebze, Kocaeli Turkey
{cihan.ulas, serhat.sahin, emir.memisoglu}
@tubitak.gov.tr

Ulaş Aşık, Cantürk Karadeniz, Bilal Kılıç, Uğur Saraç
TUBITAK BILGEM, Gebze, Kocaeli Turkey
{ulas.asik, canturk.karadeniz, bilal.kilic, ugur.sarac}
@tubitak.gov.tr

Abstract— Today, it is clearly known that the electronic devices generate electromagnetic radiations unintentionally, which may contain critical information called compromising emanations (CE). CE is also known as TEMPEST radiation, which is a code name firstly used by an U.S government program. Every developed country has a TEMPEST Test Laboratory (TTL) connected to their National Security Agency (NSA). The main objective of these laboratories is to investigate equipment, systems, and platforms processing cryptographic information in terms of CE. TEMPEST tests might take very long time depending on the item under test. In this paper, a complete Automatic TEMPEST Test and Analysis System (ATTAS) developed in TUBITAK, BILGEM TTL is introduced. The system has the following properties, which are automatic system calibration unit, automatic test matrix generator based on the SDIP-27/1 standard, implementation of tunable and nontunable tests, automatic CE investigations, rendering of the CE of video display units, playing of the CE of audio signals, measurement of detection system sensitivity, zoning of TEMPEST equipment based on SDIP-28 standard, and generation of graphical results.

Keywords—*Compromising Emanations, TEMPEST Test System*

I. INTRODUCTION

Military history of exploitation of compromising emanations began as early as 1914s during World War I. The concept of information intercept prevention came into existence when the German army successfully eavesdropped on enemy voice communication from the earth loop current of allied battlefield phone lines. US Army engaged Herbert Yardley and his staff of the Black Chamber to develop methods to detect, intercept and exploit combat telephones and covert radio transmitters [1]. During researches, US Army discovered that equipment without modifications was vulnerable to enemy attacks and started a classified program to develop methods to prevent leakage of the classified information. The standards and works on emission security are kept secret all over the world. Only the US government declassifies some part of its emission security program but the revealed material can also be found in the open computing, security, and electromagnetic-compatibility literature. The only known is the name of US national compromising-emanations test standards name and their publication year. “NAG1A” and “FS222” were the first defined compromising-emanations test standards published in the 1950s and 1960s. In 1970 a new version called “National Communications

Security Information Memorandum 5100: Compromising Emanations Laboratory Test Standard, Electromagnetics” was released. “NACSIM 5100” was replaced with “NACSIM 5100A” in 1981. The last known revision is “NSTISSAM TEMPEST/1-92” declassified in 1999 after a Freedom-of-Information-Act request made by John Young [2]. All these standards and their NATO equivalent “SDIP-27/1” are still classified documents [3].

Academic research on compromising electromagnetic emanations started in the mid 1980’s and there have been significant recent progresses. The first open publication about compromising emanation risks was an 18-page booklet released by a Swedish government committee in 1984 to inform business community [4]. The risk was brought to general attention by van Eck in 1985 [5]. In the paper, van Eck reconstructed the Cathode Ray Tubes (CRT) screen content at a distance by using low-cost home built equipment. Furthermore, attacks to recover information from RS232 cable [6], Liquid Crystal Display (LCD) [7], laser printer [8], keyboard [9], [10], and [11] have been carried out.

In this paper, Automatic TEMPEST Test and Analysis System (ATTAS) has been developed to meet the overall TEMPEST test requirements and evaluation procedures defined in SDIP-27/1 [3]. ATTAS provides several advantages with respect to manual test system and conventional CE investigations. First, the system has an automatic validation unit providing a very fast and practical system-check capability. Second, the test matrix can be generated based on the rules and procedures defined in the standard SDIP-27/1 or can be imported to the system if it is already prepared by the test engineer. Third, the traditional tunable and nontunable tests can be performed with the generated or imported test matrix. Fourth, the CE investigations are carried out automatically, where the RED signal, which represents the classified information, is required for correlation between the RED and BLACK signal, which represents the unclassified or encrypted information. The suspected CE signals can be analyzed based on the signal type, which can be a video signal, audio signal, and a digital signal. A video signal, which is assumed that their screen resolution is known, is displayed within a user-friendly panel. Similarly, if the signal is a voice signal it can be easily played by the speakers. Moreover, the detection system sensitivity (DSS) measurements can be performed automatically in a few minutes. TEMPEST Device

Zoning (TDZ) described in the SDIP-28/1 [12] standard can be carried out successfully. Finally, the TEMPEST test report builder can be used to combine the graphical results.

II. RELATED WORKS

A. Types of Compromising Emanations

CE of the Video Display Units (VDU) has a high importance in the concept of TEMPEST. Van Eck showed that CRT screen content could be obtained by affordable equipment [5]. Nowadays, the CRT monitors is almost out of date, and instead, LCD and LED monitors are in fashion. Screens, represented in 2D, are composed of streaming frames represented in 1D. The vertical representation is called as a monitor screen (S_t) at time t and its frame representation (F_t) is given in (1).

$$S_t = \begin{bmatrix} \text{row}_1 \\ \text{row}_2 \\ \cdot \\ \cdot \\ \text{row}_N \end{bmatrix}, \quad F_t = [\text{row}_1 \quad \text{row}_2 \quad \cdot \quad \cdot \quad \text{row}_N] \quad (1)$$

There are redundant blanks behind and in front of the rows and frames. These blanks provide the time for the scanning and are not visible in the monitor screen. To be able to reconstruct the information of monitor screen from an obtained frame, the Horizontal Synchronization (HS) is very crucial since it is used as conversion from 1D data to 2D screen. Both the horizontal and vertical (refresh rate) synchronization signals exist in the actual transmission between monitor and PC. In the case of CE of VDUs, an attacker can only obtain the frames; however, Furkan et al showed that the synchronization signals could be obtained from the frames by using signal-processing techniques [13]. It is also known that the synchronization signals are constant and sufficient to solve them once; moreover, VESA standards provide synchronization signals if the screen resolution is known. For instance, the HS for 1280x1024 @60 Hz resolution is given as 63.981 kHz. Frame data including frame blanks and row blanks is converted to 2D screen as shown in Fig. 1.

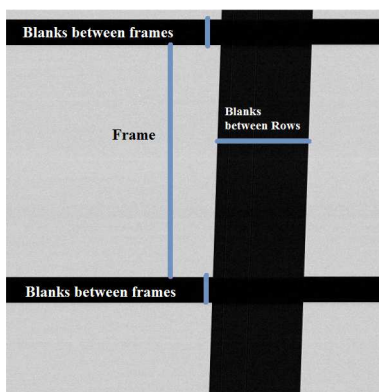


Fig. 1. A whole frame representation in 2D.

The existing ATTAS video rendering module requires the row frequency (equal to HS), which is obtained by VESA standard. An extensive report is published by Kuhn on eavesdropping risk of computer displays for analog and digital video platforms [4]. Signal processing applications for information extraction from the VDUs emissions is presented by Koksaldi [14].

Another type of the CE is composed of keyboard leakages. Keyboard is an important input device of computer processing confidential information. Although Han Fang did some analysis on CE of the keyboards [15], a breakthrough has been achieved by Vuagnoux et al, who proposed a method to recover keyboard emanations with 95% success and a distance around 20 meters. Wang and Yu analyzed a representative control circuit of keyboards by focusing on the PS/2 keyboard protocol in order to find the sensitive signals causing CE [11]. A recent study on CE of keyboard, which investigates the information leakage on the ground line of the PS/2 serial cable, is presented in 2013 [10]. It has been shown that the keystroke signals might leak to ground line network which then be recovered on the other power outlets sharing the same electric line.

B. TEMPEST Test Procedures

For any equipment under test (EUT), it is necessary to prepare a document called as TEMPEST test plan that gives the detailed information about test procedures to be performed. A TEMPEST test plan document should contain the purpose of the test, technical information about the EUT, general representation of RED/BLACK signals, potential emanations, test environment, exercising equipment, operation modes, test media, test setups, and test matrix. TEMPEST tests start with the approval of TEMPEST test plan by NTA. A test process consists of three steps, which are verification of measurement system, measurement of emissions, and advanced signal analysis. After tests, a TEMPEST test report document, containing equipment of test and their dates of calibration, test setups, TEMPEST test procedures, and graphs of the test results, is prepared. Thus, one can say that TEMPEST tests consist of following three steps, preparing a TEMPEST test plan document, executing tests and finally preparing a TEMPEST test report document.

In TEMPEST evaluation procedures, examination and classification of detected emanations is the most difficult step because of the dependency on many parameters such as detection system capabilities, techniques used in signal analyses, personnel experiences, qualification of test environment etc. CE mostly appears in three signal types, which are in baseband, modulated by a carrier signal, and impulsive emanations; therefore, it is not easy to classify detected emanations unless implemented with a detailed examination. In addition, in some cases, the electromagnetic emissions can be data related but one cannot prove whether they are compromising emanations or not. Therefore, the difficulties in the search of compromising emanations require

a fast and reliable TEMPEST test and analysis system in addition to save cost and time.

III. TEMPEST AUTOMATIC TEST AND ANALYSIS SYSTEM

The ATTAS block diagram is given in Fig. 2. The system has three main equipment, which is pre-amplifier, test receiver (FSET), and oscilloscope, connected to a control personal computer (PC). A low noise pre-amplifier is very important to increase the SNR, and in ATTAS, a custom (switchable) pre-amplifier, including two pre-amplifiers working in two different frequency bands, is used depending on the working frequency band. A pre-amplifier is used in 100 Hz - 1 GHz frequency band, which has 32 dB gain, and another amplifier is used in 1-20 GHz frequency band, which has a 26 dB gain. The second equipment, connected to control PC via GPIB/USB converter, is the TEMPEST Test Receiver (FSET) produced by the company of Rohde & Schwarz. This test receiver is devoted to the TEMPEST tests, working in the frequency range of 20 Hz - 22 GHz with at most 500 MHz bandwidth, which is the largest bandwidth in the marketplace. The last equipment is the oscilloscope, where the model of either Lecroy Wave Runner 640Zi or Lecroy WavePro 7300A, which has 4 GHz and 3 GHz bandwidths, respectively, can be used.

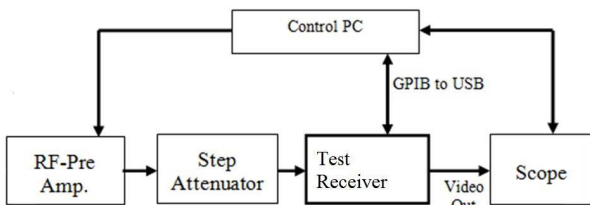


Fig. 2. ATTAS block diagram.

In Fig. 3, a sample test setup in fully anechoic chamber and the control room including ATTAS is shown. The properties of the ATTAS are introduced in the following subsections.

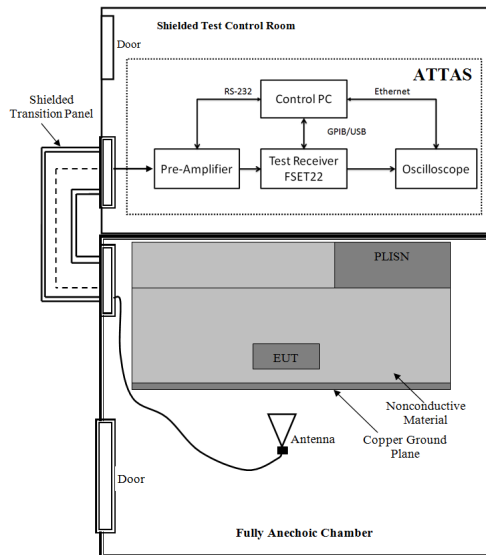


Fig. 3. Test setup and control room including ATTAS.

A. Automatic System Calibration/Validation

According to the Laboratory standards like ISO 17025, before starting tests, the test infrastructure should be checked and validated if everything is all right. For this reason, a test engineer has to start a test day by validating that the devices used in the measurement system are working properly. Every component or transducer, like cables, connectors, antennas, probes, amplifiers, RF limiters in the measurement system has a correction factor. Therefore, this fact has to be considered when evaluating the measurement results. The conventional calibration procedure is applied in three steps. First, the correction factor of the transducer or set, which may include more than one transducer like cable, antenna, and amplifier, is selected in the Test Receiver (TR). Second, the Signal Generator (SG) is tuned to a starting frequency, which might be the lowest frequency of the test receiver system, with constant amplitude. Third, the generated signal is measured in the TR while tuning it to the frequency set by the SG with the proper span and bandwidth. This procedure is repeated with frequency increments up to the highest frequency of the measurement systems. In traditional system calibration, the test engineer checks about 20 points by finding the errors between the generated and measured signal amplitudes. This error is also considered as an overall system correction factor and has to be added to the measurement results. This boring procedure takes about more than an hour for every measurement day. The aim of the automatic calibration unit is to carry out this procedure automatically by controlling the SG, TR, and amplifiers in a remote mode. With this way, the overall system correction factor is computed in much more points and loaded to the system automatically in a few minutes. Automatic calibration user interface is shown in Fig. 4.

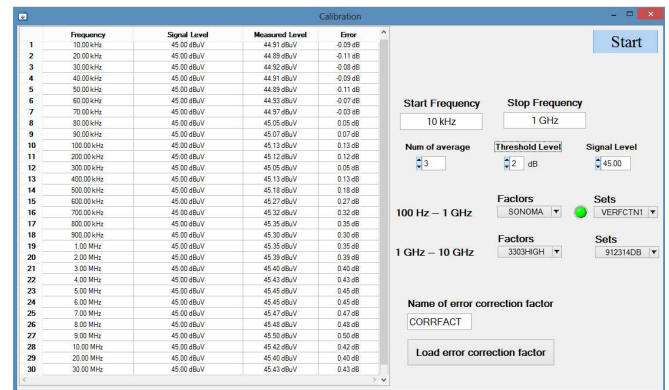


Fig. 4 Automatic calibration user interface.

B. Automatic Test Matrix Generator and Importer

The TEMPEST Test plan preparation procedure defined by the SDIP-27/1 consists of straightforward rules. These rules are based on the signal properties like speed, bandwidth, type, and the test medium, which can be Electrical Radiations (ER), Magnetic Radiations (MR), and BLACK Line Conducted (BLC). The automatic test matrix generator provides the test matrix based on the rules defined by the standard. However,

the test engineers usually prefer to prepare the test matrix manually due to the traditional reflexes. For this purpose, a user interface is developed to import a prepared test matrix from an excel file. Thus, the test engineer can start the tests easily and quickly.

C. Implementation of Tunable and Nontunable Tests

In the TEMPEST standard, tests are divided into two main parts, which are tunable and nontunable tests. Tunable tests are based on a test receiver, where FSET 22 produced by Rohde & Schwarz (RS) is used. Tunable tests are performed based on generated or imported test matrix, which contains the start frequency, stop frequency, resolution bandwidth, and transducer. In the second part, Nontunable tests are carried out based on an oscilloscope, where Lecroy Wave Runner 640zi or WavePro 7300A is used.

D. Automatic Compromising Emanation Investigations

The heart of the analysis system is the investigations of the CE automatically. In the conventional method, the CE are searched in the frequency points where the emissions pass above the limit line, which is defined by SDIP-27/1 [3]. During the tests, it is assumed that the RED signal, is known and applied periodically. In frequency points looked for CE, the test receiver system is operated in the zero-span mode, which produces AM-demodulated signal at tuned center frequency. The video out of the test receiver system is connected to the oscilloscope with a high storage capability. The test engineer constantly looks for the similarities and correlations between the RED signal and demodulated signal. The searching of CE in such a way is very problematic, especially when the RED signal is a type of audio signal. The audio signals are narrowband and mostly checked by the test engineers' ear. If we assume that the test span is wideband spectrum, such as from DC to 1GHz, and the audio signal bandwidth is 5 kHz, the test engineer has to check 200.000 points. This process obviously takes weeks or months depending on the emission levels above the limit lines. In addition, the tests are carried out with at least two people switching in every 30 minutes to save their ear and keep the tests reliable. The aim of the automatic CE investigations is to solve this problem by controlling test receiver, amplifiers, and oscilloscope remotely. Before starting the search of automatic compromising emanations, the RED signal, which we are looking for correlation, is saved with a sufficient number of samples and sampling rate. Then the spectrum is swept with a proper bandwidth, span, and transducer. The related limit line defined in the standard is added to the spectrum graph, and the frequency points above the limit line are determined. The correlation, given by (2), between the RED and demodulated signal is calculated for each frequency point. The results are listed in a table.

$$\text{corr} = \max \int_{-\infty}^{+\infty} r(t-\tau)b(\tau) d\tau \quad (2)$$

In ATTAS, the digitized signals can be interpreted as follows.

1. Displaying and Correlating CE with Zooming

In the analyses, the signal digitized by the oscilloscope, which either might be the BLACK or the RED signal, can be displayed in the control PC's screen with zooming property. The correlation between two signals can be computed and they can be shifted on each other to see the similarities on the zoom panel.

2. Playing CE of Audio Signals

In the analyses, the digitized signal by the oscilloscope, which might be either the BLACK or the RED signal, can be played on the speakers connected to control PC.

3. Rastering CE of Video Signal

In the analyses, the signal digitized by the oscilloscope, which might be either the BLACK or the RED signal, can be rendered and visualized by the system. To be able to visualize the signal, the vertical synchronization frequency has to be known, which is found from the VESA standards [16] for the time being.

E. The Detection System Sensitivity Measurements

The Detection System Sensitivity (DSS) measurements are carried out for tunable and nontunable detection systems and should apply to all signal classes as appropriate for the test to be performed. All DSS measurements should be made using correct calibration source. These methods are specified using sine wave substitution source and given as [3]:

Method 1 requires a calibrated unmodulated carrier as the substitution signal, and is applicable when measuring the DSS at the pre-detection (e.g. IF) output of tunable detection systems and at the output of nontunable detection systems.

Method 2 requires a calibrated sine wave carrier modulated at 30% by a sine wave at any suitable frequency less than or equal to the repetition rate as the substitution signal, and is applicable when measuring the DSS at the AC or DC coupled post-detection output.

Method 3 is applicable when measuring the DSS at the DC coupled post-detection output possessing technical limitations preventing the use of a modulated sine wave carrier as the substitution signal. The required substitution signal for Method 3 is a calibrated unmodulated carrier.

In ATTAS, it is considered that the Method A is more convenient than other methods for DSS measurements. In this method, the signal amplitude level is set to the minimum amplitude level of the signal generator and increased gradually until the detection system has 10 dB SNR. The applied signal level (L) is read and DSS measurement is specified as L-10.

F. Equipment TEMPEST Zoning

Equipment TEMPEST zoning (ETZ) procedures is given by SDIP-28 [12] standard as well as facility TEMPEST zoning procedures. To assign a TEMPEST zone to an equipment or system, ER test procedures given in SDIP-27/1 is applied [12].

One has to know that ETZ cannot be applied to crypto equipment and transmitters. This means that the Level A tests are out of scope of ETZ procedures. ETZ assignment can be evaluated using the following two methods.

Method 1 compares CE levels of each RED Signal of equipment with the limits and is in practice identical to a SDIP-27/1 Level B/C (ER) test. If CE levels are below the Level B ER limits defined in SDIP-27/1, the equipment is assigned an equipment zone 1. However, if CE levels exceed Level B ER limits defined in SDIP-27/1, but are below the Level C ER limits, the equipment is assigned an equipment zone 2.

Method 2 does not analyze the modulations to be compromising or not, and in worst-case assessment, all peak levels are assumed to be compromising and have to be below the limits. The bandwidth is selected based on the highest data rate of the respective category within the "Bounds on Tunable Overall Detection System Bandwidth" defined in SDIP-27/1. As a result, if peak signal levels are below the Level B ER limits, equipment is assigned equipment zone 1. If peak signal levels exceed Level B ER limits, but are below the Level C ER limits, the equipment is assigned an equipment zone 2. ATTAS implements Method 2 for convenience.

G. Automatic Test Report Builder

Automatic Test Report Builder (ATRB) is developed to generate the report of graphical representation of TEMPEST tests results. The report generation process is carried out in two steps. In the first step, each test result graph is prepared as a report page whenever a related part of the test finished. The information about the test is entered through a user interface and a single page Word report is obtained. In the second step, these single page reports are combined to obtain the report of graphical representation of TEMPEST test results.

IV. EXPERIMENTAL STUDIES

In this section, first, automatic investigations of compromising emanations (CE), a powerful part of the system, is implemented. Second, CE of the LCD monitors are captured and displayed in a user interface.

A. Investigation of CE

In order to show the system performance, we performed two different experiments. First, 300 Hz-3.5 kHz chirp signal, which represents the human voice, is amplitude modulated (Double sideband) with a 10 MHz carrier frequency by a signal generator. The spectrum of the signal is given in Fig. 5.



Fig. 5. AM-modulated chirp signal in 10 MHz.

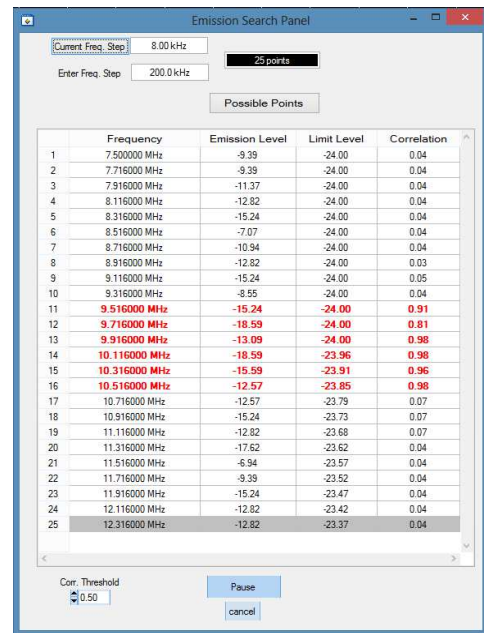


Fig. 6. Automatic CE search table of a chirp signal.

Then this signal is investigated with 200 kHz frequency steps and the result is given in Fig. 6. It is seen that the correlations are very high around 10 MHz and these points are highlighted and shown by red color in the search table. The demodulated signal is digitized with 50 kHz sampling rate for 0.5 second and is shown in scope panel as given in Fig. 7.

Here, the critical point is that the data acquisition time of the demodulated signal should be at least two times the duration of the RED signal. In this case, it is about 2.5 times. In the zoom panel, two signals can be aligned and their correlation can be computed in real time.

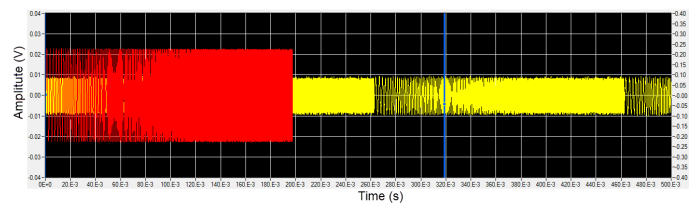


Fig. 7 Capturing the demodulated chirp signal by oscilloscope.

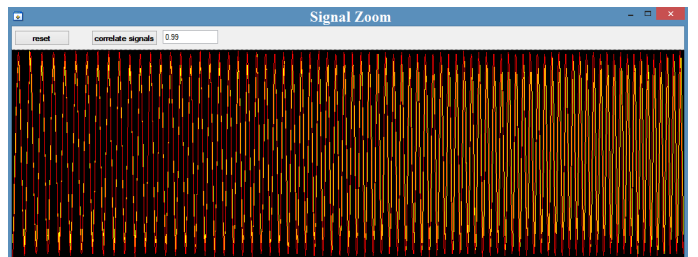


Fig. 8. Zoom Panel and real-time correlation computation.

B. Displaying CE of Video Display Units

The similar CE search procedure is applied to an LCD monitor and correlation result is computed as 66%, which is shown in zoom panel in Fig. 9. In this test setup, log-periodic

antenna is used since the CE of the monitor occurs around 776 MHz. The demodulation bandwidth of the receiver is set to 10 MHz.

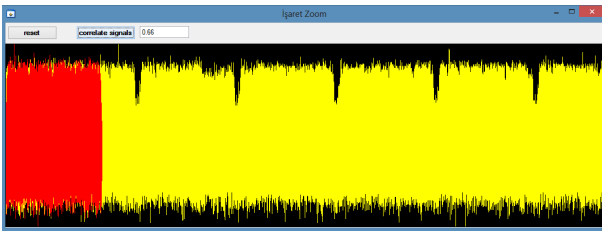


Fig. 9. An LCD Monitor compromising emanation.

In Fig. 10, the one-dimensional data of a frame is transformed to two-dimensional data with the row frequency, which is known by VESA standards [16], and the result is shown in video rendering panel. For more information about compromising emanations of video display units, we refer to [4].

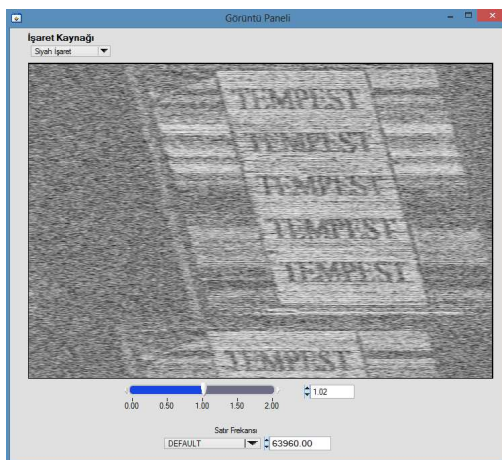


Fig. 10. Video Rendering Panel.

V. CONCLUSION

In this paper, a complete TEMPEST Automatic Test and Analysis System (ATTAS) is developed to improve the test reliability by reducing the testing time. ATTAS includes automatic system calibration unit, test matrix generator and importer, implementation of tunable and nontunable tests, automatic compromising emanations (CE) search, interpretation of the CE with displaying, zooming, rendering, and playing panels. In addition, the measurement of detection system sensitivity, device zoning based on SDIP-27/1, and a report builder of graphical results is achieved by automatically by the system. The system and the software is designed in a modular manner and suitable to update and upgrade devices used. ATTAS has been used successfully in TEMPEST Test Laboratory for almost a year.

Acknowledgments

This study is supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under the project TEMPEST Tests.

Reference

- [1] H. O. Yardley, *The American black chamber*: Naval Institute Press, 1931.
- [2] N. TEMPEST, "1-92," *Compromising Emanations Laboratory Test Requirements*, 1992.
- [3] Standard, "SDIP-27/1: NATO TEMPEST Requirements and Evaluation Procedures [confidential]," 2009.
- [4] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," *University of Cambridge Computer Laboratory, Technical Report, UCAM-CL-TR-577*, 2003.
- [5] W. Van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk?," *Computers & Security*, vol. 4, pp. 269-286, 1985.
- [6] P. Smulders, "The threat of information theft by reception of electromagnetic radiation from RS-232 cables," *Computers & Security*, vol. 9, pp. 53-58, 1990.
- [7] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in *Privacy Enhancing Technologies*, 2005, pp. 88-107.
- [8] 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.
- [9] M. Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," in *USENIX Security Symposium*, 2009, pp. 1-16.
- [10] Y. Du, Y. Lu, and J. Zhang, "NOVEL METHOD TO DETECT AND RECOVER THE KEYSTROKES OF PS/2 KEYBOARD," *Progress In Electromagnetics Research C*, vol. 41, 2013.
- [11] W. Litao and Y. Bin, "Analysis and Measurement on the Electromagnetic Compromising Emanations of Computer Keyboards," in *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, 2011, pp. 640-643.
- [12] Standard, "SDIP-28/1: NATO Zoning Procedures [confidential]," 2005.
- [13] F. Elibol, U. Sarac, and I. Erer, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system," in *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*, 2012, pp. 1767-1771.
- [14] N. E. Koksaldi, I. Olcer, U. Yapanel, and U. Sarac, "SIGNAL PROCESSING APPLICATIONS FOR INFORMATION EXTRACTION FROM THE RADIATION OF VDUs," *National Institute Of Electronics & Cryptology, Gebze, Kocaeli*, vol. 41470.
- [15] H. Fang, "Electromagnetic Information Leakage and its Protection of Computer," presented at the Science Press, Beijing, 1993.
- [16] V. M. T. Standard, "Monitor timing specifications," ed: San Jose: Video Electronics Standards Association, 1998, 1998.