Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers

Ireneusz Kubiak 1-*, Alexandru Boitan 2 and Simona Halunga 3

1 Electromagnetic Compatibility Department, Military Communication Institute, Zegrze Poludniowe 05-130, Poland
2 Special Telecommunications Services, Splaiul Independenței St., Bucharest 060044, Romania; alexandru.boitan@stsnet.ro
3 Telecommunications Department, University Politehnica of Bucharest, Bucharest 060042, Romania; simona.halunga@upb.ro
* Correspondence: i.kubiak@wil.waw.pl

Received: 2 April 2020; Accepted: 15 April 2020; Published: 19 April 2020

Abstract: The main topic of the present paper is the printed text protection against electromagnetic infiltration. There are many solutions to protect such data. One of these methods is the one that uses computer fonts that are characterized by special shapes. The suitability of the solution has to be confirmed by many tests and analyses. An important element of such researches is the class of receiving devices used. In the case of measurements of the valuable emissions arising from electronic data processing of the printed text, typical receivers that are used for measurements of electromagnetic compatibility cannot be used. They have to be dedicated devices for measuring the very low level of signal that arises unintentionally. The sensitivity of the receiver must be very high in wide measuring bands. In addition, in order to assess the method of preventing electromagnetic infiltration, it is important to verify it by independent institutions. An additional advantage is the use of different receivers in the assessment process. This paper presents the results of studies made regarding the suitability of two sets of fonts with special shapes (secure symmetrical and secure asymmetrical) in secure information processing. The analysis of the fonts was based on visual examination, a basic method of preliminary assessment of electromagnetic emissions correlated with processed text information, of the images reproduced from unwanted emissions. The tests were carried out at two independent institutions, Military Communication Institute—Poland, Special Telecommunications Services—Romania, using three different types of receivers: Tempest Test System DSI-1550A, Rohde & Schwarz FSET22 and Rohde & Schwarz FSWT. The images obtained in the two independent laboratories with different setup and test equipment confirmed thus without doubt the possibility of using special fonts as the solution against an effectiveness of electromagnetic infiltration. The above assessment is correct, regardless of the used receiver and the environment of implementation of the secure fonts.

Keywords: electromagnetic eavesdropping; electromagnetic infiltration; valuable emission; TEMPEST font; electromagnetic propagation; electromagnetic devices; electromagnetic measurements; software protection; information security; computers and information processing

1. Introduction

Information protection is an important element of human life, from both a private and a professional standpoint. To protect information that is electronically stored or processed, various methods are used, based on solutions that are not always accepted by all users. Those processes can be a source of
electromagnetic emissions correlated with the processed information, which become fully useful in the electromagnetic infiltration process.

In the TEMPEST evaluation process, all digital signals transferred from the communication ports of the tested equipment are considered to be compromising signals, such as PS/2 port connector [1], USB (Universal Serial Bus ports or peripherals) [2,3], RJ45 modular connector [4], video signals from VGA (Video Graphics Array), DVI (Digital Visual Interface), HDMI (High-Definition Multimedia Interface) and other display ports [5–7] or RS232 serial port [8]. Output devices such as printers [9–12] and video projectors [13] are also being investigated. The video display signal is considered to be the most unsafe in terms of vulnerability to electromagnetic intrusion attacks from all compromising signals that can be emitted by a personal computer. This is also recognized by the TEMPEST procedures [14], which assign to this type of signal the most restrictive corresponding category as a compromising signal. The successive video frames are similar to each other and, for this reason, the video signal has the attributes of a repetitive signal, which means that it is almost periodic [15]. This feature can allow a potential attacker to apply the mediation processes that highlight the video signal, reducing the effect of ambient noise in this way.

The effectiveness of the electromagnetic infiltration can be limited in several ways: limiting levels of electromagnetic emissions correlated (having distinctive features) with processed information [14–17], a disturbance of existing revealing emissions [18,19] or appropriate shaping of the emission source to eliminate features that enable identification e.g., of text data characters [20–22].

TEMPEST protection countermeasures now involve hardware modification of Information Technology and Communications (IT&C) equipment by applying shielding measures (shielded housings and shielding window), power and signal filtering, or modifying printed circuit boards in order to minimize the total amount of the equipment electromagnetic radiation and not only those containing information (compromising emanation). This is reflected in the cost of the shielded equipment, which is often 5–8 times higher than the modified commercial equipment. It is true that the security of sensitive information is related to national security issues and must be applied regardless of the costs involved, but maintaining the level of security of this information with reducing costs is the target of the TEMPEST protection measures, which is specified by official documents as the “protection zone model”.

The disturbance of existing revealing emissions does not lower the levels of these emissions. It introduces additional sources of electromagnetic disturbances, some of which can reach significant levels. This solution is not recommended, due to the deliberate introduction of additional sources of electromagnetic emissions into the environment.

Shaping the sources of such emissions is another method that limits the effectiveness of electromagnetic infiltration. This is achieved by changing the colors of the text and the background. An appropriate selection of color pairs may reduce the effectiveness of the source of unwanted emissions [15,16]. However, this method is not universal from the point of view of application in video standards. A certain properly selected text and background color pairs can be effective for the analogue VGA standard, but, in the case of the digital DVI (HDMI) standard, the efficiency of a color pair may not be so obvious [16].

There is a new proposed method based on computer fonts with specially designed shapes (Figure 1). Font characters shape the electrical signal of each video standard, which is a potential source of emission.

(a)
The TEMPEST measurement procedures involve two successive steps: the first proves the existence of the compromised emanation (CE) generated by the IT&C equipment, but will not be able to extract information from the restored image which represents the target of the TEMPEST domain.

Another important issue is the practical advantages of the method. This assessment is carried out using a special receiver dedicated to the measurement of electromagnetic revealing emissions. The level of these electromagnetic emissions is very low, and the bandwidth of the signals, especially digital ones, is very wide. Therefore, the sensitivity of the measuring receiver must be very high, and the available measurement bands very wide, up to 500 MHz [23–25]. The second method of verifying the graphic sources of revealing emissions is visual analysis. This analysis is based on graphic images that are obtained as a result of the rasterization process of recorded revealing emissions.

The authors are analysing the possibility of data recovery processed by electronic devices by a possible intruder that does not have access to the location in which the equipment is placed, just from spurious electromagnetic emissions. Usually such locations are secured ones, placed under guard, and, if such an intruder appears, they cannot have bulky equipment and suspicious behaviour. They cannot carry a computer or laptop and wait there while it still performs numerical algorithms to identify the data from electromagnetic emissions. That is why the visual method is used, and, as with any method based on human perception, quantitative numerical indicators do not apply. However, many test subjects have been used, and the conclusions regarding the degree of similarity between different letters and numbers written with the secure symmetrical and secure asymmetrical fonts are presented in section 4 [20]. It has been proven that the results obtained based on visual method correspond to the ones that used numerical algorithms for similarity assessment and character recognition algorithms. Moreover, the visual method is widely used in such applications and also imposed by military standards, being the first step of the TEMPEST measurement procedures for the video display signal.

The practical advantages of the new computer fonts in terms of electromagnetic protection of processed text data were carried out by two independent institutions—Military Communication Institute (MCI) and Special Telecommunications Services (STS)—with extensive experience in the study and classification of electromagnetic emissions. This allowed for a reliable evaluation of the fonts and independent method verification.

2. Methods

The verification of the new set of fonts based on visual analysis was carried out in two measurement environments: an anechoic chamber of the laboratory of the MCI and an anechoic chamber of STS. Each laboratory uses a different measuring receiver, which was the purpose of the evaluation of new fonts in the secure processing of text information.

The TEMPEST measurement procedures involve two successive steps: the first proves the existence of the CE on a certain frequency (the image recovery when considering the video signal as CE) and the second is the evaluation of the CE level. The level of the emanation is compared with the limits stipulated by the TEMPEST procedures for the classification of the equipment in a certain risk category
for information security. Therefore, the possibility of image recovery does not automatically mean that equipment under test (EUT) fails the test.

2.1. Military Communication Institute

The tests were carried out inside an anechoic chamber of electromagnetic compatibility laboratory of MCI (Figure 2). A Tempest Test System DSI 1550A receiver and a special set of antennas were used for these tests. The secure fonts were installed on a typical desktop computer with a 24” monitor (1024 × 768, 60 Hz). The monitor was connected to the main unit of the computer by DVI and VGA standard interfaces. The sizes of fonts were equal to 36 points and 24 points. The distance between the antenna and the monitor was equal to 1 m (the distance according to the MIL-STD-461E (F and G)). An electromagnetic emission was measured on a frequency of 860 MHz ($BW = 50$ MHz) [26].

![Figure 2. Communication Institute test bed.](image_url)

2.2. Special Telecommunications Services

The measurements were performed in a TEMPEST laboratory consisting of two shielded enclosures that have a common wall, as illustrated in Figure 3. One of the enclosures is a semi-anechoic chamber (there is no radio absorbent material on the floor) and is actually the testing room. The equipment is positioned in accordance to the American EMC standard, MIL-STD-461E. This standard has many similarities, but also some differences with the test configuration specified by the TEMPEST procedures, but in the end it has the closest configuration of all EMC standards. As TEMPEST procedures are classified, information cannot be disclosed, so we will consider the configuration of this EMC standard as a reference.
The tests were performed with a Fujitsu Siemens laptop, Lifebook C110. The chosen equipment is an older generation laptop and was used with the 220V mains power supply unit. The laptop’s electric charger is usually an electromagnetic noise generator that makes the process of video image recovery more difficult to fulfill. Very often, the emissions of these electric chargers are in the frequency range of up to about 500 MHz. For this reason we selected a much higher recovery frequency, respectively 910 MHz.

It does not matter which EUT is chosen for testing, but to do comparative tests, we also used, besides the analyzed fonts, 2 other common fonts, namely Times New Roman and Arial.

It should be mentioned that, after establishing the reception and the video recovery parameters, only the images displayed by the EUT have been modified, while all the reception parameters and the analysis of the compromising signal remained unchanged until the end of the tests performed. We used a Rohde & Schwarz (R&S) FSET 22 test receiver and specialized TEMPEST analysis software. Unfortunately, we had to crop from the analyzed images the information that includes the video recovery parameters, because it represents sensitive information that we are not allowed to publish. The test receiver parameters are: 10 MHz Resolution Bandwidth (RBW), 50 ms sweep time, SPAN 0 working mode, and narrow filter pre-selector, and internal preamp amplification was 10 dB. The display resolution of the EUT is 1024 × 768 with the refresh rate of 60 Hz. Thus, all the time parameters of the displayed video signal can be found in the VESA Coordinated Video Timings (CVT) Standard, version 1.2 (February 2013): vertical refresh of approximately 48.363 kHz (most important), pixel frequency of 65.0 MHz, front and back porches (horizontally and vertically), the whole line and whole frame duration.

Another interesting discussion would be the size of the font that would be most suitable for use in our tests. Usually documents are edited with size 12, while PowerPoint presentations use size 28 or even larger to be visible to all participants. So, we used the following dimensions: 36, 28, 24, 20, 18, 14 and 12.

3. Results

3.1. Military Communication Institute

The tests were carried out for different sizes of font characters. For the tests, besides the secure fonts, traditional fonts Arial and Times New Roman, were used, such that one could observe more easily the differences between secure fonts and traditional fonts in the protection of text information against electromagnetic eavesdropping.

Additionally visual analyses and correlation analyses were carried out for each secure font. The analyses were based on values of character error rate (CER) [20].

\[
CER = \frac{c + k}{s} = \frac{c + (r - e)}{s} \tag{1}
\]
where:

- $r$—number of wanted characters in the analyzed image,
- $c$—number of incorrectly recognized characters,
- $e$—number of correctly recognized characters,
- $k$—number of unrecognized and wanted characters ($k = r - e$),
- $g$—the number of all characters in the image.

For secure fonts, this parameter has high values in contrast to traditional fonts. This made it impossible to recognize each character of the secure fonts in reconstructed images. To confirm the results and the efficiency of using the secure fonts for electromagnetic protection of processed information against electromagnetic penetration, additional tests were conducted in another laboratory. The results are shown in the next chapter of this paper.

During the first stage of the tests, selected characters of the fonts were displayed on the monitor. The characters were separated by one space each (Figure 4). The solution is not typical for the processing of text data. However, we can observe the shape of each character on the output of Side Channel Attack (SCA) better. For the Arial and Times New Roman fonts, the reading of the characters is not hard.

![Figure 4](image-url)
Figure 4. Reconstruction of the displayed image based on sensitive emissions measurement on frequency 840 MHz (BW = 50 MHz, the size of characters-36 points): (a) Arial font, (b) Times New Roman font, (c) secure asymmetrical font, (d) secure symmetrical font.

For the special fonts, the situation is totally different. The characters in particular sets (‘a’, ‘c’, ‘e’, ‘n’, ‘i’, ‘s’, ‘u’, ‘z’), (‘g’, ‘y’) and (‘b’, ‘h’, ‘k’) look similar. We have to remember that the size of the characters is 24 points. The observed phenomenon will be more beneficial for smaller sizes of the primary characters.

In the second step of tests, the texts were displayed on the monitor. The tests included sequences of characters (size 20 points) without additional spaces. This situation was shown in Figure 5. For Arial and Times New Roman fonts, each character could be selected. The characters of secure fonts remain illegible. Only upper and lower elongations of the characters (e.g., ‘b’, ‘d’, ‘g’, ‘h’, ‘k’) could be recognized.
Figure 5. Reconstruction of the displayed image based on sensitive emissions measurement on frequency 840 MHz ($BW = 50$ MHz, the size of characters—24 points): (a) from the top—secure symmetrical font, secure asymmetrical font, Arial font, (b) from the top—secure symmetrical font, secure asymmetrical font, Times New Roman font.

3.2. Special Telecommunications Services

In Figures 6–11 are shown the test results in the form of reproduced images from registered revealing emissions. The images contain characters of traditional and secure fonts from 12 points up to a size of 36 points. The recording of revealing emissions was made using two receivers, enabling the measurement of very weak electromagnetic emissions correlated with data processed electronically.

It can also be observed that all the characters displayed are intelligible within the restored images, regardless of the font size (Figures 6, 7, 10 and 11). We can consider that the clarity of the recovered images from the compromising radiation corresponding to the Arial font is slightly better than that of the Times New Roman font. We continued with the display of secure asymmetrical and secure symmetrical fonts, choosing the same font size. The image recovery corresponding to these fonts can be seen in Figures 8 and 9.
Figure 6. Image recovered when Arial font was displayed—R&S FSET receiver.

Figure 7. Image recovered when Times New Roman font was displayed—R&S FSET receiver.

Figure 8. Image recovered when secure asymmetrical font was displayed—R&S FSET receiver.

Figure 9. Image recovered when secure symmetrical font was displayed—R&S FSET receiver.
These 3 primary colors, with values between 0 and 255. Thus, the blue color is coded for example "reverse video" option enabled are more intelligible and less tiring for the eyes. Due to the fact that for secure asymmetrical font again and the results are shown in Figure 13.

TEMPEST procedures. Thus, the video recovery process for the font Arial was repeated, but this time the video recovery process, which represents the "worst case scenario" mentioned repeatedly in the 4. Discussion of using TEMPEST fonts are the same, regardless of the reception equipment used in our tests.

Improvement in the quality of the recovered image is observed and, thus, we can say that the effects using the FSWT receiver, we used a gain of 20 dB amplification. However, no significant improvement in the quality of the recovered image is observed and, thus, we can say that the effects of using TEMPEST fonts are the same, regardless of the reception equipment used in our tests.

4. Discussion

In the equipment TEMPEST evaluation, mainly upper case letters are used, because it facilitates the video recovery process, which represents the "worst case scenario" mentioned repeatedly in the TEMPEST procedures. Thus, the video recovery process for the font Arial was repeated, but this time with the use of the upper case letters and numbers, as illustrated in Figure 12. We performed the tests for secure asymmetrical font again and the results are shown in Figure 13.

![Image recovered with Font 28 with blank spaces](Figure 10.png)

**Figure 10.** Image recovered with Font 28 with blank spaces: secure asymmetrical and secure symmetrical—R&S FSWT receiver.

![Image recovered with Times New Roman font](Figure 11.png)

**Figure 11.** Image recovered with Times New Roman font—R&S FSWT receiver.

In Figures 10 and 11, we have illustrated the recovery image results obtained by using the FSWT receiver produced by the Rohde&Schwarz Company, which is the latest TEMPEST receiver model released on the market by the German company. This equipment comes with the raster module built in. It is true that, when using the FSET22 receiver, we allocated about 30 minutes to find the optimal video recovery parameters, while when using the FSWT receiver, we solved the same objective with five clicks. This is the feature of the German manufacturer, as well as the level of integration for the pre-selection filters. The only difference compared to the first part of the tests performed is that when using the FSWT receiver, we used a gain of 20 dB amplification. However, no significant improvement in the quality of the recovered image is observed and, thus, we can say that the effects of using TEMPEST fonts are the same, regardless of the reception equipment used in our tests.

![Image recovered when Arial font with upper case letters was displayed](Figure 12.png)

**Figure 12.** Image recovered when Arial font with upper case letters was displayed.
Color coding in RGB format (red, green and blue) is done by combining in some proportions these 3 primary colors, with values between 0 and 255. Thus, the blue color is coded for example [0,0,255] or "0000FF" in hexadecimal format (HEX) while black is represented by [0,0,0] or "000000" (HEX) and the white color of [255,255,255] or "FFFFFF" (HEX). The inverted video option practically means the reversal of the white color with the black, meaning the consideration of the values [255,255,255] for black and [0,0,0], for white respectively. So it does not represent an additional processing of the video CE signal, but it is only the option for a TEMPEST engineer regarding the visualization of the restored image. In the opinion of our specialists, the images restored with the “reverse video” option enabled are more intelligible and less tiring for the eyes. Due to the fact that the TEMPEST specialist spends several hours each working day with such images displayed, this technical aspect related to the working mode is very important to them. The restored images illustrated in Figures 6–13 were performed with the “reverse video” option enabled. Without activating this setting, the image shown in Figure 14 is obtained.

![Image recovered when secure asymmetrical font with upper case letters was displayed.](image1.png)

**Figure 13.** Image recovered when secure asymmetrical font with upper case letters was displayed.

We can consider that the text is intelligible for the font size of 36, 28 and 24 and not for all the letters, this statement being valid only for size 36 in case of Arabic numerals, and even at this size, the number 2 can be easily confused with the number 8. However, it can be observed that the date of the measurements cannot be understood for the secure asymmetrical font with a size less than 28 and for the secure symmetrical font with a size less than 24. We consider that for the font size 12, no alphanumeric character is intelligible, regardless of the font considered, secure asymmetrical or secure symmetrical. It is also true that the tested fonts are difficult to track even in the Word Office editing environment and that the human operator needs an adaptation period to use these fonts.

In conclusion, we consider that the fonts are efficient in terms of resistance to the video recovery process and that the secure asymmetrical font is more efficient than the secure symmetrical one, although the characters of the secure asymmetrical font have been restored with a better contrast. The documents edited with size 12 are impossible to recover if any of these fonts would be used.
Next, we considered that dimension 24 represents the intelligibility limit for the two TEMPEST fonts analyzed. Thus, we continued to use as a test video signal a page with size 24, corresponding to all four previously used fonts. The image recovery results corresponding to this video signal can be seen in Figure 15.

![Figure 15. Image recovered with Font 24: Arial, Times New Roman, secure asymmetrical and secure symmetrical.](image1)

Here, we can identify all the numbers for the secure symmetrical font and partially for the secure asymmetrical. The most readable characters are ‘b’, ‘g’, ‘k’, ‘p’, ‘q’, ‘s’ and ‘t’, while the numbers 2, 3 and 4 can be identified, even for the secure asymmetrical font. The characters ‘a’, ‘c’, ‘n’, ‘o’, ‘u’ and ‘v’ can be easily confused with each other (they have an almost identical shape in the restored image) and also the letters ‘g’ and ‘y’.

Next, we increased the font size to see if the quality of the restored image is improved and the results are not positive in this sense (the text is not intelligible), as can be seen in Figure 16.

![Figure 16. Image recovered with Font 28: Arial, Times New Roman, secure asymmetrical and secure symmetrical.](image2)

For intelligibility reasons, we have introduced blank spaces between alphanumeric characters written with secure asymmetrical and secure symmetrical fonts. The result can be seen in Figure 17. In this case, we consider that the letters ‘b’, ‘c’, ‘d’, ‘f’, ‘p’, ‘q’, ‘r’, ‘s’ and ‘t’ can be identified for the secure asymmetrical font and the letters ‘b’, ‘f’, ‘m’, ‘p’, ‘q’, ‘r’, ‘s’ and ‘t’ for the secure symmetrical font.

The numbers from 1 to 7 can be identified for the secure symmetrical font, while the secure asymmetrical font makes it impossible to identify the numbers 5 and 6.

![Figure 17. Image recovered with Font 28 with blank spaces: secure asymmetrical and secure symmetrical.](image3)
As we mentioned before, we can conclude that secure asymmetrical font is safer than secure symmetrical and for this reason we repeated the test in which all the alphanumeric characters were displayed with the fonts Arial, Times New Roman (TNR) and secure asymmetrical with dimension 28 (we skipped over dimension 24), as illustrated in Figure 18.

![Figure 18. Font 28: Arial, TNR and secure asymmetrical—upper case.](image-url)

We can observe in Figure 18 that the fonts Arial and Times New Roman are 100% intelligible, while the secure asymmetrical font is not intelligible at all. We have further introduced blank spaces between alphanumeric characters to increase the degree of intelligibility, as illustrated in Figure 19.

Our attempt was partially successful, meaning that the letters ‘C’, ‘E’, ‘F’, ‘G’, ‘L’, ‘P’ and ‘T’ are 30% intelligible, as well as the numbers ‘5’, ‘6’ and ‘7’. Next, we wrote the alphanumeric characters with bold and the result can be seen in Figure 20. As we can see, the level of intelligibility for the secure asymmetrical font does not increase compared to Figure 19.

Since we were not successful in understanding the information written with secure asymmetrical font contained in the video restorations illustrated above, we increased the font to the maximum possible size from our point of view, respectively size 72. We have also left the font size 36 and 28 for comparison reasons and the result is shown in Figure 21.

In order to analyze the characteristics of each alphanumeric character of the secure asymmetrical font, we continued the tests only with the display of the size 72 characters and numbers, both for upper and lower case letters, as can be seen in Figure 22a–c.

![Figure 19. Font 28 with blank spaces: Arial, TNR and secure asymmetrical.](image-url)
From Figure 22, we can observe that certain alphanumeric characters have similar shape characteristics and can be very easily confused between each other if they are not even identical:

1. lower case letters that have similar shape (Figure 22a)
   - the letters ‘a’, ‘c’ and ‘o’;
   - the letters ‘I’, ‘j’ and ‘r’;
   - the letters ‘l’ and ‘t’;
   - the letters ‘g’ and ‘y’.

2. upper case letters that have similar shape (Figure 22b)
   - the letters ‘A’, ‘B’, ‘D’, ‘O’ and ‘Q’;
   - the letters ‘I’ and ‘J’.

3. the numerical characters can be differentiated between each other, as we can see in Figure 22c.

   Additionally, some numbers can be easily confused with the capital letters as follows: ‘2’ with ‘Z’, ‘I’ with ‘I’ and ‘8’ with ‘B’.
Appropriate tests were carried out for VGA standard. The standard is still very popular in classified systems, because it has a higher resistance to electromagnetic infiltration than the DVI standard. Analyzing Figure 23 and the previous Figures, it can be observed that the new solution in form of secure fonts is a universal one. The new approach could be effective for both the analogue and the digital video standards.
5. Conclusions

This article presents the results of research and analysis of the possibilities of using secure fonts (secure symmetrical and secure asymmetrical) in the protection of processed text data against electromagnetic infiltration. The analyses were based on the visual method as the main method in the classification process of revealing emissions.

The presented secure fonts are a new and evolving method that can support the protection of text data against electromagnetic eavesdropping. Any new solution that can decide on information security must be subject to verification. The best approach in this case is to assess the effectiveness of the method by independent institutions, which also have various measuring devices. Thus, it is possible to carry out independent analyses, and their results can fully confirm or contradict the suitability of the methods in the area of application under consideration.

The fonts presented in this paper can be applied as a security measure against electromagnetic compromising emissions, by applying the security policies that have to be applied to the computer and communication systems.

The tests of secure fonts were carried out at two independent institutions: Military Communications Institute (Poland) and Special Telecommunications Services (Romania). These institutions used various receiving systems (Military Communications Institute: Tempest Test System DSI 1550A; Special Telecommunications Services: Rohde&Schwarz FSET22 and Rohde&Schwarz FSWT), which additionally confirmed the effectiveness of the new proposed method. The tests were carried out in anechoic chambers. The source of unwanted emissions was a typical stationary computer set (in case of MCI) and a portable computer (in case of STS). In each case, revealing emissions were detected, which were registered and rasterized. The images obtained in this way showed the superiority of the secure fonts over traditional ones in the field of protection of text information against electromagnetic penetration. This applies to cases when the font character size was not larger than 24 points. Character recognition is possible for larger sizes. For traditional fonts, the text was readable for virtually any size of characters.

The conclusions are also true for analogue graphic standard. In Figure 23, each considered font is presented. The size of characters was equal to 14 points and the text written by using secure fonts is very difficult to read.

The presented method of using secure fonts in the protection of text data against electromagnetic infiltration will still be developed in the future. The fonts must be fully usable, i.e., contain the required characters for the full editing of text documents.

The main originality of the paper stands in the use of the secure symmetrical and secure asymmetrical sets of characters and numbers that were patented by the Polish Office Pattern in the form of the Industrial Design (No. 24487) and Patent (No. 231691). We propose the use of these fonts
to be introduced as one of the official TEMPEST countermeasures in the classified NATO documents, that impose the regulations of the activities involved in this technical field and which represent national security measures for the IT equipment of each Member State (NATO and EU). Their security have been tested by the MCI, Poland, in their laboratory, but here it is the first time when they are also checked in STS, Romania, in an independent laboratory with a different setup and test equipment. Since in the two testing environments there have been obtained similar results, that assess the fact that the secure symmetrical and secure asymmetrical sets of characters and numbers are less vulnerable to interception through revealing electromagnetic emissions. We consider this to be the beginning of a long process of EU and/or NATO endorsement of this TEMPEST protection countermeasure.

6. Patents

The secure symmetrical and the secure asymmetrical fonts obtained the protection of Polish Office Pattern in the form of the Industrial Design (No. 24487) and Patent (No. 231691).

**Author Contributions:** Conceptualization, I.K., A.B. and S.H.; methodology, I.K. and A.B.; software, I.K. and A.B.; validation, I.K. and A.B.; formal analysis, I.K. and A.B.; investigation, I.K. and A.B.; resources, I.K., A.B. and S.H.; writing—original draft preparation, I.K., A.B. and S.H.; writing—review and editing, I.K., A.B. and S.H.; visualization, I.K. and A.B.; supervision, I.K. and S.H.; project administration, I.K. and S.H.; All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**

1. Vuagnoux, M.; Pasini, S. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In Proceedings of the 18th Conference on USENIX Security Symposium SSYM‘09, Montreal, QC, Canada, 10–14 August 2009; USENIX Association: Berkley, CA, USA, 2009; pp. 1–16.

2. Boitan, A.; Bărtusică, R.; Halunga, S.; Popescu, M.; Ionuţă, I. Compromising Electromagnetic Emanations of Wired USB Keyboards. In Proceedings of the Third International Conference on Future Access Enablers for Ubiquitous and Intelligent Infrastructures (FABULOUS), Bucharest, Romania, 12–14 October 2017; Springer: Cham, Switzerland, 2017.

3. Boitan, A.; Halunga, S.; Bindar, V.; Fratu, O. Compromising Electromagnetic Emanations of USB Mass Storage Devices. In press. Available online: https://doi.org/10.1007/s11277-020-07329-8 (accessed on 14 April 2020).

4. Wample, B.; Uluagac, S.; Beyah, R. Information Leakage in Encrypted IP Video Traffic. In Proceedings of the IEEE Global Communications Conference GLOBECOM, San Diego, CA, USA, 6–10 December 2015; IEEE: Piscataway, NJ, USA, 2015. [CrossRef]

5. Kuhn, M.G. Compromising Emanations: Eavesdropping Risks of Computer Displays; Technical Report No. 577; UCAM-CL-TR-577; University of Cambridge: Cambridge, UK, 2004.

6. Nan, Z.; Yinghua, L.; Qiang, C.; Yiyeng, W. Investigation of Unintentional Video Emanations from a VGA Connector in the Desktop Computers. IEEE Trans. Electromagn. Compat. 2017, 59, 1826–1834. [CrossRef]

7. Macovei, A.; Butnariu, V.; Boitan, A.; Rosu, G.; Trip, B.; Halunga, S. Detection of Electromagnetic Emissions Transmitted on The Power Line Through Electrical Conduction. In Proceedings of the International Conference on Applied and Theoretical Electricity (ICATE), Craiova, Romania, 4–6 October 2018; IEEE: Piscataway, NJ, USA, 2018. [CrossRef]

8. Smulders, P. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Comput. Secur. 2002, 9. [CrossRef]

9. Boitan, A.; Halunga, S.; Bărtusică, R.; Bindar, V. Video signal recovery from the laser printer LCD display. Microelectron. Nanotechnol. 2018, 10977. [CrossRef]

10. Kubiak, I.; Loughry, J. LED Arrays of Laser Printers as Valuable Sources of Electromagnetic Waves for Acquisition of Graphic Data. Electronics 2019, 8, 1078. [CrossRef]

11. Grzesiak, K.; Przybysz, A. Emission Security of Laser Printers. In Concepts and Implementations for Innovative Military Communications and Information Technologies; Military University of Technology: Warsaw, Poland, 2010.
12. Kubiak, I. Laser printer as a source of sensitive emissions. *Turk. J. Electr. Eng. Comput. Sci.* 2018, 26, 1354–1366. [CrossRef]

13. Boitan, A.; Bătușică, R.; Halunga, S.; Fratu, O. Electromagnetic Vulnerabilities of LCD Projectors. In Proceedings of the 6th Conference on the Engineering of Computer Based Systems, Bucharest, Romania, 2–3 September 2019; University Politechnica of Bucharest: Bucharest, Romania, 2019; pp. 1–6. [CrossRef]

14. Lee, H.K.; Kim, J.H.; Kim, S.C. Emission Security Limits for Compromising Emanations Using Electromagnetic Emanation Security Channel Analysis. *IEICE Trans. Commun.* 2013, 96, 2639–2649. [CrossRef]

15. Kubiak, I. Video signal level (colour intensity) and effectiveness of electromagnetic infiltration. *Bull. Pol. Acad. Sci.* 2016, 64, 2007–2018. [CrossRef]

16. Kubiak, I. Influence of the method of colors on levels of electromagnetic emissions from video standards. *IEEE Trans. Electromagn. Comput.* 2018, 61, 1–9. [CrossRef]

17. Idita, A.; Butnariu, V.; Rosu, G.; Trip, B.; Boitan, A.; Băltag, O. Study of Shielding Effectiveness on Spurious Emissions of Information Systems by Means of Metallic and Carbon Powder Screens. In Proceedings of the International Conference on Applied and Theoretical Electricity (ICATE), Craiova, Romania, 4–6 October 2018; IEEE: Piscataway, NJ, USA, 2018. [CrossRef]

18. Tajima, K.; Ishikawa, R.; Mori, T.; Suzuki, Y.; Takaya, K. A Study on Risk Evaluation of Countermeasure Technique for Preventing Electromagnetic Information Leakage From ITE. In Proceedings of the International Symposium on Electromagnetic Compatibility—EMC, Angers, France, 4–7 September 2017; IEEE: Piscataway, NJ, USA, 2017. [CrossRef]

19. International Telecommunications Union. *Mitigation Methods Against Electromagnetic Security Threats; Series K: Protection Against Interference; Recommendation K.115, 11/2015; Telecommunication Standardization Sector of ITU: Geneva, Switzerland, 2015.

20. Kubiak, I. Font Design—Shape Processing of Text Information Structures in the Process of Non-Invasive Data Acquisition. *Computers* 2019, 8, 70. [CrossRef]

21. Ketenci, S.; Kayikcioglu, T.; Gangal, A. Recognition of Sign Language Numbers via Electromyography Signals. In Proceedings of the 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16–19 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 2593–2596.

22. Bahare, J.; Abdolah, C. Persian Sign Language Recognition Using Radial Distance and Fourier Transform. *Int. J. Image Graph. Signal Process.* 2014, 1, 40–46. [CrossRef]

23. Yuan, K.; Grassi, F.; Spadacini, G.; Pignari, S.A. Crosstalk-Sensitive Loops and Reconstruction Algorithms to Eavesdrop Digital Signals Transmitted Along Differential Interconnects. *IEEE Trans. Electromagn. Comput.* 2017, 59, 256–265. [CrossRef]

24. Xie, C.H.; Wang, T.; Hao, X.; Yang, M.; Zhu, Y.; Li, Y. Localization and Frequency Identification of Large-Range Wide-Band Electromagnetic Interference Sources in Electromagnetic Imaging System. *Electronics* 2019, 8, 499. [CrossRef]

25. Ko, W.L. Time Domain Solution of Electromagnetic Problems. *Electromagnetics* 1992, 12, 403–433. [CrossRef]

26. Cihan, U.; Aşık, U.; Cantürk, K.; Sarhat, S.; Bilal, K.; Ugur, S. Automatic tempest test and analysis system design. *Int. J. Cryptogr. Inf. Secur.* 2014, 4. [CrossRef]