

TEMPEST Font Protects Text Data against RF Electromagnetic Attack

Ireneusz KUBIAK

Abstract: Nowadays an electromagnetic penetration process of electronic devices has a big significance. Processed information in electronic form could be protected in different ways. Very often used methods limit the levels of valuable emissions. But such methods could not always be implemented in commercial devices. A new solution (soft tempest) is proposed. The solution is based on TEMPEST font. The font does not possess distinctive features. This phenomenon causes that at an output of Side Channel Attack the possibilities of recognition of each character which appears on the reconstructed image for sources in the form of graphic lines (VGA and DVI) are limited. In this way the TEMPEST font protects processed data against electromagnetic penetration not only for VGA and DVI standards. The data are protected during printing them on laser printers too.

Keywords: digital image processing; digital signal processing; eavesdropping process; protection of information; soft TEMPEST; valuable (sensitive) emission

1 INTRODUCTION

Protection of information against electromagnetic penetration process is a very important challenge. To protect information various methods and solutions are used. Most popular solution is a restricted access to space where classified information is processed [1, 2]. However, electronic devices are sources of electromagnetic emissions. These emissions could be correlated with processed information. Then the data could be received in a non-invasive way. The non-invasive data acquisition is imperceptible for owner of such data [3-6].

The most spectacular phenomenon consists in the opportunity of displaying acquired data in a form that is comprehensible for a person. This in particular concerns sources of emissions in the shape of graphic lines, e.g. VGA or DVI standards [7-12] and laser systems of typical laser printers [13-16].

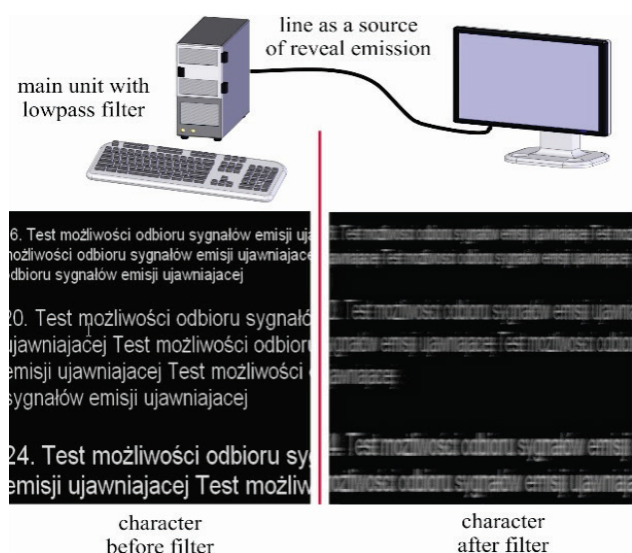


Figure 1 Influence of filtering of the electric signal on the form of text data-VGA standard (filter with capacity 5 nF, image resolution 1024 x 768, image restoration 60 Hz)

Because the non-invasive data acquisition is very dangerous, the sources of electromagnetic emissions correlated with processed graphic information are the subject of analyses and tests. There are searched the best and the most effective methods which could protect

processed information against electromagnetic penetration. A shielding is a very popular method which limits levels of electromagnetic disturbances from IT devices [2, 17]. Other method consists in filtering electric video signals Fig. 1, [18, 19].

arial font is the basis for the set of fonts, it is easily identified in the electromagnetic infiltration process.

a)
arial font is the basis for the set of fonts, it is easily identified in the electromagnetic infiltration process.

b)
l|l|l|l|l| l| Hi lili| för Hi lii
l, l il iilü identified elGGtromagneiie
iEifjtlliiön

c)
atial i©rat is í6e basis f@£ île set ©í
í©rats, it is easily id s ratified ira tie
eíeetísmagraetie iraiift«ati©ra
gíseess.

d)
Figure 2 Sang Mun fonts and effectiveness of Optical Character Recognition program: a) main document-Sang Mun Noise font, b) main document-Sang Mun Flower, c) document after operation of OCR program-scanned document from Fig. 2a, d) document after operation of OCR program-scanned document from Fig. 2b

Markus Kuhn proposed a solution consisting of a filtering system applied on video standard of desk computer. Markus Kuhn's approach limits over 20%, 30%, 40% and 50% of signal spectrum. This produces the desired effect.

However, the limitation of signal spectrum causes that

reconstructed characters on an "eavesdropped" screen are illegible Fig. 1. Legibility level of information is very low. In this case a very important problem has to be mentioned. The filtering of video signal is not a solution which could be applied to different graphic sources of sensitive emissions. It is effective in case of analog standard. The problem is connected with the resolution of working of the monitor. If the resolution is changed the parameters of video signal are changed too. The phenomenon causes that one filter is not effective in all ranges of working resolution of monitor.

DVI standard as a digital standard is sensitive to changing of electric parameters of video signal. The changes of the parameters cause disturbances of displayed picture on the screen. To protect DVI standard a method based on colors of a text and a background could be used [7, 17].

The shape of video signal can be formed by appropriate shape of computer font. Such approach is proposed by Sang Mun. His idea is connected with new fonts which have additional graphic elements (e.g. noise, flowers, Fig. 2a and Fig. 2b). The Arial font is the basis for the set of fonts. However Sang Mun's fonts are easily identified in the electromagnetic eavesdropping process (next chapter of the paper). But characters of these fonts are not recognized by Optical Character Recognition (OCR) programs (Fig. 2c and Fig. 2d).

To prove usefulness of the new solution in the form of TEMPEST font a lot of tests were carried out. The level of protection of information against electromagnetic penetration was verified. A method of correlation between letters at Side Channel Attack (SCA) output was used.

There are commercial fonts, which could have similar features as TEMPEST font. Such font is Null Pointer font Fig. 3, [20]. Null Pointer font is a typical computer font which has the characteristics of TEMPEST font. Each character of this font is built only from horizontal and vertical lines. But widths of these lines are various. The phenomenon allows easily identifying each character of the font included in reconstructed image.

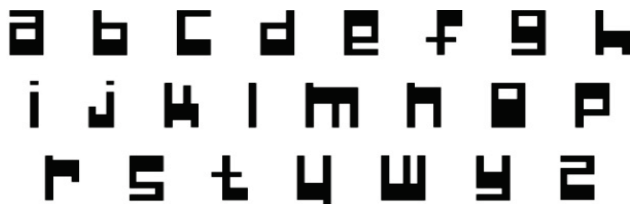


Figure 3 The letters of the Null Pointer font

In the paper a new method is presented to protect the processed text information against electromagnetic penetration. The method uses soft solution based on TEMPEST font [21]. New idea is effective for different graphic sources of sensitive emissions, e.g. DVI and VGA video standards, different types of laser printers [16].

2 A COMPUTER TEMPEST FONT

The design of safe font takes into account the features of the SCA for electromagnetic emissions. The SCA has the features of a high-pass filter:

$$x'(t) = \lim_{\Delta t \rightarrow 0} \frac{x(t + \Delta t) - x(t)}{\Delta t} + s(t) \quad (1)$$

where: $x'(t)$ -signal $x(t)$ at the output of the SCA, $x(t)$ -the reveal emission signal at the input of the SCA, $s(t)$ -natural noise and disturbances inside of the SCA.

Therefore, in reconstructed images only vertical and diagonal edges of graphic shapes (in particular of letters) are visible. These lines correspond to impulses (a rising edge of impulse, a trailing edge of impulse) which decide about displaying of graphic shapes. Taking into account these features the TEMPEST font was proposed. The font was called Safe Symmetrical font Fig. 4. It is one of three collections of TEMPEST fonts (Symmetrical, Asymmetrical and Simple fonts). The names of these fonts are connected with the shapes of letters. For example letters of Safe Symmetrical font are built from vertical lines of the same thickness but different than horizontal lines. For the Asymmetrical Safe font the thicknesses of vertical lines are different. Additionally letters of Simple Safe font are built from vertical and horizontal lines of the same thickness. The fonts are characterized by different levels of legibility and they could be used interchangeably. I carried out a questionnaire concerning legibility of safe fonts and traditional fonts. The new fonts did not get very bad notes. Additionally the protection level against electromagnetic eavesdropping is compared.

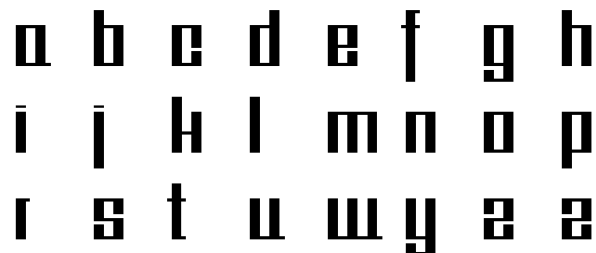


Figure 4 The characters of Symmetrical Safe font

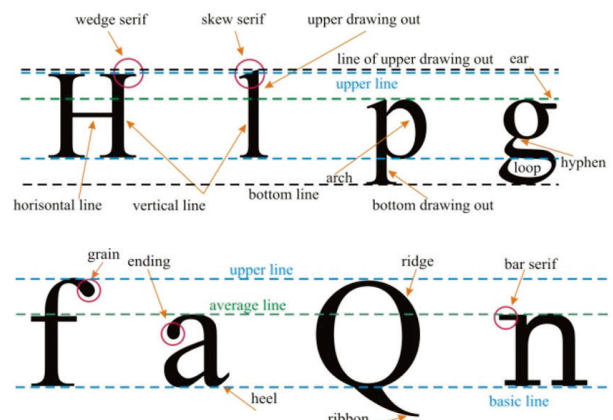


Figure 5 Distinctive features of letters

The construction of Safe Symmetrical font is connected with maximizing the similarity of inter-characters. It is possible because letters of the font do not have distinctive features. In such case given character could be recognized as other character. Such phenomenon can occur in case of every source of valuable emission which is correlated with processed graphic information, e.g. VGA analog standard, DVI digital standard, laser

printers.

Every letter and digit of the font only includes various widths of vertical and horizontal lines. Some basic characteristics of two-element writing have been retained:

- a narrower horizontal line is found in upper and lower parts of letter (for several letters the narrower line exists in the middle part of letter),
 - a wide vertical line is found on the left and right sides of a character,
 - none of the characters bear any decorative elements
- Fig. 5.

For the tests of valuable emissions connected with safe font the TEMPEST Test System DSI-1550A was used. The receiver has a video output interface. The interface makes possible record of the valuable emissions. This is, however, a signal module. Therefore the reconstructed images include only vertical and diagonal edges of letters according to [2]:

$$x''(t) = \left| \lim_{\Delta t \rightarrow 0} \frac{x(t + \Delta t) - x(t)}{\Delta t} + s(t) \right| \quad (2)$$

The purpose of the design of individual letters was maximization of similarity between the letters. Simultaneously the letters should be distinguishable to guarantee smooth reading.

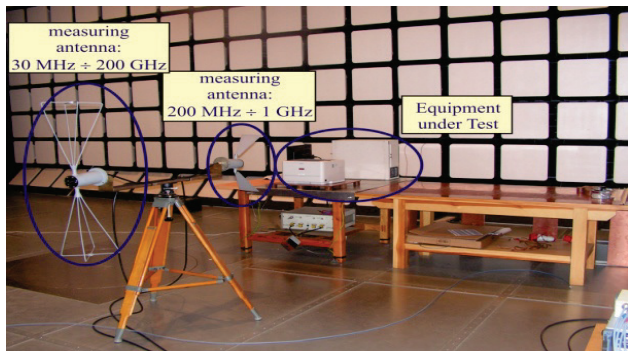


Figure 6 Real measuring system

Additionally widths of the letters of safe font should be comparable with widths of letters of traditional fonts. Then the statistical parameters numbers of letters and spaces per sheet of paper will be met.

The tests were carried out in ideal measurement conditions (for the tests the semi-anechoic chamber was used, Fig. 6).

3 INTER-CHARACTER CORRELATION OF COMPUTER FONTS

3.1 The Input of the Side Channel Attack

The inter-character correlation for individual letters was calculated for respective fragments of the analyzed image. Each fragment including one letter was compared with a pattern which included searched letter according to:

$$R_{j,i}^z = \frac{\sum_{n=0}^{N_w-1} \sum_{m=0}^{M_w-1} A_{n,m} \cdot B_{n,m}}{\sqrt{\sum_{n=0}^{N_w-1} \sum_{m=0}^{M_w-1} A_{n,m}^2 \cdot \sum_{n=0}^{N_w-1} \sum_{m=0}^{M_w-1} B_{n,m}^2}} \quad (3)$$

where:

$$A_{n,m} = x_{n+j \cdot N_w, m+i \cdot N_w} - \bar{x}_{j,i} \quad (4)$$

$$B_{n,m} = y_{n,m} - \bar{y} \quad (5)$$

$$\bar{x}_{j,i} = \frac{1}{N_w \cdot M_w} \sum_{n=0}^{N_w-1} \sum_{m=0}^{M_w-1} x_{n+j \cdot N_w, m+i \cdot M_w} \quad (6)$$

$$\bar{y} = \frac{1}{N_w \cdot M_w} \sum_{n=0}^{N_w-1} \sum_{m=0}^{M_w-1} x_{n,m} \quad (7)$$

and $0 \leq j \leq b - 1$; $0 \leq i \leq d - 1$; $b = N_d/N_w$ row number of correlation image; $d = M_d/M_w$ column number of correlation image; $x_{n,m}$ is pixel amplitudes of analyzed image with letters of alphabet; $y_{n,m}$ is pixel amplitudes of pattern image (single letters of alphabet); M_a is column number of analyzed image with characters of alphabet; N_a is row number of analyzed image with characters of alphabet; M_w is column number of pattern image (single letters of alphabet); N_w is row number of pattern image (single letters of alphabet); I is number of column of correlation image; m is number of column of pattern image (single letters of alphabet); j is number of row of correlation image; n is number of row of pattern image (single letters of alphabet).

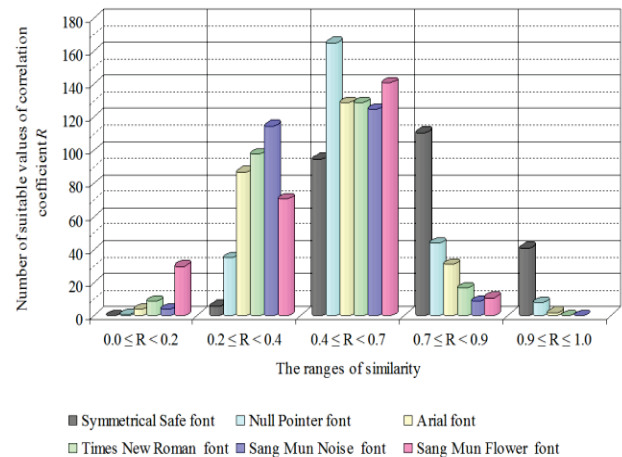


Figure 7 The number of the values of inter-character correlation R^z for appropriate ranges of similarity on the input of the SCA

Relation (3) was used both for the inter-character correlation calculated at SCA input and output. High R^z values make distinctive features of given characters partly disappear at SCA input. Consequently, it becomes impossible to visually recognize letters at SCA output and R^z values do not allow to correctly mark a letter in a location where it is found. In such case the phenomenon is defined by high values of Character Error Rate.

The values of the inter-character correlation (3) are shown in Fig. 7. The similarity between characters of safe font is higher than other fonts. Therefore the safe font could be used to protection classified information against the non-invasive acquisition. Graphic forms of the values of correlation coefficient R for selected characters of analyzed fonts are shown in Fig. 8.

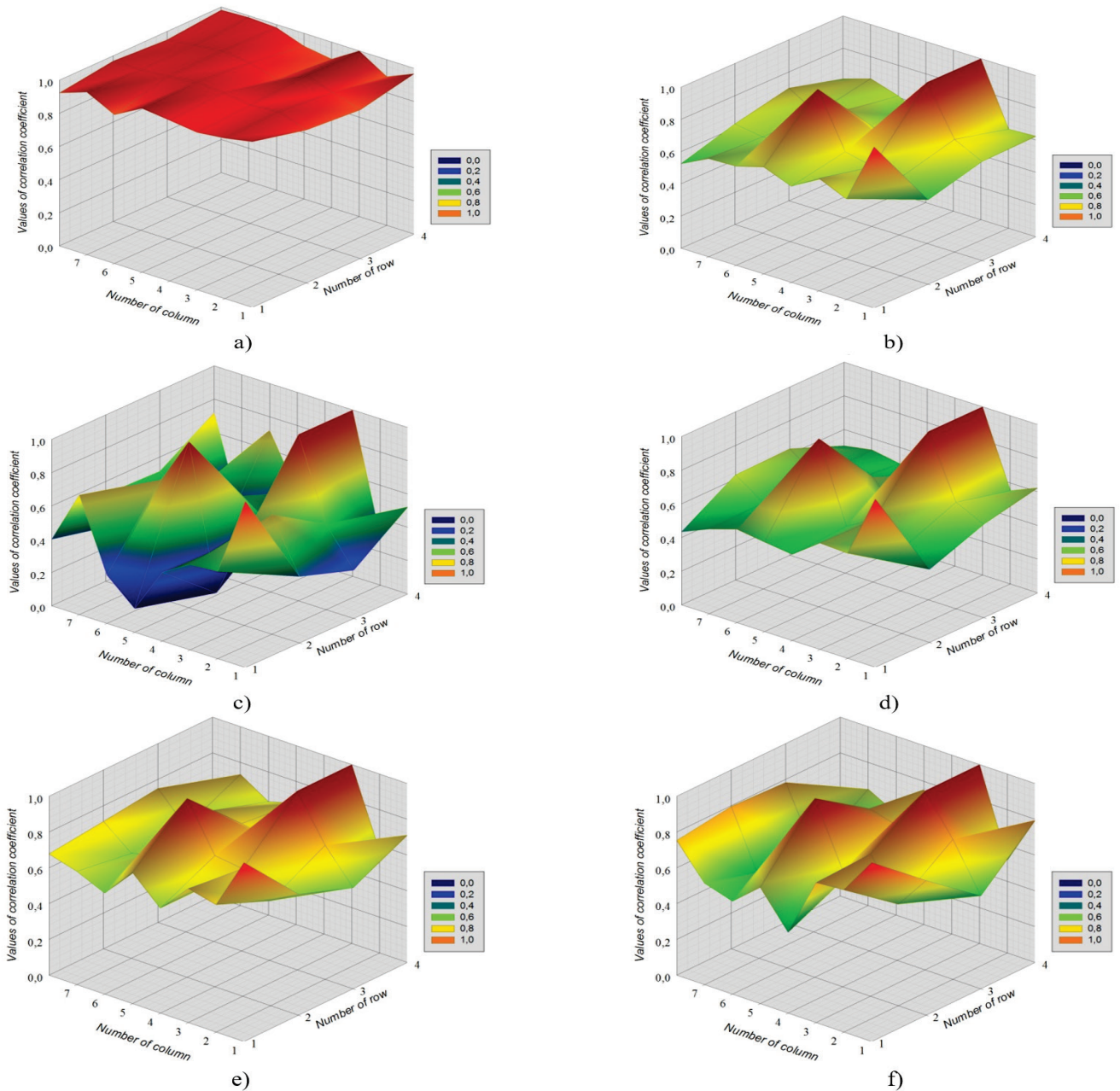


Figure 8 Graphic forms of the values of correlation coefficient R for selected characters of analyzed fonts, character "a" as a pattern image: a) Safe Symmetrical font, b) Arial font, c) Times New Roman font, d) Sang Mun Noise font, e) Sang Mun Flower font, f) Null Pointer font

a c e n o p u z
 z u c o a u n c
 p e a z c o n e
 c p a p z u o u

Figure 9 A matrix of selected characters

The selected characters created a matrix Fig. 9. The distribution of the selected characters in the matrix was random. We can notice that the values of maxima of correlation coefficient R^Z for discordance of characters (discordance of pattern image and analyzed fragment of reconstructed image) are a little smaller than the values of correlation coefficient R^Z for conformity of characters. Of course it is true only for safe font. For other fonts the differences are bigger. The situation makes possible to

recognize almost each character of these fonts in a reconstructed image.

3.2 The Output of the Side Channel Attack

The usefulness of the safe font in counteracting the eavesdropping process was tested using visual method. In this case the visual method was selected because graphic lines of video standards and laser printer were sources of valuable emissions. Moreover the visual method was supported by coefficient of inter-character correlation and values of CER [22]. The values of the inter-character correlation were calculated according to (3). Obtained results are shown in Tab. 1, Tab. 2 and Tab. 3 and in Fig. 10. The values of inter-character correlation are higher for TEMPEST font than for traditional fonts. The second and the third range of inter-character correlation include most values for TEMPEST font in contrast to traditional fonts, Sang Mun fonts and Null Pointer font.

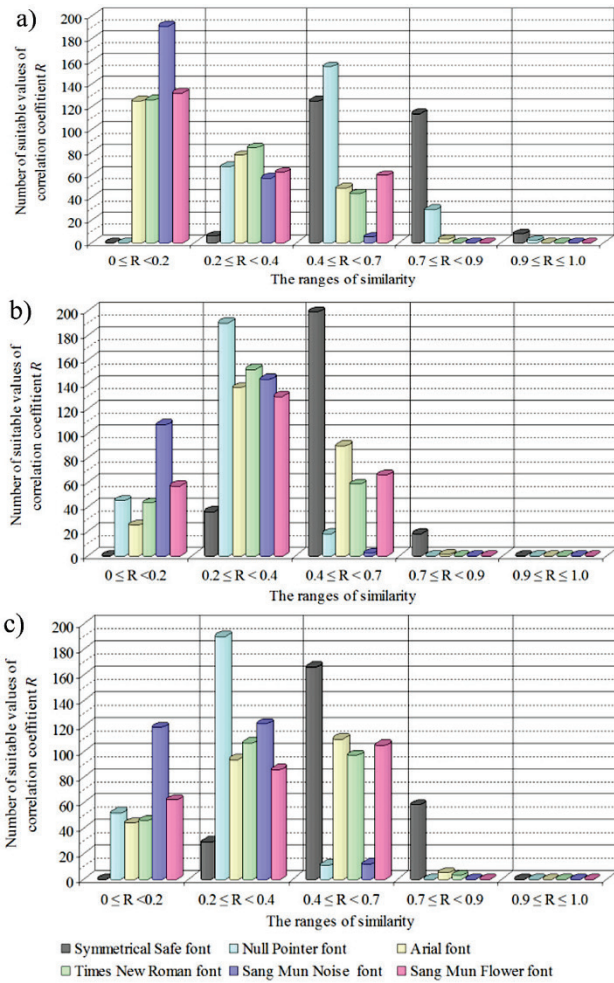


Figure 10 The number of the values of the inter-character correlation for each range of relationship: a) analog standard, b) digital standard, c) laser printer

Table 1 The number of values of the inter-character correlation for each range of relationship (VGA standard, reconstructed characters)

| The value of character correlation coefficient R^2 | Number of relationships | | | | | |
|--|-------------------------|-----|-----|-----|-----|-----|
| | 1) | 2) | 3) | 4) | 5) | 6) |
| $0.0 \leq R < 0.2$ lack relationship | 0 | 125 | 126 | 191 | 132 | 0 |
| $0.2 \leq R < 0.4$ weak relationship | 6 | 77 | 84 | 57 | 62 | 67 |
| $0.4 \leq R < 0.7$ moderate relationship | 125 | 48 | 43 | 5 | 59 | 155 |
| $0.7 \leq R < 0.9$ rather strong relationship | 114 | 3 | 0 | 0 | 0 | 29 |
| $0.9 \leq R \leq 1.0$ very strong relationship | 8 | 0 | 0 | 0 | 0 | 2 |

Legend: 1) Symmetrical Safe font, 2) Arial font, 3) Times New Roman font, 4) Sang Mun Noise font, 5) Sang Mun Flower font, 6) Null Pointer font

Table 2 The number of values of the inter-character correlation for each range of relationship (DVI standard, reconstructed characters)

| The value of character correlation coefficient R^2 | Number of relationships | | | | | |
|--|-------------------------|-----|-----|-----|-----|-----|
| | 1) | 2) | 3) | 4) | 5) | 6) |
| $0.0 \leq R < 0.2$ | 0 | 25 | 43 | 107 | 57 | 45 |
| $0.2 \leq R < 0.4$ | 36 | 137 | 152 | 144 | 130 | 190 |
| $0.4 \leq R < 0.7$ | 199 | 90 | 58 | 2 | 66 | 18 |
| $0.7 \leq R < 0.9$ | 18 | 1 | 0 | 0 | 0 | 0 |
| $0.9 \leq R \leq 1.0$ | 0 | 0 | 0 | 0 | 0 | 0 |

The letters of TEMPEST font are characterized by lower level of similarity. The phenomenon has an influence on errors number in attempts of finding a correct letter in a reconstructed image.

Table 3 The number of values of the inter-character correlation for each range of relationship (laser printer, reconstructed characters)

| The value of character correlation coefficient R^2 | Number of relationships | | | | | |
|--|-------------------------|-----|-----|-----|-----|-----|
| | 1) | 2) | 3) | 4) | 5) | 6) |
| $0.0 \leq R < 0.2$ | 0 | 44 | 46 | 119 | 62 | 52 |
| $0.2 \leq R < 0.4$ | 29 | 94 | 107 | 122 | 86 | 190 |
| $0.4 \leq R < 0.7$ | 166 | 110 | 97 | 12 | 105 | 11 |
| $0.7 \leq R < 0.9$ | 58 | 5 | 3 | 0 | 0 | 0 |
| $0.9 \leq R \leq 1.0$ | 0 | 0 | 0 | 0 | 0 | 0 |

On the basis of values of inter-character correlation of traditional and Sung Mun fonts these fonts could not be considered as TEMPEST fonts. These fonts have additional graphic shapes which make easier the recognition of characters. The same phenomenon applies to Null Pointer font. The characters of this font are built from vertical and horizontal lines but widths of these lines are different.

4 CHARACTER ERROR RATE (CER)

Next tests were carried out for the traditional fonts and Symmetrical Safe fonts. It was dictated that the Sang Mun fonts cannot be used as safe fonts. Low similarity between characters of these fonts eliminates the solution as effective in electromagnetic protection of information.

The eavesdropping process is based on the reconstructed images. Therefore visual method is the main method which is used to search information on these images [23-25]. However, the visual analysis is computer-aided. In this case the correlation method based on CER is useful. The parameter determines the error values in the process of data acquisition which was used to the classifying of Arial, Times New Roman and Safe Symmetrical fonts from the viewpoint of protection of information.

For the purpose of analysis the following was taken: n -the number of all wanted letters which the reconstructed image includes, d -the number of letters which were incorrectly recognized, b -the number of letters which were rightly recognized, a -the number of letters which were unrecognized but which were wanted ($a = n - b$), m -the number of all letters which the reconstructed image included. Then:

$$CER = \frac{d + a}{m} = \frac{d + (n - b)}{m} \tag{8}$$

Tab. 4 includes the values of errors for tested fonts.

Table 4 The values of errors ($\times 10^{-3}$) calculated according to (8) for different sources of valuable emissions and for SNR_{DVI3} , SNR_{VGA3} , $SNR_{Printer3}$

| Character | VGA standard | | | DVI standard | | |
|-----------|--------------|-----|-----|--------------|----|-----|
| | 1) | 2) | 3) | 1) | 2) | 3) |
| a | 3 | 3 | 24 | 2 | 3 | 166 |
| b | 1 | 159 | 91 | 5 | 5 | 5 |
| c | 3 | 48 | 15 | 60 | 17 | 49 |
| e | 1 | 12 | 438 | 60 | 14 | 378 |
| l | 3 | 3 | 277 | 18 | 8 | 41 |
| n | 112 | 109 | 817 | 40 | 17 | 425 |
| o | 70 | 2 | 848 | 80 | 65 | 488 |
| p | 68 | 3 | 720 | 46 | 14 | 421 |
| r | 4 | 202 | 560 | 22 | 6 | 2 |
| s | 3 | 5 | 254 | 23 | 3 | 281 |
| u | 19 | 8 | 809 | 11 | 8 | 295 |
| y | 3 | 3 | 717 | 6 | 5 | 249 |
| z | 1 | 2 | 447 | 9 | 54 | 379 |

Table 5 The values of errors ($\times 10^{-3}$) calculated according to (8) for different sources of valuable emissions and for SNR_{DVI3} , SNR_{VGA3} , $SNR_{Printer3}$

| Character | Laser printer | | |
|-----------|---------------|----|-----|
| | 1) | 2) | 3) |
| <i>a</i> | 5 | 7 | 280 |
| <i>b</i> | 0 | 14 | 127 |
| <i>c</i> | 73 | 24 | 484 |
| <i>e</i> | 7 | 14 | 433 |
| <i>l</i> | 143 | 8 | 5 |
| <i>n</i> | 49 | 87 | 426 |
| <i>o</i> | 32 | 51 | 311 |
| <i>p</i> | 3 | 5 | 299 |
| <i>r</i> | 34 | 27 | 3 |
| <i>s</i> | 2 | 2 | 267 |
| <i>u</i> | 5 | 14 | 387 |
| <i>y</i> | 0 | 2 | 66 |
| <i>z</i> | 5 | 5 | 358 |

Legend: 1) Arial font, 2) Times New Roman font, 3) Safe Symmetrical font

For the purpose of analysis, $n = 31$, which produces $m = 651$. Characters have been located randomly in 31 matrices, each sized 21×31 . Fig. 11 includes fragments of the reconstructed images. Certainly the quality of the pictures is not good [25-28]. It is caused by very weak signals and disturbances inside SCA [29]. However in such conditions characters of Arial and Times New Roman fonts still are recognized [29-31].

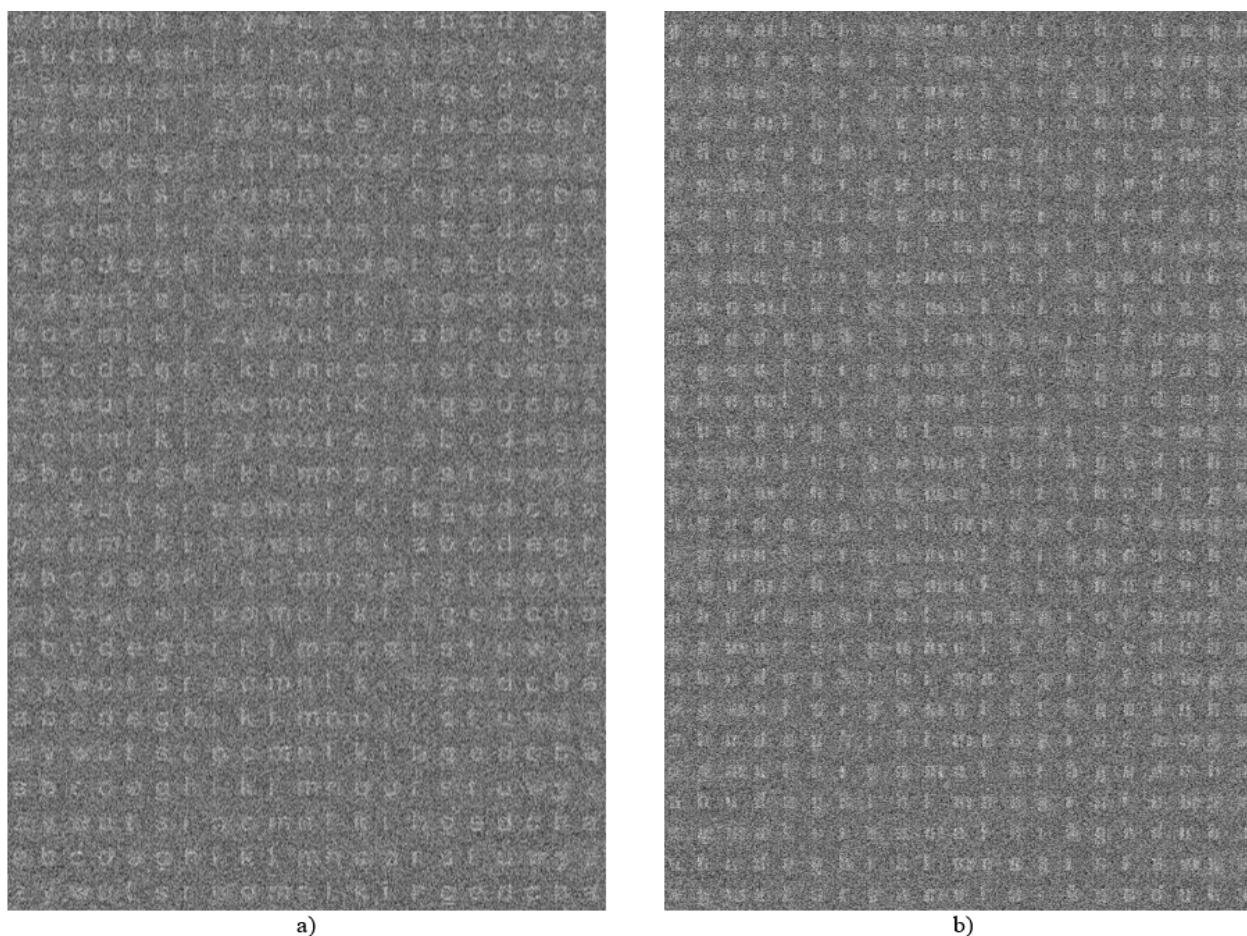


Figure 11 Examples of reconstructed images for: a) Symmetrical Safe font, b) Arial font ($SNR = SNR_{DVI3}$, $SNR_{DVI3} < SNR_{DVI2} < SNR_{DVI1}$)

5 CONCLUSIONS

In the paper a new computer font (TEMPEST font) was presented to protect processed information against the electromagnetic penetration. TEMPEST font was devoid of distinctive features in contrast to traditional fonts (Arial and Times New Roman). The new method was tested with other very popular computer fonts. There were also analyzed Mun's font, Null Pointer font, filtering of video signal and a method of colours (background and alphabet characters).

In the analyses the reconstructed images from very weak signals were used. The images included text data written by traditional fonts and TEMPEST font. To recognize the characters of these fonts the visual method was used. The analyses were supported by values of inter-

character correlation and values of errors (CER). These parameters achieved big values for new font compared to traditional fonts.

Because the Symmetrical Safe font does not have distinctive features its characters were not recognized. This makes restoring text data impossible. Values of errors confirm usefulness of the Safe Symmetrical font in counteracting the electromagnetic infiltration process.

The filtering method of video signal is not useful in case of analogue VGA standard [3, 32, 33, 34, 35]. This standard is not sensitive to changes of signal shapes in contrast to DVI standard. The filtering of digital video signal could result in display of false pixels and even the screen could be switched off. Comparable effects might take place in the case of laser printers.

6 REFERENCES

- [1] Tajima, K., Ishikawa, R., Mori, T., Suzuki, Y., & Takaya, K. (2017). A study on risk evaluation of countermeasure technique for preventing electromagnetic information leakage from ITE. *International Symposium on Electromagnetic Compatibility EMC Europe. Angers, France*. <https://doi.org/10.1109/EMCEurope.2017.8094753>
- [2] Lee, H. K., Kim, J. H., & Kim, S. C. (2013). Emission Security Limits for Compromising Emanations Using Electromagnetic Emanation Security Channel Analysis. *IEICE Transactions on Communications*. E96-B, 2639-2649. <https://doi.org/10.1587/transcom.E96.B.2639>
- [3] Song, T. L., Yook, J. G. (2014). Study of jamming countermeasure for electromagnetically leaked digital video signals. *IEEE International Symposium on Electromagnetic Compatibility*. Gothenburg, Sweden, 1161-1165.
- [4] Kubiak, I. (2017). Power line as a source of sensitive emissions from laser printers. *Przegląd Elektrotechniczny*, 6, 106-111.
- [5] Nan, Z., Yinghua, L., Qiang, C., & Yiying W. (2017). Investigation of Unintentional Video Emanations from a VGA Connector in the Desktop Computers. *IEEE Transactions on Electromagnetic Compatibility*.
- [6] Grzesiak, K. & Przybysz, A. (2011). Software Raster Generator. *Telecommunication review and Telecommunication news*, 11, 1596-1600.
- [7] Kubiak, I. (2016). Video signal level (colour intensity) and effectiveness of electromagnetic infiltration. *Bulletin of the Polish Academy of Sciences - Technical Sciences*, 64, 207-2018. <https://doi.org/10.1515/bpasts-2016-0023>
- [8] Przybysz, A. (2014). Emission security of DVI and HDMI interfaces. *Telecommunication review and Telecommunication news*, 7, 669-673.
- [9] Jun, S., Yongacoglu, A., Sun, D., & Dong W. (2016). Computer LCD recognition based on the compromising emanations in cyclic frequency domain. *IEEE International Symposium on Electromagnetic Compatibility*. Ottawa, Canada. 164-169.
- [10] Loughry, J. & Umphress, D. A. (2002). Information Leakage from Optical Emanations. *ACM Transactions on Information Systems Security*, 5, 262-289. <https://doi.org/10.1145/545186.545189>
- [11] Jinming, L., Jiemin, Z., Taikang, L., & Yongmei, L. (2017). The reconstitution of LCD compromising emanations based on wavelet denoising. *12th International Conference on Computer Science and Education (ICCSE)*. Houston, USA. 294-297. <https://doi.org/10.1109/ICCSE.2017.8085505>
- [12] Tac-Lim, S., Yi-Ru, J., & Jong-Gwan, Y. (2015). Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR. *IEEE Transactions on Electromagnetic Compatibility*, 57, 164-172. <https://doi.org/10.1109/TEMC.2014.2372039>
- [13] Tokarev, A. B., Pitolin, V. M., Beletskaya, S. Y., & Bulgakov, A. V. (2016). Detection of informative components of compromising electromagnetic emanations of computer hardware. *International Journal of Computer Technology and Applications*, 9, 09-19.
- [14] Grzesiak, K. & Przybysz, A. (2010). Emission security of laser printers, Military Communications and Information Systems Conference. Wroclaw, Poland. 353-363.
- [15] Kubiak I. & Przybysz, A. (2016). Printing technology and electromagnetic protection of information. *Przegląd Elektrotechniczny*, 1, 177-181. <https://doi.org/10.15199/48.2016.01.42>
- [16] Choudary, O. & Kuhn M. G. (2014). Template attacks on different devices. *Lecture Notes in Computer Science*. 8622, 179-198. https://doi.org/10.1007/978-3-319-10175-0_13
- [17] Litao, W. & Bin, Y. (2011). Analysis and Measurement on the Electromagnetic Compromising Emanations of Computer Keyboards. Seventh International Conference on Computational Intelligence and Security. Sanya. 640-643.
- [18] Kuhn, M. G. (2003). *Compromising emanations: eavesdropping risks of computer displays*. Technical reports published by the University of Cambridge Computer Laboratory
- [19] Kuhn, M. G. (2002). Optical Time-Domain Eavesdropping Risks of CRT Displays. IEEE Symposium on Security and Privacy. Berkeley, California. *IEEE Computer Society*. 3-18
- [20] Kubiak, I. (2015). Null Pointer computer font - electromagnetic safe or not? *Telecommunication review and Telecommunication news*, 1, 11-18. <https://doi.org/10.15199/59.2015.1.3>
- [21] Kubiak, I. (2014). Computer font resistant to electromagnetic infiltration process. *Przegląd Elektrotechniczny*, 6, 207-215
- [22] Regodić, M., Gigović, L., Bajić, Z., & Vasiljević, S. (2017). Contrast enhancement of colour digital images. *Tehnički vjesnik*, 24(3), 935-941. <https://doi.org/10.17559/TV-20150410194409>
- [23] Bahare, J. & Abdolah, C. (2014). Persian Sign Language Recognition Using Radial Distance and Fourier Transform. *International Journal of Image, Graphics and Signal Processing*, 1, 40-46. <https://doi.org/10.5815/ijigsp.2014.01.06>
- [24] Michael, J. M. (2000). The Pentagon worries that spies can see its computer screens, someone could watch what's on your VDT. *The Wall Street Journal*, 8.
- [25] Çalışkan, A. & Çevik, U. (2018). An Efficient Noisy Pixels Detection Model for CT Images using Extreme Learning Machines. *Tehnički vjesnik*, 25(3), 679-686. <https://doi.org/10.17559/TV-20171220221947>
- [26] Cihan, U., Aşık, U., & Cantürk, K. (2015). Analysis of Information Leakages on Laser Printers in the Media of Electromagnetic Radiation and Line Conductions. *International Conference on Information Security and Cryptology*. Ankara, Turkey.
- [27] Cihan, U., Aşık, U., & Cantürk, K. (2016). Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines. *Computers & Security*, 58, 250-267. <https://doi.org/10.1016/j.cose.2016.02.001>
- [28] Cihan, U., Aşık, U., Cantürk, K., Sarhat, S., Bilal, K., & Ugur, S. (2014). Automatic tempest test and analysis system design. *International Journal on Cryptography and Information Security*, 4. <https://doi.org/10.5121/ijcis.2014.4301>
- [29] Jurić, I., Nedeljković, U., Novaković, D., & Pinčjer, I. (2016). Visual experience of noise in digital images. *Tehnički vjesnik*, 23(5), 1463-1467. <https://doi.org/10.17559/TV-20150317101822>
- [30] Ketenci, S., Kayıkçıoğlu, T., & Gangal, A. (2015). Recognition of sign language numbers via electromyography signals. *Signal Processing and Communications Applications Conference*. Malatya, Turkey. 2593-2596. <https://doi.org/10.1109/SIU.2015.7130416>
- [31] Nedeljković, U., Novaković, D., & Pinčjer, I. (2017). Detecting universal structure and effects of typefaces. *Tehnički vjesnik*, 24(2), 557-564. <https://doi.org/10.17559/TV-20150831131738>
- [32] Nidhi, C. & Amnesh, G. (2012). A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise of RGB Values and Explosive Inter-Pixel Displacement. *International Journal of Image, Graphics and Signal Processing*, 2, 16-22. <https://doi.org/10.5815/ijigsp.2012.02.03>
- [33] Jun, S., Yongacoglu, A., Degang, S., & Dong, W. (2016). Computer LCD recognition based on the compromising emanations in cyclic frequency domain. *IEEE International Symposium on Electromagnetic Compatibility*. Ottawa, Canada. 164-169.

- [34] Mahshid, Z., Saeedeh, H. T., & Ayaz, G. (2009). Security limits for Electromagnetic Radiation from CRT Display. *Second International Conference on Computer and Electrical Engineering*. Dubai, United Arab Emirates. 452-456.
- [35] Nan, Z., Yinghua, L., Qiang, C., & Yiyang, W. (2017). Investigation of Unintentional Video Emanations from a VGA Connector in the Desktop Computers. *IEEE Transactions on Electromagnetic Compatibility*, 59(6), 1826-1834. <https://doi.org/10.1109/TEMC.2017.2699479>

Contact information:

Ireneusz KUBIAK, PhD
(Corresponding author)
Military Communication Institute,
22A Warszawska St., 05-130 Zegrze, Poland
E-mail: i.kubiak@wil.waw.pl