symmetry

Article

Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process

Alexandru Boitan [1], Ireneusz Kubiak [2], Simona Halunga [3,*], Artur Przybysz [2] and Andrzej Stańczak [2]

1 Special Telecommunications Services, Splaiul Independentei St., 060044 Bucharest, Romania; alexandru.boitan@stsnet.ro

2 Department of Electromagnetic Compatibility, Military Communication Institute—National Research Institute, 05-130 Zegrze, Poland; i.kubiak@wil.waw.pl (I.K.); a.przybysz@wil.waw.pl (A.P.); a.stanczak@wil.waw.pl (A.S.)

3 Telecommunications Department, University Politehnica of Bucharest, 060042 Bucharest, Romania

* Correspondence: simona.halunga@upb.ro

Received: 16 October 2020; Accepted: 18 November 2020; Published: 20 November 2020

Abstract: The protection of information processed electronically involves a large number of IT devices from computer sets or laptops to monitors, printers, servers, etc. In many cases, classified information processing might be associated with the use of projectors, which are an indispensable element of meetings for a limited group of people. Such devices are connected to computers through interfaces of various analogue and digital standards and can become an additional source of unwanted emissions, and the distinctive features of these emissions allow the information displayed to be unwantedly reproduced. This paper offers evidence of the existing threat related to electromagnetic infiltration of several projectors, by showing images reconstructed from registered revealing emissions. The paper presents an analysis of several solutions that can be used to reduce the level of infiltration susceptibility of projectors or to highlight this property in the device assessment process. The possibilities of using special computer fonts and the so-called method of colors—background color and text color—is analyzed. The tests were carried out on randomly selected projectors in two independent laboratories, and, based on these results, a number of interesting conclusions have been highlighted at the end.

Keywords: electromagnetic eavesdropping; electromagnetic infiltration; projector; information protection; revealing emission; valuable emission

1. Introduction

Electronic devices are now widely used for information processing, and this applies not only to single devices but also to more complex systems, that may be used for personal purposes, inside companies or even for military applications. Lots of information is provided through these systems, many of them being sensitive ones from the user's point of view, and when dealing with confidential military information, special measures must be taken to ensure its confidentiality. Usually, commercial equipment is not tested with respect to confidentiality risks, therefore all military equipment has to be analyzed in Tempest domain. This study is a very good example of an asymmetrical approach in communication engineering, in which a group of users try to protect themselves from a potential intruder who, without the knowledge of the rightful users of the system, tries to intercept their communication and information shared through various devices based on capturing unwanted electromagnetic emanations of various devices used.

The results presented in this paper were obtained after performing specialized laboratory measurements that are specific to the Tempest field [1–4]. This technical field was first discovered and promoted by the US government and referred to the protection of classified information in the military domain. The goal has been maintained over the years and the standardization of this field has expanded to NATO SECAN Doctrine and Information Publications (SDIPNATO standards for Tempest) and EU (IASG- Information Assurance Security Guidelines on Accreditation of EUTEMPEST Companies standards) areas [3,4]. Any member country, NATO or EU, must comply with the requirements of these standards when handling classified information. Obviously, each member country also proposed and developed its own national standards that can be applied together with the international ones (NATO or EU) at a national level. TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) standards cover all subjective aspects for equipment that processes such information. The standards include rules for evaluating the level of protection offered by the physical space in which the equipment will operate (SDIP-28/1), the level of protection offered by the equipment (SDIP-27/2) as well as the installation rules that must be implemented when installing it (SDIP-29/1). All the measurements, evaluations and interpretation of the results presented in this paper are made in accordance with the above-mentioned standards.

The information infiltration process represents the access to information processed by the equipment through reception and processing techniques of electromagnetic emissions generated by the targeted equipment without having physical access to it. The risks associated with the process of electromagnetic infiltration are very often described and analyzed in relation to computers [5–7], monitors [5,8–11] or laser printers [12–15]. Each such device becomes a source of undesirable emissions, which enable non-invasive acquisition of information. For each of the above-mentioned devices, the cheapest and the best solutions for reducing the effectiveness of the electromagnetic infiltration process are studied in order to be implemented at the producer, for common type applications. However, in the case of military applications, when the information processed by such devices is of critical importance, sometimes classified, this problem become even more crucial.

The risk of electromagnetic infiltration has also been studied for peripheral communications of personal computers (PC), such as the keyboard, whether it is USB [16,17] or PS/2 [16,18,19] type, RS-232 communication cable [20] that is still used in many existing implementations, USB devices [21], Ethernet communication [22] or VGA video graphics array connectors [9]. In [23], researchers performed studies and measurements for several shielding configurations for the electromagnetic screens and their suitability and efficiency of the electromagnetic emissions of information systems, while in [24] the authors performed channel measurements to evaluate the electromagnetic emanation security in the 200–1000 MHz frequency bandwidth, and proposed some adaptive security limits that depends on the total radio attenuation and on the extent of required confidentiality. In [25], researchers presented several testing and countermeasure methods against electromagnetic security threats and some a risk evaluation method of countermeasure technique for preventing electromagnetic information leakage is studied, based on the International Telecommunication Union (ITU) recommendation [26]. In [27], the authors propose a 2D electromagnetic imaging system to localize interference sources and identify the Electromagnetic Interference (EMI) frequency in real time while in [28], the authors presented several time-domain methods for solving electromagnetic problems.

It should be noted that, in many cases, other equipment, that usually are not considered as a potential hazard, may be a significant source of undesirable emissions. Often, however, these devices may become a weak element of the IT system from the point of view of infiltration susceptibility. Such a device can be a projector [29], which is an additional source of displaying the processed data. It is often used during business meetings, briefings or closed seminars due to the confidentiality of the data presented. Of course, special computers are used, as well as special double shielded signal cables, which, in the opinion of many users, should ensure protection of the information presented. In this paper the main objective is represented by the effect produced by the use of colors on the level of compromising radiation of the tested equipment, that, in this case, were different types of video projectors and several equipment from this category were selected in order to achieve the objectivity of the tests performed. Projectors very often are used to present classified information which have to be protected, therefore they have to be tested by Tempest procedures as well.

The aim of this article is to present the existing risk related to the use of typical projectors in a system with special devices that are dealing with confidential data and to propose solutions to reduce the level of this risk. The possibility of using special computer fonts was proposed and their effectiveness was compared with traditional fonts [15,30,31]. Due to the specificities of the modern presentations, this solution was connected with the method of colors, based on the appropriate selection of the background color and the color of the text characters.

The solution consists in an appropriate selection of pairs of colors that can also be used in the process of assessing devices equipped with screens in terms of meeting electromagnetic protection requirements in accordance with NATO Tempest Standard SDIP-27/2 [3] and UE Tempest Standard IASG 7-03 [4]. During this type of experiments, the tested device should operate in the most effective mode with respect to the electromagnetic infiltration process. As will be shown later in this article, for a selected pair of background and text colors, the reproduced images from the recorded revealing emissions may contain more or less distinct computer font characters. Such a phenomenon can be the basis used for recommendations for those testing devices designed to process classified information.

2. Materials and Methods

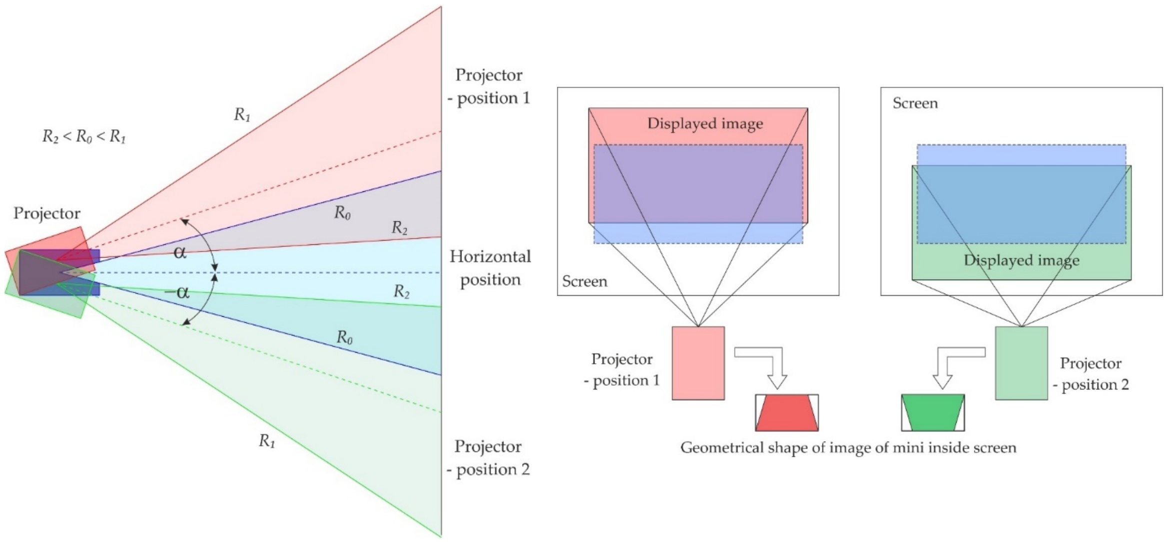
2.1. Equipment Used and Discussion

The agglomeration of many devices in one place may sometimes raise doubts as to which device is the source of the spurious emissions. Such a problem can be encountered when assessing devices in accordance with the SDIP-27/2 standard. This may concern, for example, a system consisting of a computer set (laptop) and a projector, as well as a transmission medium, usually a video cable that is transmitting the electrical signals, represented in accordance with various standards, from the computer to the projector. When evaluating the projector, it is necessary to minimize the impact of the remaining system components on the test results. A TEMPEST class computer, which is characterized by low levels of electromagnetic disturbances, can be used as a computer set. You can also use a special signal cable—double shield and shielded connectors. In such a system, the tested projector remains the only source of undesirable emissions. The test bed set is depicted in Figure 1 that shows two views of the test bed set: (**a**) from right side and (**b**) from left side. For the tests a Tempest Test System DSI-1550A receiver and a special set of antennas: A rod antenna HE525 (100 Hz–30 MHz), a biconical antenna HE526 (30–200 MHz), a dipole antenna HE527 (200 MHz–1 GHz) and a double ridge horn antenna (EMCO, 1–18 GHz) were used.

(**a**) (**b**)

Figure 1. The test system used in the anechoic chamber of the laboratory of the Military Communication Institute—National Research Institute, (**a**) testbed view from right side (**b**) testbed view from left side

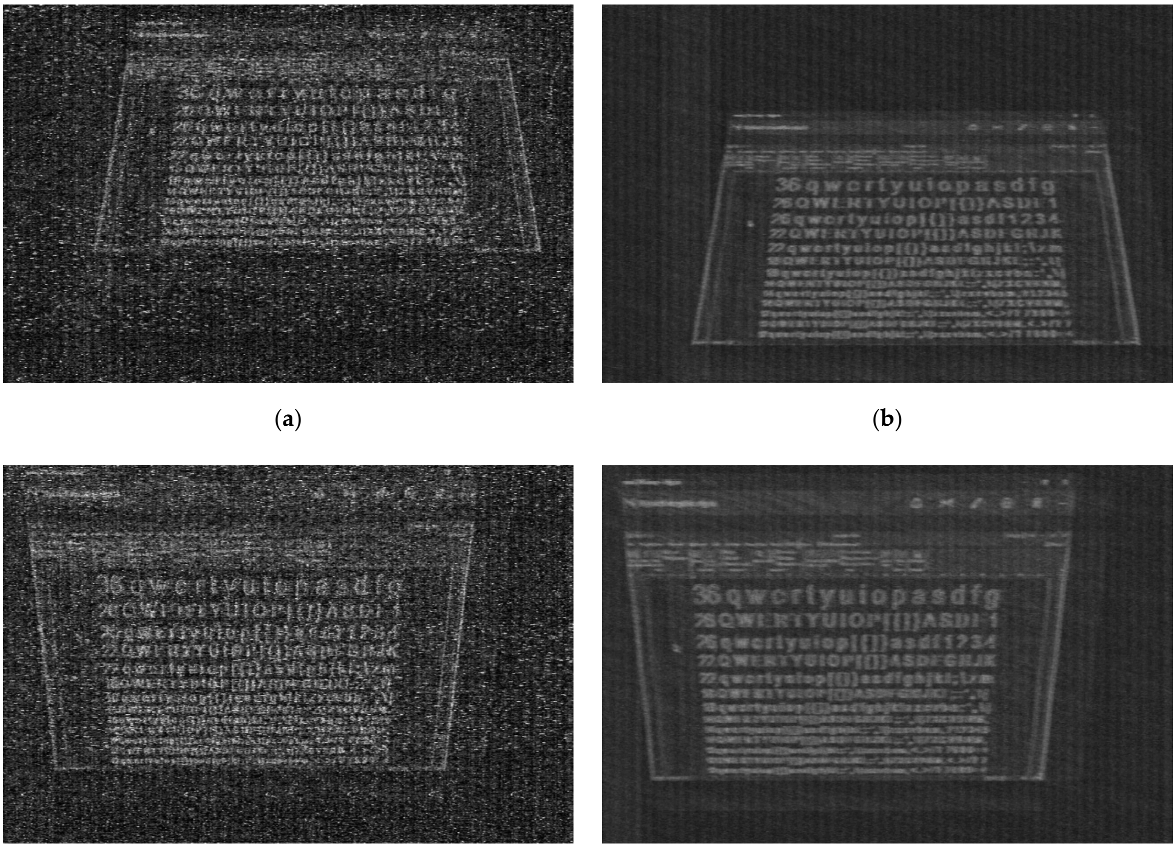
Before starting the research and analysis related to the electromagnetic safety of projectors, tests were carried out on each equipment involved, the results of which confirmed that the cooperating devices are not a source of undesirable emissions. The NEC VT57 projector, that has a VGA interface only, was included in the preliminary analysis. The projector's manufacturer has used a manual correction of the geometric dimensions of the image displayed on the screen depending on the angle of the projector. The correction consists in changing the geometrical parameters of the image that is appearing on the internal screen of the projector, which is the main source of unwanted emissions. The influence of changing the geometrical parameters of the projectors' image on the projected image is shown in Figure 2. R_0, R_1 and R_2 are distances between the projector and a screen (a wall) where the picture is displayed for different positions of the projector. For position 1 and position 2, the displayed pictures require correction because the distance R_1 (for the top edge of the picture–position 1) is longer than R_2 (for the bottom edge of the picture–position 1). The same situation is observed for the location of the projector in position 2, when the distance R_1 (for the bottom edge of the picture is longer than R_2 for the top edge of picture). When the projector is directed straight to the screen the distances R_0 are equal and the displayed picture does not require correction.



(**a**) (**b**)

Figure 2. (**a**) changes in the geometrical parameters of the image of the original projector "projected" on the screen depending on (**b**) its position (tilt), affecting the image displayed on the screen magnetization as a function of applied field.

This image correction mechanism deteriorates the image quality, due to the duplication and elimination of some pixels in the upper and lower part of the image, depending on the direction of the geometrical changes of the image. The phenomenon of changing the image shape, leading to a trapezoidal shape of the displayed image, could be observed especially on old cathode-ray tube (CRT) monitors, used several years ago, as shown in Figure 3. Figure 3a shows the case of the projector in position 2, while Figure 3b shows it in position 1 of the projector. For both cases the pictures displayed on the screen has been corrected.



(**a**) (**b**) (**c**) (**d**)

Figure 3. Examples of the images reconstructed based on the recorded unwanted emissions from the NEC VT57 projector for the extreme positions of the geometric correction of the displayed image: (**a**) $a < b$, original image, (**b**) $a < b$, image after 30-fold summing of images, (**c**) $a > b$, primary image and (**d**) $a > b$, image after 30-fold summing of images (a—upper trapezoid base, b—bottom trapezoid base).

Since the said projectors' internal screen is the main source of the emissions correlated with the projected image, the introduced picture shape correction was observed on the images reproduced from the recorded emissions arising from the internal screen of the abovementioned projector; the pictures displayed on the internal screen had trapezoid shape. This directly proves that the projector is the only source of valuable emissions.

Another method to correct the geometric parameters of the image displayed on the screen, resulting from the different inclination of the projector in relation to the horizontal plane, is to change the position of the internal optical elements of the projector.

Such a solution has been implemented in newer and more expensive projectors, like the ACER D1P1426, that is equipped with VGA (Video Graphics Array) and HDMI (High Definition Multimedia Interface) interfaces. In this case, the geometrical changes of the primary image are not noticeable in the process of electromagnetic infiltration as such changes do not occur.

Preliminary research results clearly show that a projector, as a graphic data display device, presents a risk of confidentiality loss like a typical computer monitor. Safe use of this type of equipment requires the use of counter measuring solutions to prevent unwanted emissions. On the other hand, it is necessary to use appropriate tests that would fully allow assessing the resistance of the device to the effectiveness of the electromagnetic infiltration process. Both aspects have been analyzed and their results are presented later in the article.

2.2. Test Bed Setup

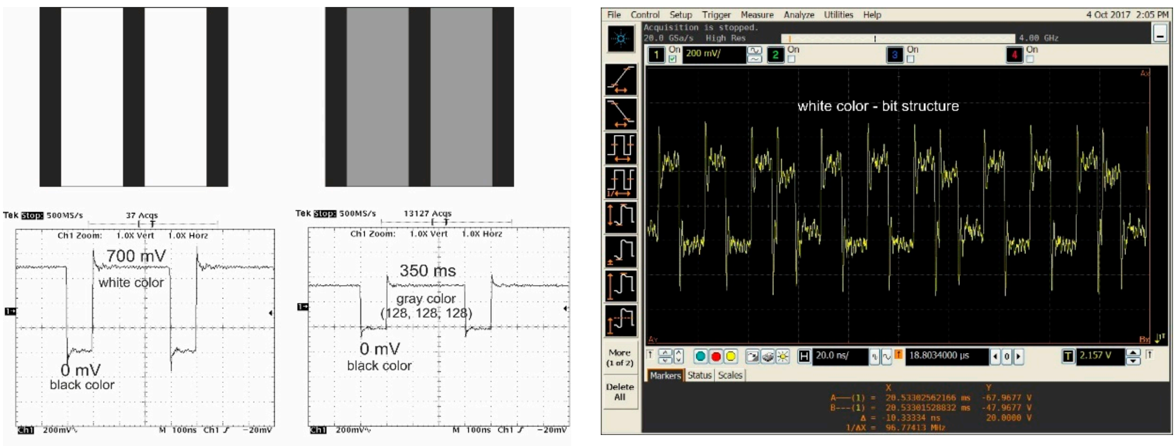
The aim of the tests and analyses was:

- to demonstrate the risk of information loss in a non-invasive way, related to the uncritical use of projectors to display information graphically;
- to propose the use of safe fonts to counteract the process of electromagnetic infiltration;
- to present the method of colors used as a solution supporting electromagnetic protection of processed graphic information;
- to indicate the method of colors as a test signal in emission safety tests according to SDIP-27/2 standard [3].

Relevant tests were carried out for three selected types of projectors: VT57 NEC, D1P1426 ACER, EH-TW650 EPSON, which used an analog and/or digital video standard (VGA, HDMI). This approach shown that the discussed risk of losing confidentiality is not a coincidence, and can apply to any type of projector, regardless of the manufacturer. As for other devices used for graphical display of processed information, it is advisable to propose solutions that can counteract the generation of emissions that can be correlated with the original signal. In the further part of the article, the authors analyze the effectiveness of the safe fonts [6,31], that proved to be efficient for the protection of processed text data for computer monitors and laser printers. Then the safe fonts were indicated as a universal solution that can be used in various devices processing text data to protect them against electromagnetic penetration. Results show that the projector is another device of this type in which these fonts can be used.

The method based on safe fonts is an effective and non-invasive solution. It does not eliminate completely the effects of the existence of the emission source, which are emissions correlated with the information processed, but their special designed shape directly influences the emission sources making them worthless in the process of electromagnetic infiltration.

The research also used the method of colors as a solution that can protect the processed text data. This can be achieved by eliminating the significant differences in the amplitude values of the video signal (analog VGA standard) RGB, which determine the color of the background and text, as shown in Figure 4a. The voltage differences are the source of revealing emissions allowing the reconstruction of the information. In the case of a digital video standard, the selection of color pairs is related to the correlation of bit structures of colors. The high degree of similarity of such structures makes it difficult to distinguish them on the receiving side of revealing emissions and thus to reproduce the data as shown in Figure 4b.



(**a**) (**b**)

Figure 4. Examples of time courses of electrical signals for (**a**) VGA and (**b**) HDMI standards.

The method of colors can also be considered from a different angle. Research on devices processing classified information requires the use of forcing signals during tests, shaping the emission source (e.g., projector, monitor and printer) with the highest radiation efficiency.

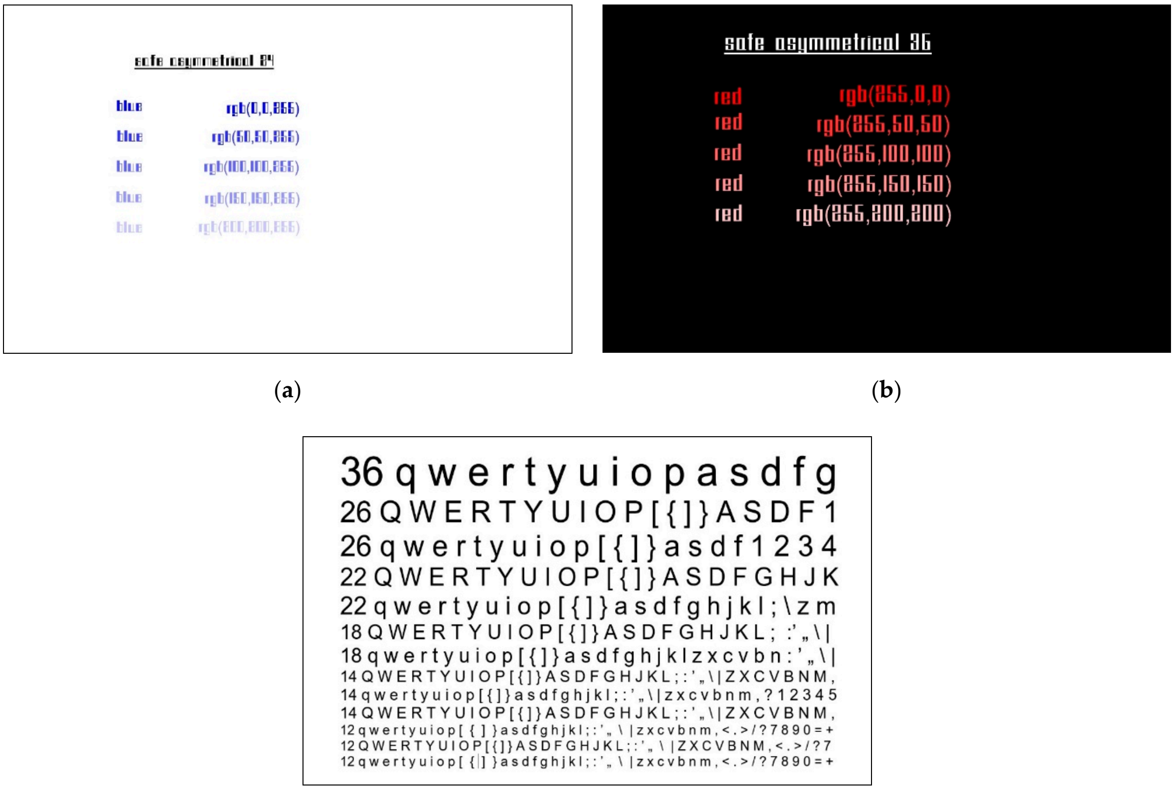
In the case of text type data, it is possible to shape the electromagnetic radiation through the choice of background and text colors. The present paper proposes pairs of colors which, due to this property, can be recommended for use in the assessment of special devices in accordance with the SDIP-27/2 document [3]. This is the opposite of the operation previously described where the color pairs are selected to reduce the radiation efficiency of the revealing emission source. The color method can therefore have a dual use.

During the research, several test images were used, as presented in Table 1; examples of such images are shown in Figure 5. The images contain simple text written using safe fonts (safe symmetrical and safe asymmetrical) of various sizes and for different combinations of background colors (white and black) and text (black, green, red and blue with varying degrees of intensity). Such test and research scenarios allowed to achieve the set research goals:

- to demonstrate the superiority of safe fonts over traditional ones in protecting text data processed by the projector against electromagnetic infiltration;
- to indicate pairs of colors that increase the level of electromagnetic safety;
- to indicate pairs of colors that increase the radiation efficiency of the source of undesirable emissions for the assessment of the device in accordance with SDIP-27/2 [3].

Table 1. Background and text color parameters for test images.

Background Color	**Value of RGB—Text**		
	R	**G**	**B**
Black or white (RGB:000 or 255 255 255)	0	0	0
	50	50	50
	100	100	100
	150	150	150
	200	200	200
	255	0	0
	255	50	50
	255	100	100
	255	150	150
	255	200	200
	0	255	0
	50	255	50
	100	255	100
	150	255	150
	200	255	200
	0	0	255
	50	50	255
	100	100	255
	150	150	255
	200	200	255



(**a**) (**b**)

(**c**)

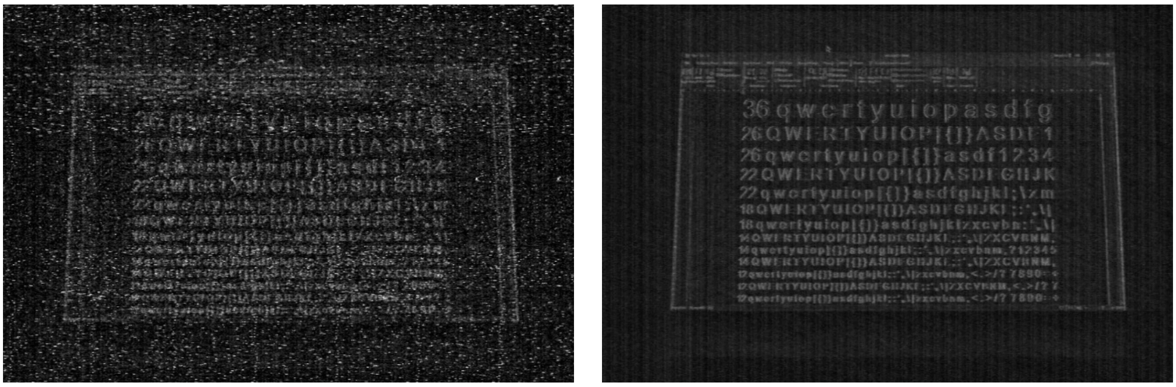
Figure 5. Examples of test images displayed by the projector for the assessment of: (**a**) the method of colors—white background (255, 255, 255), font safe asymmetrical-size 24p., blue color as the basic font color, (**b**) the method of colors—black background (0, 0, 0), safe symmetrical font-size 36p., red color as the basic font color, (**c**) electromagnetic infiltration susceptibility—white background (255, 255, 255), traditional Arial font—black color of font (0, 0, 0).

In the table above, the horizontal colors (grey, red, green, blue) show parameters of RGB for different intensity of black, red, green and blue colors used in the tests.

3. Results

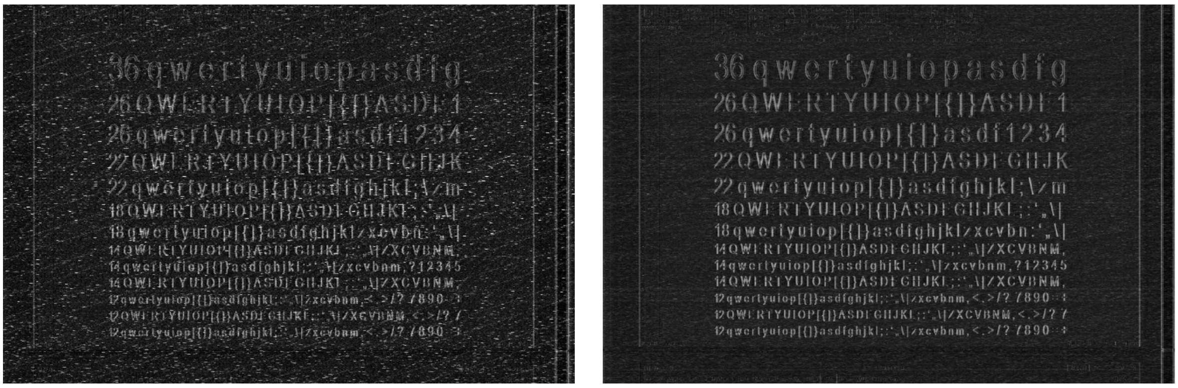
Relevant tests described in Section 2 were carried out in two independent laboratories: The STS Laboratory (Romania) and the Laboratory of the Military Communication Institute—National Research Institute (Poland). Both laboratories have high competence in the field of testing and evaluating special devices and developing of analyses methods of revealing emissions. The dedicated TEMPEST Test System DSI-1550A receiver from Dynamic Sciences International (Poland) and FSET 22 Receiver R&S (Romania) were used for the tests.

In the first stage of the research, it was shown that projectors are a source of revealing emissions, as shown in Figures 6–8. This applies to both operation systems, using the VGA and HDMI standards. In each case, the recorded revealing emissions made it possible to reproduce the data that was legible and understandable.



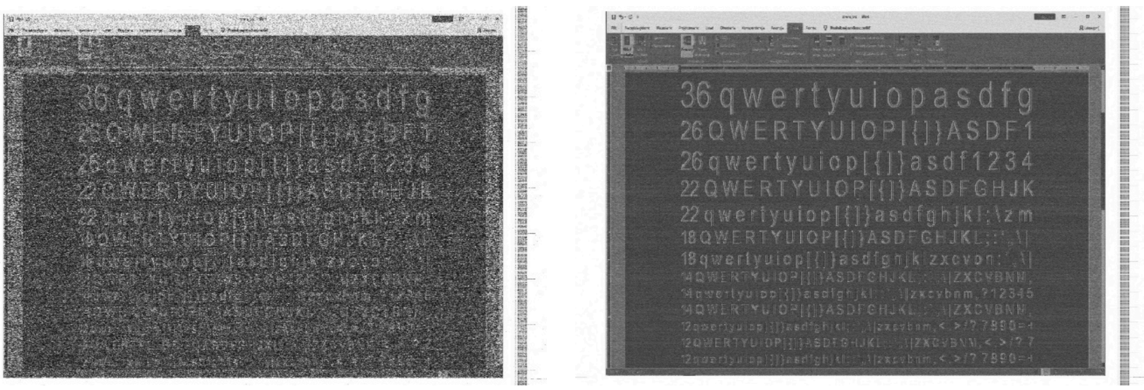
(**a**) (**b**)

Figure 6. An image reconstructed from the registered revealing emission measured at the frequency f_o = 386 MHz, BW = 20 MHz: (**a**) original image and (**b**) image after applying the 30-fold summation operation.



(**a**) (**b**)

Figure 7. An image reconstructed from the registered revealing emission measured at the frequency f_o = 286 MHz, BW = 50 MHz: (**a**) original image and (**b**) image after applying the 30-fold summation operation.



(**a**) (**b**)

Figure 8. An image reconstructed from the registered revealing emission measured at the frequency f_o = 742 MHz, BW = 50 MHz: (**a**) original image and (**b**) image after applying the 30-fold summation operation.

4. Discussions

Relevant tests described in Section 2 were carried out in two independent laboratories: The STS Laboratory (Romania) and the Laboratory of the Military Communication Institute—National Research

Institute (Poland). Both laboratories have high competence in the field of testing and evaluating special devices and developing of analyses methods of revealing emissions. The dedicated TEMPEST Test System DSI-1550A receiver from Dynamic Sciences International (Poland) and FSET 22 Receiver R&S (Romania) were used for the tests.

In the first stage of the research, it was shown that projectors are a source of revealing emissions, as shown in Figures 6–8. This applies to both operation systems, using the VGA and HDMI standards. In each case, the recorded revealing emissions made it possible to reproduce the data that was legible and understandable.

4.1. Video Projectors

Two types of projectors from two different manufacturers were tested for revealing emissions. The projectors differed in the technology of transferring images from the computer to the screen. Regardless of the technology used, devices of this type are a source of undesirable emissions and their levels allow for non-invasive obtaining of information. The reproduced images, despite the poor quality, become legible after using the image summation method. It is possible to recognize individual characters of a computer font (in the case of Arial font tests) for characters up to 12p. This phenomenon applies to both the projector operation in the VGA standard and in the HDMI standard. Therefore, the safe display of data requires the use of solutions that will allow for the appropriate modification of the emission source, which is the projector, which will reduce its efficiency.

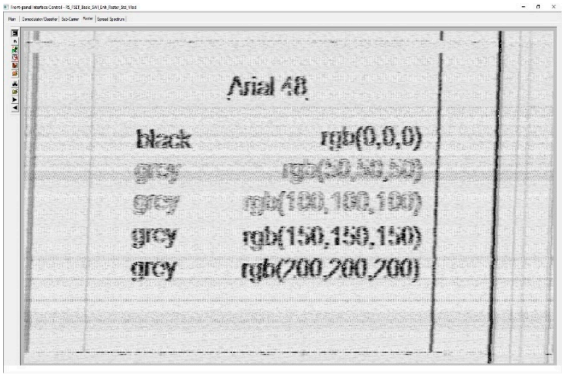
The use of design solutions that interfere with the construction of the projector is costly and dangerous because may lead to high temperatures generated by the modified device. The process of electromagnetic shielding of any electronic equipment also involves the application of specific protection measures to the ventilation holes. This can lead to inadequate ventilation of the equipment and obviously to overheating of the electronic components which can lead to improper malfunction or even damage to the equipment. The electromagnetic shielding measures described both in the TEMPEST and in the electromagnetic compatibility (EMC) fields represent general principles and not punctual/dedicated countermeasures. Thus, many times, this process is very complex and at the same time expensive, as it involves the “try and test” method. After applying the shielding measures, the equipment is subjected to tests to verify its normal functionality as well as shielding effectiveness of the applied measures. Moreover, the warranty of the equipment on which such measures have been applied is supported by the authorized company that applied these measures and not by the company producing the commercial equipment. It should be noted that the frequency range of revealing emissions is very wide. Such emissions are measured at frequencies of several hundred MHz and even above 1 GHz. The wide range of frequencies at which these emissions can be received generates the need to identify suitable and costly shielding materials that can attenuate or even eliminate these unwanted emissions depending on their amplitude.

Thus, in this paper the authors propose low-cost and effective solutions that modify the source of electromagnetic emissions and not the effects of the occurrence of such a source. These solutions imply the use of safe fonts and of the method of colors related to the combination of appropriate colors of the text and the background on which the text appears.

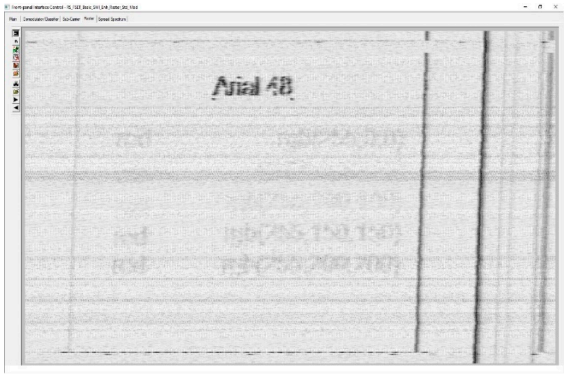
Research on the use of safe fonts and the method of colors to protect data against electromagnetic penetration was carried out the use the EH-TW650 projector from EPSON. At the same time, it was shown that another projector from the third manufacturer was also a source of unwanted emissions. The tests were carried out for the video signal of the HDMI standard and for the projector operation in the $1920 \times 1080 \times 60$ Hz mode.

4.1.1. The Method of Colors

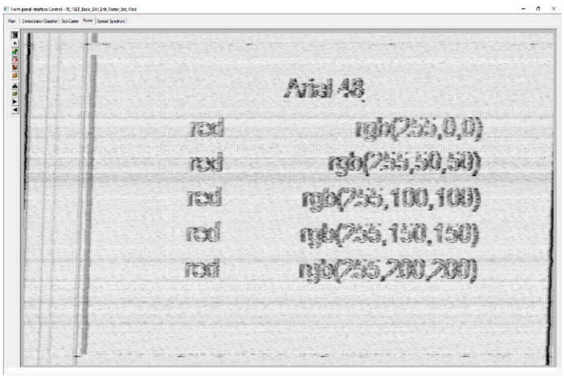
The method of colors is based on the appropriate selection of the color of the text and the background, in order to minimize the compromising emanations. For that we carried out research in order to recover the text displayed by the projector when typical Arial computer font was used. The image recovered based on processing compromising emissions around f_o = 455 MHz are shown in Figure 9 for different combinations of text and background and for different size of characters, while in Figure 10 are presented the images recovered based on the emissions around f_o = 495 MHz. The text and background colors corresponded to the combinations shown in Table 1.



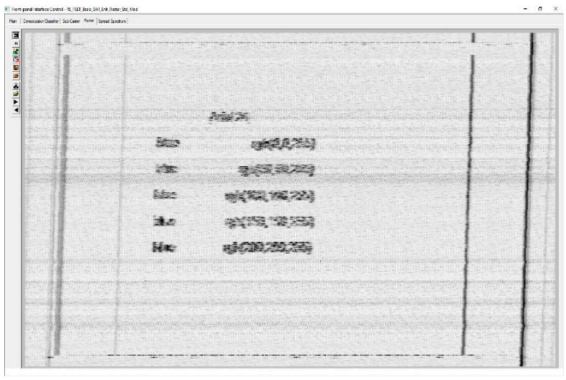
(**a**)



(**b**)

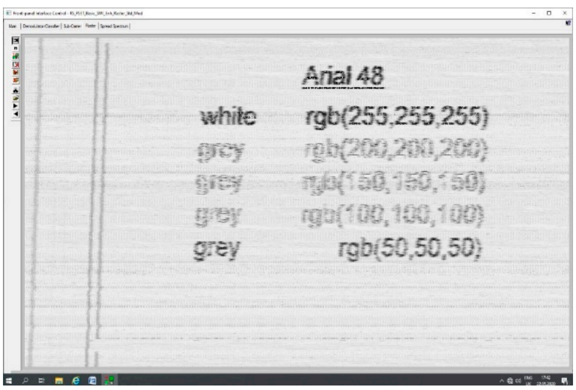


(**c**)

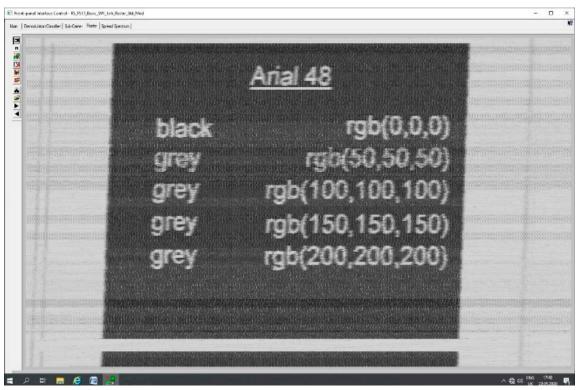


(**d**)

Figure 9. A reconstructed image on based on valuable emission measured on frequency f_o = 455 MHz: Arial font, (**a**) dimension 48p., text color—black, background color—white, (**b**) dimension 48p., text color—red, background color—white, (**c**) dimension 48p., text color—red, background color—black and (**d**) dimension 24p., text color—blue, background color—white.



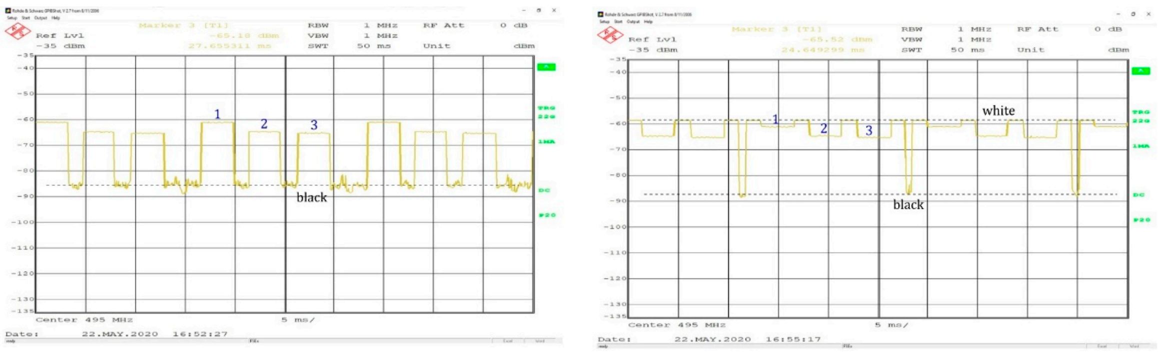
(**a**)



(**b**)

Figure 10. A reconstructed image based on valuable emission measured on frequency f_o = 495 MHz: Arial font, dimension 48p., (**a**) text color—white, background color—black and (**b**) text color—black, background color—white.

To understand this phenomenon there was recorded time course of valuable emission on frequency 495 MHz, obtaining the results presented in Figure 11, where marker 1 represents the red color, marker 2 the green color and marker 3 the blue color on white background (Figure 11a) and respectively black background (Figure 11b). We can see different levels of signal amplitudes for different used colors. When those differences are smaller the graphic elements on reconstructed image are visible weakly.



(**a**) (**b**)

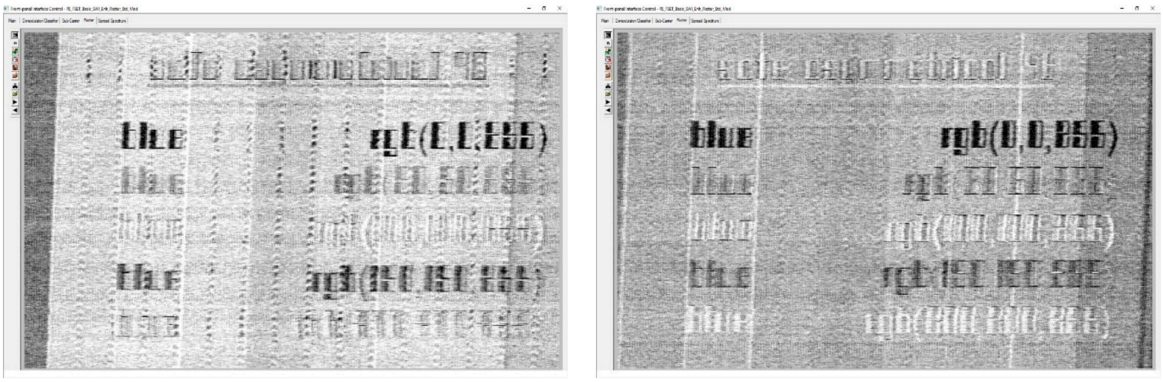
Figure 11. A time course of a valuable emission measured on frequency f_o = 495 MHz: A marker 1—red color, a marker 2—green color, a marker 3—blue color, (**a**) background—black color and (**b**) background—white color.

4.1.2. The Method of Colors and Safe Fonts

The method of colors can be combined with the use of safe fonts. Such approach has an impact on two aspects related to the protection of information against electromagnetic penetration. A properly selected pair of colors may reduce the level of measured electromagnetic emissions, systematized in Table 2. Safe fonts do not affect the emission level but only the shape of the displayed characters of the computer fonts. Their high correlation properties between font characters, additionally, make it difficult to distinguish the characters and thus the legibility of information, as it can be seen from Figures 12 and 13.

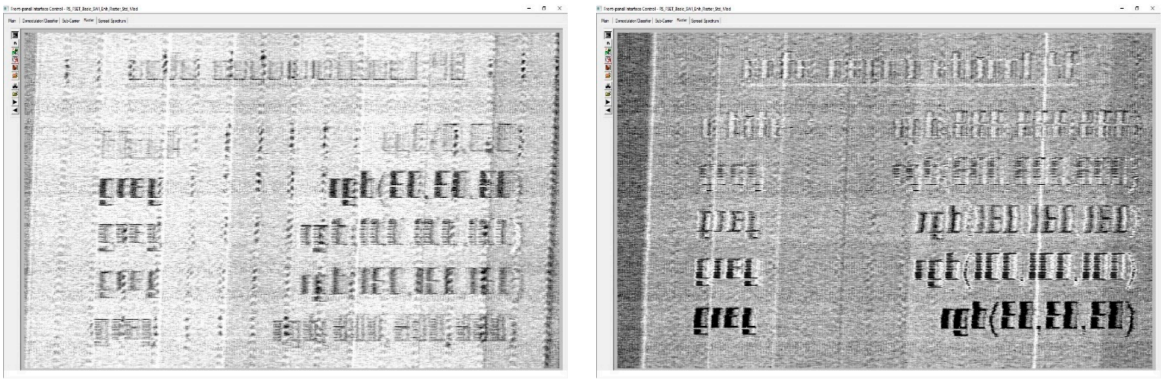
Table 2. Pairs of text and background colors for which the effectiveness of the electromagnetic infiltration has been reduced.

Frequency of Revealing Emission	Text Color RGB	Background Color RGB
520 MHz (Figure 14a,b)	100, 100, 255	255, 255, 255
	200, 200, 255	255, 255, 255
520 MHz (Figure 14c–e)	50, 50, 255	0, 0, 0
	100, 100, 255	0, 0, 0
	200, 200, 255	0, 0, 0
520 MHz (Figure 14f,g)	255, 100, 100	0, 0, 0
	255, 200, 200	0, 0, 0
520 MHz (Figure 14h,i)	50, 255, 50	0, 0, 0
	100, 255, 100	0, 0, 0
455 MHz (Figure 14j–n)	255, 0, 0	255, 255, 255
	255, 50, 50	255, 255, 255
	255, 100, 100	255, 255, 255
	255, 150, 150	255, 255, 255
	255, 200, 200	255, 255, 255

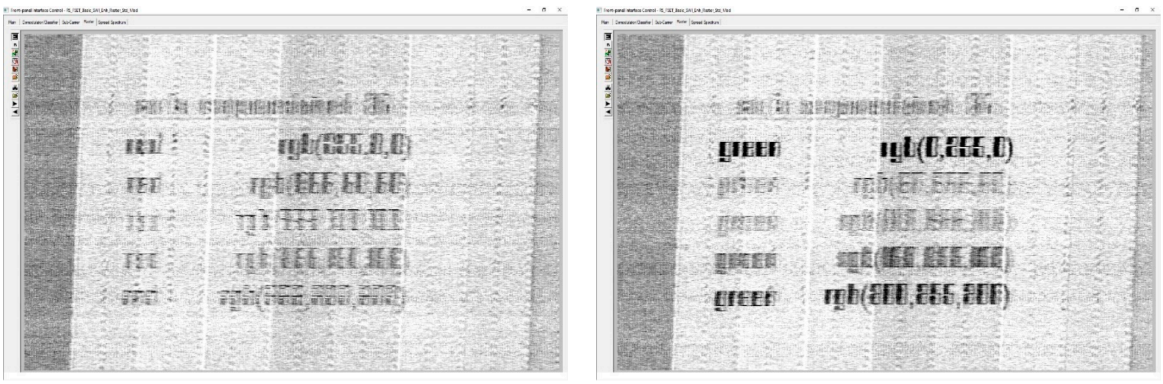


(**a**) (**b**)

Figure 12. A reconstructed image on based on valuable emission measured on frequency f_o = 520 MHz: Safe asymmetrical font, dimension 48p., text color—blue, (**a**) background color—white and (**b**) background color—black.



(**a**) (**b**)



(**c**) (**d**)

Figure 13. A reconstructed image on based on valuable emission measured on frequency f_o = 520 MHz: Safe asymmetrical font, dimension 48p., (**a**) text color—black, background color—white, (**b**) text color—white, background color—black, (**c**) text color—red, background color—black and (**d**) text color—green, background color—black.

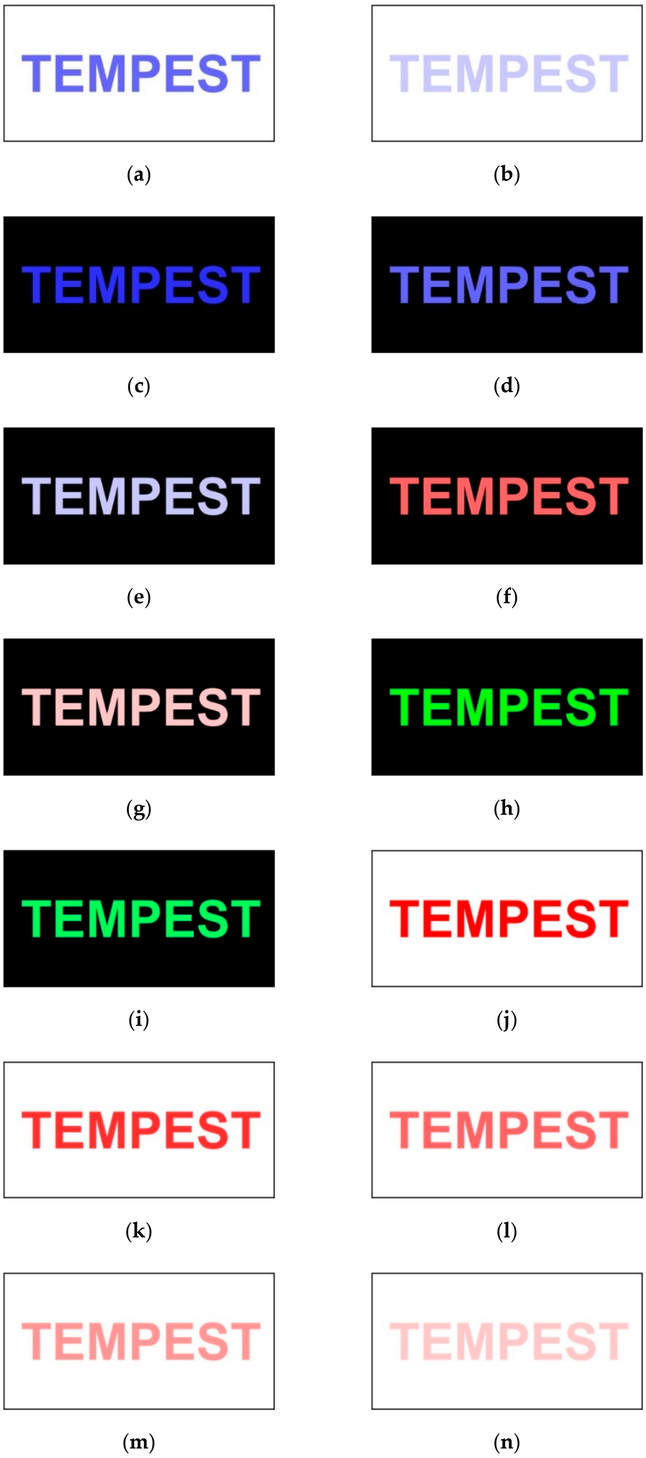


Figure 14. Examples of pairs of colors for which the effectiveness of electromagnetic infiltration process is limited: (**a**) text—(100, 100, 255), background—(255, 255, 255), (**b**) text—(200, 200, 255), background—(255, 255, 255), (**c**) text—(50, 50, 255), background—(0, 0, 0), (**d**) text—(100, 100, 255), background—(0, 0, 0), (**e**) text—(200, 200, 255), background—(0, 0, 0), (**f**) text—(255, 100, 100), background—(0, 0, 0), (**g**) text—(255, 200, 200), background—(0, 0, 0), (**h**) text—(50, 255, 50), background—(0, 0, 0), (**i**) text—(100, 255, 100), background—(0, 0, 0), (**j**) text—(255, 0, 0), background—(255, 255, 255), (**k**) text—(255, 50, 50), background—(255, 255, 255), (**l**) text—(255, 100, 100), background—(255, 255, 255), (**m**) text—(255, 150, 150), background—(255, 255, 255) and (**n**) text—(255, 200, 200), background—(255, 255, 255).

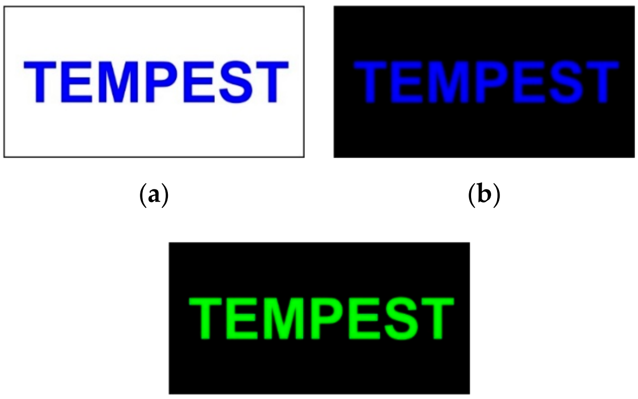
However, a careful analysis of the results obtained from examining the projector as a source of undesirable emissions shows that the method of colors does not always have to be effective for the selected pairs of colors. This is due to the complexity of the radiation source, that is the projector. This means that its radiation properties are highly dependent on the frequency at which the revealing emissions occur.

A properly selected pair of colors can reduce the level of measured emissions at one frequency, while at another frequency the measured level of this emission may remain unchanged. The method of colors can therefore reduce the number of incidences of undesirable emissions.

The second important conclusion related to the research carried out using the method of colors is the possibility of increasing the radiation efficiency of the revealing emission source. Figure 14 shows examples of colors of text and background that can counteract electromagnetic infiltration. However, color pairs with different properties may be selected. This property leads to increased susceptibility to electromagnetic infiltration. This phenomenon is beneficial from the point of view of research related to the assessment of devices designed to process classified information (in accordance with the SDIP-27/2 document [3]). In this case, it is necessary to put the device under test into the operating mode, characterized by the most effective property of radiating the energy of the electromagnetic field. The method of colors turns out to be very advantageous in this regard. It is possible to choose such pairs of colors (text and background) for which the measured revealing emission creates very good conditions for obtaining of processed graphic information in non-invasive way. During the research, several such pairs were selected, which are included in Table 3, and their graphical representation is presented in Figure 15.

Table 3. Combination of colors for text and background for which the effectiveness of the electromagnetic infiltration process increases.

Frequency of Revealing Emission	Text Color RGB	Background Color RGB
520 MHz (Figure 15a,b)	0, 0, 255	255, 255, 255
	0, 0, 255	0, 0, 0
520 MHz (Figure 15c)	0, 255, 0	0, 0, 0



(**a**) (**b**) (**c**)

Figure 15. Examples of pairs of colors for which the effectiveness of electromagnetic infiltration process increases: (**a**) text—(0, 0, 255), background—(255, 255, 255), (**b**) text—(0, 0, 255), background—(0, 0, 0) and (**c**) text—(0, 255, 0), background—(0, 0, 0).

5. Conclusions

This paper presents the risks associated with the use of projectors used to present data subject to electromagnetic protection. The tests of revealing emissions were carried out in two independent research laboratories, as described in Section 3. Three types of projectors from NEC, ASUS and EPSON were tested, using different technologies for transferring the image from the computer to the screen.

Data transmission between the projectors and the computer took place via graphic interfaces based on the VGA and HDMI standards. Since projectors as well as computers and other connected devices like laser printers, projectors, monitors, multifunction devices and voice over Internet protocol (VoIP) phones are subject of manipulating sensitive information, they also have to be tested by Tempest procedures as well. The obtained test results confirmed the assumptions that the projector is a source of undesirable emissions. Such emissions occurred in the frequency range from 200 MHz to 1.5 GHz. The levels of registered revealing emissions made it possible to reconstruct the information. In addition, the use of the image summation algorithm significantly improved the image quality, by increasing the signal-to-noise ratio(SNR) values, and the data contained in it became very clear.

Two solutions were proposed to counteract the possibility of electromagnetic infiltration of projectors:

- the safe fonts;
- the method of colors.

The safe fonts were introduced in Patent (No. P.408372) and analyzed in [6,31], but only with black fonts on white background, never in combination with the method of colors. While safe fonts directly counteract the formation of valuable revealing emissions (drawings), the method of colors can have two applications. The first is to counteract electromagnetic infiltration, while the second is to increase the efficiency of radiation, thus increasing the efficiency of the electromagnetic infiltration process. The second solution may be a forcing signal proposal for tests carried out according to SDIP-27/2 [3] because the assessment of devices processing classified information should be carried out for the least favorable operating mode with respect to the effectiveness of protection against electromagnetic penetration.

The conducted research has shown that, in RGB system, we can select color pairs for which the processed text is more protected than for other pairs of colors. An example of such color combinations is: 200, 200, 200 (text) and 255, 255, 255 (background). Another more user-friendly pair is 50, 255, 50 (text) and 0, 0, 0 (background).

Research in the field of meeting the requirements of the SDIP-27/2 [3] document requires that the device under evaluation should work in high efficiency conditions as a source of undesirable emissions. For this purpose, the appropriate operating mode of the device must be indicated. In the case of testing graphic imaging devices, it must be a reference signal for forced operation e.g., of a monitor. The solution in this area could be the method of colors. As shown in chapter 4, selecting the appropriate color pair can result in high performance of the monitor as a source of radiated emissions correlated with the displayed information. The ideal solution is to select a pair of 0, 0, 255 (text) and 0, 0, 0 (background, Figure 12b) or 50, 50, 50 (text) and 0, 0, 0 (background, Figure 13b).

However, computer users do not always use the RGB color mode. The Cyan-Magenta-Yellow color model (CMY) is also a very frequently used, that uses other primary colors that may have a different effect than the RGB color mode on the effectiveness of the electromagnetic infiltration process, as shown in Figures 16 and 17. This is an example showing a case of using cyan on a black background for text editing. The measured emission at 910 MHz shows that, in this case, the properties of the method of colors may have also an effect on the level of protection of the information against electromagnetic penetration. As a future work, we intend to perform further research in this area.

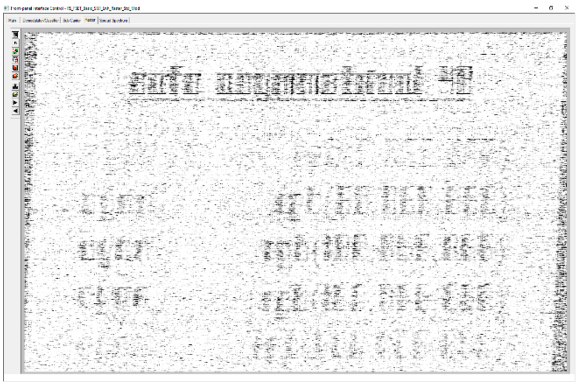


Figure 16. A reconstructed image on based on valuable emission measured on frequency f_o = 910 MHz: Safe asymmetrical font, dimension 48p., text color—cyan, background color—black.

Figure 17. A time course of a valuable emission measured on frequency f_o = 495 MHz: A marker 1—cyan color, a marker 2—amagenta color, a marker 3—yellow color, background color—black.

6. Patents

The safe symmetrical and the safe asymmetrical fonts are new computer fonts. Due to the universality of their use and the acceptance of the potential users, works on improving the shapes of the characters are still being continued. Despite the high level of similarity between the characters, each safe font can be used in the secure processing of information. These fonts have obtained the protection of the Polish Patent Office in the form of Industrial Design (No. 24487) [30] and Patent (No. P.408372) [31].

Author Contributions: Conceptualization, A.B., I.K. and A.P.; methodology, A.B., I.K. and A.P.; validation, A.B., I.K. and A.P.; formal analysis, A.B., I.K., S.H., A.P. and A.S.; investigation, A.B., I.K. and A.P.; resources, A.B., I.K., S.H. and A.P.; writing—original draft preparation, A.B., I.K. and S.H.; writing—review and editing, A.B., I.K., S.H. and A.S.; visualization, A.B., I.K. and A.S.; supervision, I.K. and S.H.; project administration, S.H. and I.K. 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. TEMPEST and EMS Policy. Available online: https://www.ncsc.gov.uk/information/tempest-and-ems-policy (accessed on 13 October 2020).
2. *Information Assurance Security Guidelines on Accreditation of EU TEMPEST Companies*; Council of the European Union, The General Secretariat: Brussels, Belgium, 2019. Available online: https://data.consilium.europa.eu/doc/document/ST-7887-2019-INIT/en/pdf (accessed on 16 November 2012).

3. *NATO Standard (2009) SDIP-27/2: NATO TEMPEST Requirements and Evaluation Procedures*; (Published March 2016 but not for Publicuse, NATOCONFIDENTIAL); NATO Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN), Supreme Headquarters Allied Powers Europe (SHAPE): Mons, Belgium, 2009.
4. *EU Standard (2013) IASG 7–03: Information Assurance Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures*; (Published March 2016 but not for Publicuse, EUCONFIDENTIAL); General Secretariat of the Council of the European Union (GSC): Brussels, Belgium, 2013.
5. 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.
6. Kubiak, I. Font Design—Shape Processing of Text Information Structures in the Process of Non-Invasive Data Acquisition. *Computers* **2019**, *8*, 70. [CrossRef]
7. Ulas, C.; Sahin, S.; Memisoglu, E.; Asık, U.; Karadeniz, C.; Kılıc, B.; Sarac, U. Automatic Tempest test and analysis system design. *Int. J. Cryptogr. Inf. Secur.* **2014**, *4*, 1–12. [CrossRef]
8. Kuhn, M.G. *Compromising Emanations: Eavesdropping Risks of Computer Displays*; Technical Report No.577; UCAM-CL-TR-577; University of Cambridge: Cambridge, UK, 2004.
9. Zhang, N.; Lu, Y.; Cui, Q.; Wang, Y. Investigation of unintentional video emanations froma VGA connector in the desktop computers. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1826–1834. [CrossRef]
10. Kubiak, I. Video signal level (colour intensity) and effectiveness of electromagnetic infiltration. *Bull. Pol. Acad. Sci. Tech. Sci.* **2016**, *64*, 207–218. [CrossRef]
11. Kubiak, I. Influence of the method of colors on levels of electromagnetic emissions from video standards. *IEEE Trans. Electromagn. Compat.* **2018**, *61*, 1129–1137. [CrossRef]
12. Boitan, A.; Bărtușică, R.; Halunga, S.; Bîndar, V. Video signal recovery from the laser printer LCD display. In *Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies, IX*; Proceedings of SPIE: Bellingham, WA, USA, 2018; Volume 10977, p. 1097726. [CrossRef]
13. 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]
14. 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. Available online: https://www.wil.waw.pl/artprac/Emission_security_of_laser_printers.pdf (accessed on 13 October 2020).
15. Kubiak, I. Laser printer as a source of sensitive emissions. *Turk. J. Electr. Eng. Comput. Sci.* **2018**, *26*, 1354–1366. Available online: https://pdfs.semanticscholar.org/3d8d/c38f55f1636a4f7dc62c90d4fca567f0f4e1.pdf (accessed on 13 October 2020). [CrossRef]
16. Vuagnoux, M.; Pasini, S. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In Proceedings of the USENIX Security Symposium, Montreal, QC, Canada, 10–14 August 2009; pp. 1–16. Available online: https://static.usenix.org/events/sec09/tech/full_papers/sec09_attacks.pdf (accessed on 13 October 2020).
17. Boitan, A.; Bărtușică, R.; Halunga, S.; Popescu, M.; Ionuță, I. Compromising Electromagnetic Emanations of Wired USB Keyboards. In *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*; Springer: Cham, Switzerland, 2017; pp. 39–44. [CrossRef]
18. Rognean, X.; Rosu, G.; Boitan, A.; Trip, B.; Butnariu, V.; Kasmi, C.; Fichte, L.O.; Baltag, O. Study of Compromising Emissions of PS/2 Keyboards by Correlative Methods. *Rev. Roum. Des Sci. Tech. Ser. Electrotech. Energetique* **2020**, *65*, 15–20. [CrossRef]
19. Trip, B.; Butnariu, V.; Velicu, V.; Halunga, S.; Boitan, A. Analysis of PS/2 Compromising Emanations. In *International Conference Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies (ATOM202020—23 August 2020, Constanta, Romania)*, 10th ed.; in press.
20. Smulders, P. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Comput. Secur.* **1990**, *9*, 53–58. [CrossRef]
21. Boitan, A.; Halunga, S.; Bîndar, V.; Fratu, O. Compromising Electromagnetic Emanations of USB Mass Storage Devices. *Wirel. Pers. Commun.* **2020**, 1–26. [CrossRef]

22. Wampler, C.; Uluagac, S.; Beyah, R. Information leakage in encrypted IP video traffic. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–7.
23. Idita, A.; Butnariu, V.; Rosu, G.; Trip, B.; Boitan, A.; Baltag, 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; pp. 1–6.
24. Lee, H.K.; Kim, Y.H.; Kim, S.C. Emission security limits for compromising emanations using electromagnetic emanation security channel analysis. *IEICE. Trans. Commun.* **2013**, *96*, 2639–2649. [CrossRef]
25. 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 2017 International Symposium on Electromagnetic Compatibility—EMCEUROPE, Angers, France, 4–7 September 2017; pp. 1–4.
26. International Telecommunications Union. *Mitigation Methods Against Electromagnetic Security Threats*; SeriesK: Protection Against Interference; Recommendation K.115,11/2015; Telecommunication Standardization Sector of ITU: Geneva, Switzerland, 2015.
27. Xie, C.H.; Wang, T.; Hao, X.; Yang, M.; Zhu, Y.; Li, Y. Localization and Frequency Identification of Large-Range Wide-Band Electromagnetic Interference Sourcesin Electromagnetic Imaging System. *Electronics* **2019**, *8*, 499. [CrossRef]
28. Lee Ko, W. Time domain solution of electromagnetic problems. *Electromagnetics* **1992**, *12*, 403–433. [CrossRef]
29. Boitan, A.; Bătuşică, R.; Halunga, S.; Fratu, O. Electromagnetic Vulner abilities of LCDP rojectors. In *Proceedings of the 6th Conference on the Engineering of Computer Based Systems, Bucharest, Romania, 2–3 September 2019*; University Politechnicaof Bucharest: Bucharest, Romania, 2019; pp. 1–6. [CrossRef]
30. Kubiak, I. *Computer Font Resistance to Electromagnetic Infiltration. The Research and Analysis Results*; Publishing House of the Military University of Technology: Warsaw, Poland, 2014.
31. Kubiak, I.; Boitan, A.; Halunga, S. Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers. *Appl. Sci.* **2020**, *10*, 2828. [CrossRef]