Steganography of vector graphics and typography in infrared security printing

Tajana Koren Ivančević, Maja Rudolf, Nikolina Stanić Loknar

University of Zagreb Faculty of Graphic ArtsGetaldićeva 2, 10 000 ZagrebCroatia, E-mail: tkoren@grf.hr

Abstract

The paper elaborates on linear graphics and typographic elements in the function of hiding information in security printing. Hidden information is introduced with the goal to protect the originality of the produced graphic designs so their counterfeiting would be impossible. Those graphic designs are made with programmed linear and typographical elements that have different response in the part of the spectrum visible to the human eye, and in the near infrared part of the spectrum observed with instruments. In order to have different response in the said spectrum parts, in each of the two designs colors are separated in two different ways. In order to achieve unique results, complex algorithms and random numbers are used for color separation. Unique graphic designs have been obtained by merging design and security against counterfeiting.

Keywords: Security elements, CMYKIR, near infrared spectrum, typography, vector graphic

1 Introduction

The paper is a further link to many years of researching dye response in the near infrared part of the spectrum. The theory on different color response for the part of the spectrum that is visible to the eye, and that of the near infrared area was developed in 2009 under the name CMYKIR separation (V. Žiljak et al, 2009). From that moment to date the theory has been further developed and continuous application is being found in various graphic industry fields (V. Žiljak et al, 2011; I. Žiljak et al, 2009; Friščić et al, 2015). Research in the field of Infraredesign is divided into several phases. One phase is preparing the coloring agent for specific printing conditions (V. Žiljak et al, 2012), and another phase is making the design that contains double information. This paper is focused on design issues and planning of security graphics. New algorithms are developed that have the goal to accelerate the process of security element generating on one hand, and by applying stochastics - to lessen the influence of the human factor during the very process of designing, on the other hand (Koren et al, 2008). It is also shown in the paper how to program security elements to be hidden to the human eye, and visible with the help of instruments. Steganography in security printing is achieved by controlled application of the black component with CMYKIR separation in positions set with the help of algorithms. The relation between typography and linear graphics is researched as a supplement to former works (Koren et al, 2010; Koren Ivančević et al, 2015). Typographical elements and linear graphics of very fine liniature have been used, as well as rosettes derived from them. Such linear graphics are difficult to counterfeit from the start because they contain several security features (Pap et al, 2014). Very thin lines in securities have a fine linear structure possible to produce only with very high quality printing techniques. They are programmed with Bezier's curve in such a way that besides repetition, they have variable elements such as altering tension points or various transformations. With CMYKIR separation it was achieved to make one graphic visible to the human eye, and the other in the near infrared part of the spectrum. A third security element was introduced during the process of their programming, - a different picture in the visible field and another in the infrared part of the spectrum. The fourth security element is hidden in pseudo-random numbers. They are used when programming line and typography positions, but also for color separation. In some designs random values are used for all the four colors (CMYK), while the values for certain components in other designs are precisely set through different parameters. When observing a graphic design, elements visible in the near infrared part of the spectrum are not visible or apparent to the human eye, but are merged with the overall. There are five solutions shown in the paper for securing information in infrared printing.

2 Experimental part

Experiments in security design are elaborated in programming language Postscript, combining typography and Bezier's curves. Each one of the letter character parameters and vector elements, such as position, color and size are available for mathematical manipulation. Stochastic parameter alteration is applied in graphics planning for the visible part of the spectrum, while planning for the graphics in infrared part of the spectrum remains in strictly set values. Font Minion Pro Medium is used in all given examples.

2.1 Letter character mask filled with random characters

In the first experiment the letter "a" is filled with randomly generated letter characters. Besides having an irregular rhythm of appearing, letter characters are programmed in such a way that the values for the C, M, and Y channels are pseudo-random numbers. They are controlled by a seed parameter obtained with the congruential method of generating random numbers. By observing the thus filled letter "a" with the naked eye, it is not possible to spot any meaningful message or word in the shown multitude of letter characters (Figure 1). By observing the C, M, and Y channels, it is also apparent that the letter characters have random response in one of the channels, i.e. in several channels, depending on the random value that the certain channel had acquired in the repeating process (Figure 2).

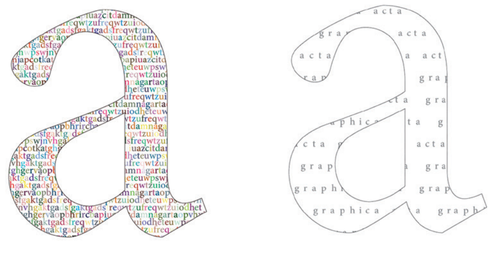

Figure 1. Letter character "a" mask filled with random letter characters, visible to the human eye at the left and the picture visible in the NIR part of the spectrum at the right

The letter characters shown in channel K are programmed separately from the CMY channels, so that only they would be visible with the help of instruments in the near infrared part of the spectrum (NIR) (Figure 1 right).

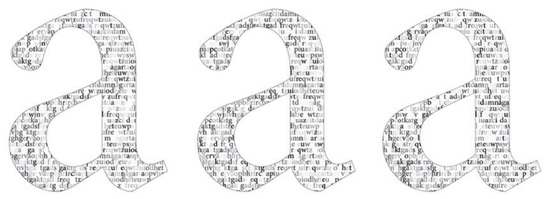

Figure 2. Letter character "a" mask through C, M, and Y channels, from left to right

Figure 3 shows what would happen should anyone try to reproduce a design secured in the described way. By scanning the picture from the paper, it is translated into the RGB color system. By converting the picture back to the CMYK system, there is different channel separation and there is no trace of any coherent message.

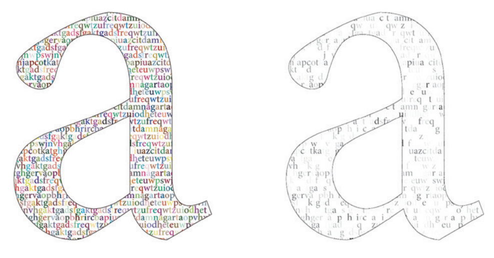

Figure 3. Wrong separation by switching from RGB to CMYK system

2.2. Rosette formed linear graphic as a security element

This example shows two letter characters filled with the same very thin line graphic in rosette form (Figures 4 and 5). In both of the examples the C, M, and Y channel values are random, but there is a different algorithm in the K channel separation. The black channel K is a variable with an initial value of 0 in the first example (Figure 4), and it is gradually increased with each line repetition until it reaches the maximum coverage value of 100%. The NIR response simulation is shown in Figure 4 on the right. Figure 5 shows a version of the same rosette where black (K) is separated as C, M, and Y, i.e. with random choice between the minimum (0%) and maximum coverage value (100 %). The two pictures observed in daylight or through the separation of C, M, and Y channels do not show any visible or apparent differences, whereas there is a completely different distribution visible in channel K (Figure 4 right and 5 right).

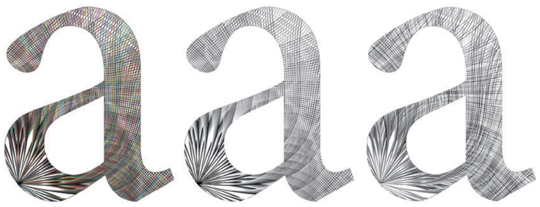

Figure 4. Letter mask on rosette with C, M, and Y random coverage values, with gradient rise in K coverage values. Left: CMYK, right: black channel response simulation in the NIR part of the spectrum

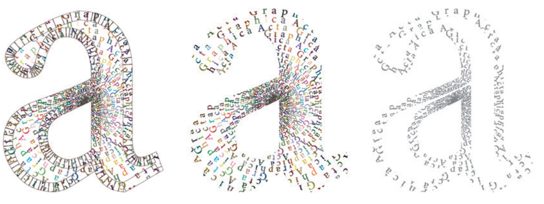

Figure 5. Letter mask on rosette with C, M, Y, and K random coverage values. Left CMYK, right: response simulation of the black channel in the NIR part of the spectrum

2.3 The letter charater and its outline filled with text

In this example the letter character and its outline are filled with a repeating text (Figure 6). For easier understanding the first example has a stroked thick outline so that there would be a clearly noticeable difference in the separation of the CMYK and CMYKIR (Figure 6 left).The text “Acta Graphica” fills the mask of the letter character as well as that of the outline spreading itself along an imagined spiral and diminishing in size with each repetition. Even though it is not observed with the naked eye, the text filling the letter character “mask” is separated differently in comparison to the text that fills the outline of that mask. In both cases pseudo-random numbers were used in color parameters with stochastic altering in each letter sign of the written text. Stochastic choice of coverage values was used in C, M, and Y channel separation in the complete mask area, while the black component was separated differently within the outline and the mask filling. In the filling of the character the K component is completely eliminated in the separation, and its value is always 0%. The value is constant in the letter character outline and amounts to 50% of the full tone. When observing the K channel, only the text in the letter character outline is seen clearly, while there is no response of the filling in the infrared part of the spectrum (Figure 6 right).

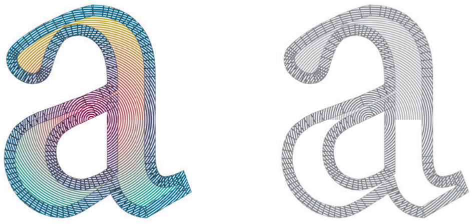

Figure 6. Letter character mask in the visible part of the spectrum with different black separation in the outline and filling (left and middle), and response simulation in the NIR part of the spectrum (right)

2.4 The letter character filled with linear graphics and altering color

In this example there is also experimenting with different CMYKIR separation settings for the outline and the filling of the letter character. Both the letter and its outline are filled with concentric circles of very fine liniature. The concentric circles are differently colored going from the center to the periphery along the x axis, and differently along the y axis, where color changes from magenta into yellow upwards and from magenta to cyan going downwards (Figure 7 left). The algorithm allows color parameter manipulation in all directions as gradation, and shown in the enclosed example, or stochastically. Figure 7 right shows separation of the black channel that will be seen in NIR (the letter character outline and part of the letter character mask concentric circles). Figure 8 displays separation of the remaining three channels (CMY) after adjusting the parameters for the desired colors in the visible part of the spectrum. Figure 9 shows the possible algorithm modifications from the previous example where only a part of the circles are seen in the infrared part, while the mask is fully hidden. In this way only the upper letter character mask filled with thin concentric circles is shown.

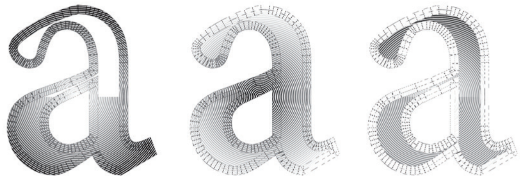

Figure 7. Letter character filled with concentric circles with changing colors, left: CMYK, right: simulation of response in NIR

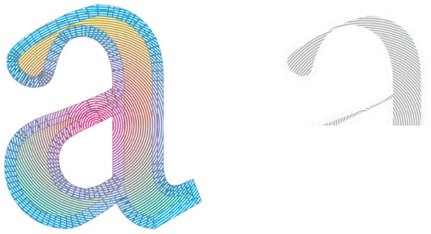

Figure 8. Separation of C, M, and Y channels from the example in Figure 7

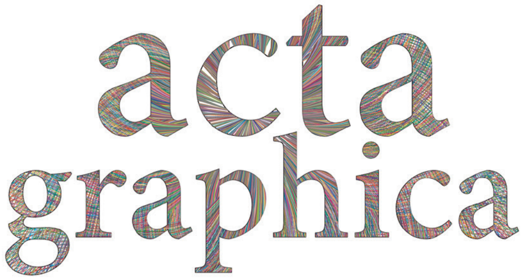

Figure 9. Letter character filled with concentric circles, with change of color. Left: CMYK, right: simulation of response in NIR

2.5 The rosette text mask

The text “acta graphica” is set as a mask of a very complex rosette that has three differently programmed parts, consisting of Bezier’s curves with repetition and parameter altering, i.e. altering of tension points (Figure 10). In this way each letter character of “acta” and “graphica” seems to be filled with different curves or graphics. In two examples (Figure 10 and Figure 12) black channel is separated differently in order to demonstrate entirely different solutions obtained by parameter change in the channel separation algorithms.

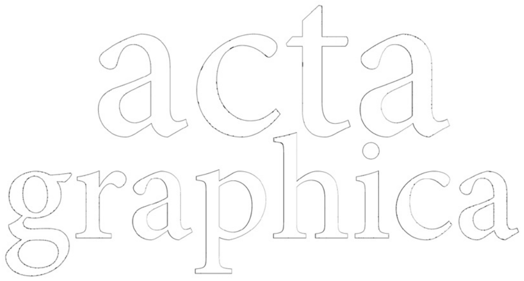

Figure 10. Text mask on rosette CMYK

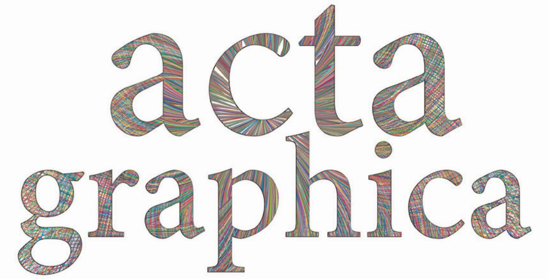

Figure 11. Response simulation Figure 10 in NIR

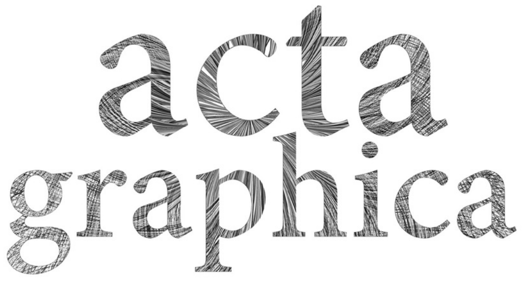

Figure 12. Text mask on rosette with eliminated K component CMYK

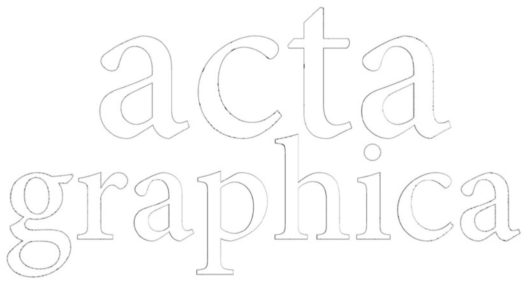

Figure 13. Response simulation Figure 12 in NIR

Pseudo-random numbers were used in the first example (Figure 10) for all the four colors, resulting in the NIR as random line reproduction (Figure 11). In the second example (Figure 12), the K component is completely eliminated from color separation in the rosette, resulting as only a thin outline around the text (Figure 13).

3. Conclusion

The solutions shown in the paper have multiple application possibilities in protecting securities or other graphic elements prone to counterfeiting. It is not possible to derive such solutions without knowing the CMYKIR theory. The targeted different separation for the visible part and the infrared part of the spectrum disappears by scanning, i.e. changing into the RGB color system. Pseudo-random numbers used for color separation make them unique and unrepeatable. The use of printing elements with programmed text messages visible only in the infrared part of the spectrum opens the possibility of application on any graphic product because it is possible to adapt the letter character combination to the purpose of the product that needs to be secured. This experiment shows that there is possibility of development in the field of infrared area security graphics and creative design of graphic solutions with the help of complex algorithms.

4. References

1. Žiljak V., Pap K., Žiljak I., 2009. CMYKIR security graphics separation in the infrared area. Infrared Physics and Technology, Vol. 52, 2-3; pp: 62-69
2. Žiljak, V. Pap, K. Žiljak-Stanimirović, I., 2011. Development of a prototype for zrgb infraredesign device. Technical Gazette, 18, 2; pp: 153-159
3. Žiljak I., Pap K., Žiljak Vujić J., 2009. Infrared design on textiles as product protection. Tekstil, Vol. 58 No. 6, pp: 239-253
4. Friščić, M., Žiljak Vujić, J., Žiljak, V., 2015. CMYKIR Separations for Printing on Transparent Polymer Materials. Acta Graphica, 26(3), pp: 16-22
5. Žiljak V., Pap K., Žiljak-Stanimirović I., Žiljak-Vujić J., 2012. Managing dual color properties with the Z-parameter in the visual and NIR spectrum. Infrared physics & technology, Vol.55, 4; pp: 326-336
6. Koren T., Stanić N., Rudolf M.,2008. Understanding random numbers through Postscript. Proceedings of the Design 2008, Workshop Design of Graphic Media, ed. Žiljak V.; pp: 1487-1490
7. Koren T., Žiljak Stanimirović I., Politis A.E., Barišić M., 2010. The steganography of the typography in the digital printing technology. Proceedings of the 11 th International Design Conference Design 2010, Workshop: Design Graphics with security elements, ed. Žiljak V., Milčić D.; Vol.4, pp: 1897-1902
8. Koren Ivančević T.; Stanić N.; Rudolf M., 2015. Programming typographic elements for infrared security printing, Proceedings Tiskarstvo & Dizajn 2015, pp: 250-257
9. Pap K., Stanić Loknar N., Rudolf M., Koren T., 2014. Security graphics by Postscript management of lines and typography. Proceedings of 18th International Conference on Printing, Design and Graphic Communication Blaž Baromić 2014, ed. M. Mikota , pp: 228-238