



ELSEVIER

1 June 2000

OPTICS
COMMUNICATIONS

Optics Communications 180 (2000) 15–20

www.elsevier.com/locate/optcom

A new optical random coding technique for security systems

Zeev Zalevsky, David Mendlovic^{*}, Uriel Levy, Gal Shabtay

Tel-Aviv University, Faculty of Engineering, Department of Electrical Engineering, 69978 Tel-Aviv, Israel

Received 11 October 1999; received in revised form 19 January 2000; accepted 3 April 2000

Abstract

A novel technique for random optical encoding is suggested. The proposed technique is based upon two binary masks: an encoding mask and a decoding mask. Each mask in itself is random, and contains no information that may be decoded. Only when the two masks are joined together, the decoded information is revealed. This way, the encoding of gray level as well as color information is possible. This approach is especially suitable for security applications. © 2000 Published by Elsevier Science B.V. All rights reserved.

1. Introduction

The need to encode information, in a way that will make it immune to decoding by unauthorized persons, exists for thousands of years. Recently, due to their parallelism and high spatial resolution, a few interesting encoding techniques were investigated and implemented by optical means. Some of these techniques are described in Refs. [1–5]. Ref. [1] uses a phase encoded joint transform correlator (JTC) to decode the encrypted image with the same random phase mask used in the encryption procedure. Ref. [2] proposes a security verification method using a

transform random phase masks as an optical mark bonded to a document or other product. This mask consists of separated and shifted fragments of a reference phase mask. Ref. [3] presents a security verification system consisting of holographic security emblem in which information is covertly stored and an automated reader based on a JTC. A holographic encoding method is used to produce an emblem that stores the required phase and/or amplitude information in the form of a complex 3-D diffraction pattern that can only be interpreted through the use of a second ‘key’ hologram. Ref. [4] suggests to use a new, phase only encryption technique, that is based on a phase coding method. This method uses a generalization of the Zernike phase contrast technique, but overcomes the small phase angle limitation of the Zernike method. An experimental demonstration of this phase coding technique for image formation has been introduced by Ref. [5]. In this approach, the spatial average value of an

^{*} Corresponding author. Fax: +972-3-642-3508; e-mail: mend@eng.tau.ac.il

input phase modulated image is combined with pre estimated phase retardation reduced by a phase contrast filter.

Hereby, we suggest a technique which reconstructs information from two random spatial masks. The first mask encodes the desired information while the second mask serves as a decoding mask. Each mask in itself is completely random, and therefore encoding is extremely complicated. Only when both masks are simultaneously used, the encoded information is revealed. Only when the exact encoding and decoding masks are used, exact reconstruction of the hidden information is obtained. The following approach is suitable for the encoding and decoding of gray level as well as color information. In addition, it can be used as a tool to encrypt the transmission of temporal signals, making it especially useful for security applications.

2. Encoding procedure

The image to be encoded is divided into rectangular pixels. Within each such a pixel, a corresponding binary rectangle is plotted. The decoding mask is built out of rectangles having random widths in both dimensions and a random position within a predefined region of the specific pixel that is being decoded. The encoding mask contains the same random rectangles as well. Their positions are matched to the positions and widths of the decoding rectangles such that the multiplication between the two masks results in the desired gray level of that specific pixel in the encoded image. Observing the schematic Fig. 1, one may see that the amount of overlap between the

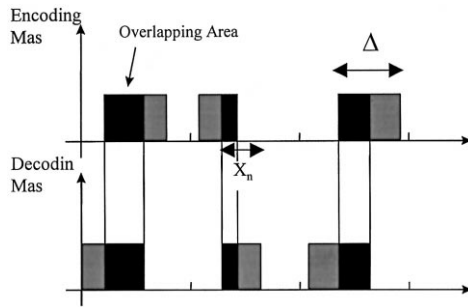


Fig. 1. Schematic plot of the technique.

specific rectangles in the encoding and decoding masks is proportional to the gray level of the specific pixel of the encoded image. If no overlap exists, the multiplication in that specific pixel yields a zero value. Otherwise, the energy of that pixel after the multiplication corresponds to the overlapping area. Thus, the spatial resolution used for the positioning of those rectangles within the pixel must correspond to the number of gray-scale values that exist within the encoded image. Mathematically, one may write the following expression for each (n,m) pixel of the decoding mask:

$$DM_{n,m}(x,y) = \text{rect}\left(\frac{x - x_n - n\Delta}{\Delta_{x_n}}, \frac{y - y_m - m\Delta}{\Delta_{y_m}}\right) \quad (1)$$

where $\Delta_{x_n}, \Delta_{y_m}$ are the widths of the binary rectangle, x_n and y_m are its horizontal and vertical position within the pixel's region, respectively, and Δ is the pixel's width and height. All those variables (besides Δ) are random variables with uniform probability density function. The fact that those parameters are randomly distributed, drastically reduces the probability of decoding the information without the decoding mask.

Denoting by $g(n,m)$ the image to be encoded, one may write the expression for the encoding mask as:

$$EM_{n,m}(x,y) = \text{rect}\left(\frac{x - x_n - n\Delta + \Delta_{x_n} - \Delta_{x_n}\sqrt{g(n,m)}}{\Delta_{x_n}}, \frac{y - y_m - m\Delta + \Delta_{y_m} - \Delta_{y_m}\sqrt{g(n,m)}}{\Delta_{y_m}}\right) \quad (2)$$

where $g(n,m)$ is normalized to unity.

The rectangle dimensions must be restricted to the region $(1/4)\Delta \leq \Delta_{x_n}, \Delta_{y_m} \leq (1/2)\Delta$ in order to achieve reasonable light efficiency on one hand, while on the other hand avoiding overlap between neighboring pixels. The requirement for neighboring pixels to be separated also leads to the following condition: $|x_n| \geq (3\Delta_{x_n} - \Delta/2), |y_m| \geq (3\Delta_{y_m} - \Delta/2)$.

This way the following equation may be written for the energy of the overlapping area between the two masks:

$$\iint_{(x,y) \in \text{pixel}(n,m)} EM_{n,m}(x,y) \times DM_{n,m}(x,y) dx dy = g(n,m). \quad (3)$$

As mentioned earlier, the number of gray levels is proportional to the positioning accuracy of the plotting device. Keeping in mind that a complete overlap yields the maximal number of gray level value, while non-overlapping areas yield a minimal gray level value, the number of gray levels is given by:

$$NG = \frac{\min(\Delta_{x_n})}{PS} = \frac{\Delta}{4PS} \quad (4)$$

where NG is the number of available gray levels and PS is the positioning accuracy of the plotting device. Assuming a pixel size of 64 μm and positioning accuracy of 1 μm , 16 gray levels are available.

The optical setup for testing the quality of the reconstructed information is presented in Fig. 2(a). The two masks are joined and the light intensity passing through is proportional to the spatial multiplication between them. This operation reconstructs the decoded information. The decoded information may serve as the input for an optical correlator, which compares it to the reference information and reproduces a correlation peak, which gives an indication of the quality of reconstruction. Another option

is to use a CCD camera in order to grab the obtained image and perform decisions digitally.

Up to now, no propagation distance between the two masks has been assumed. However, they do not need to be physically attached. The two masks may be placed in a certain predetermined distance of Z as seen in Fig. 2(b). In this case the encoding mask should be the inverse Fresnel transform of the mask written in Eq. (2):

$$EM_{n,m}(x,y) = \iint \text{rect} \left(\frac{x_0 - x_n + \Delta_{x_n} - \Delta_{x_n} \sqrt{g(n,m)}}{\Delta_{x_n}}, \frac{y_0 - y_m + \Delta_{y_m} - \Delta_{y_m} \sqrt{g(n,m)}}{\Delta_{y_m}} \right) \times \exp \left[\frac{i\pi}{\lambda Z} \{ (x_0 - x)^2 + (y_0 - y)^2 \} \right] dx_0 dy_0. \quad (5)$$

Since this Z distance is unknown to the intruder, his decoding operation becomes even more complicated. However, in this configuration the encoding mask is not a pure amplitude mask, and may contain phase information as well. Although the production of this mask is more complex, it may be advantageous for security applications.

3. Encoding colored information

A variation on the above method should be used when the spatial information is colored and represented using the RGB representation. In this case, each pixel should be divided into three non-uniform sub regions, representing the red, green and blue information respectively. In each sub region a proper rectangle is plotted. Note that in order to increase the decoding complexity, the colors of the rectangles plotted in the sub regions of the decoding mask may not match the colors of the rectangles in the corresponding sub regions of the encoding mask. However, the overall mixture between the colors of all three sub regions in the encoding and the decoding masks should reproduce the desired color with its proper intensity. For the color information case, each section of the encoding mask can be expressed math-

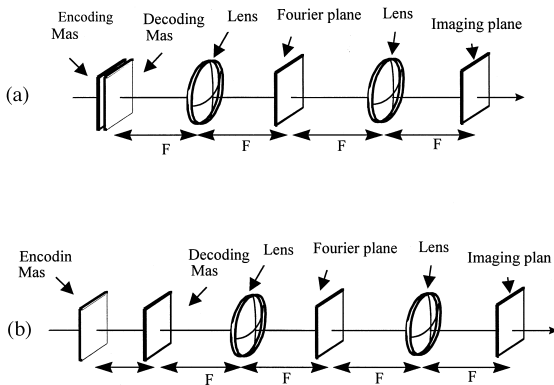


Fig. 2. Two possibilities for optical setup that test the quality of reconstruction.

ematically as:

$$EM_{ni,mi}(x,y) = \text{rect}\left(\frac{x - x_{ni} + \Delta_{x_{ni}} - \Delta_{x_{ni}}\sqrt{g(ni,mi)} - n\Delta}{\Delta_{x_{ni}}}, \frac{y - y_{mi} + \Delta_{y_{mi}} - \Delta_{y_{mi}}\sqrt{g(ni,mi)} - m\Delta}{\Delta_{y_{mi}}}\right) \quad (6)$$

where $i \in [1-3]$ correspond to red, green and blue, respectively.

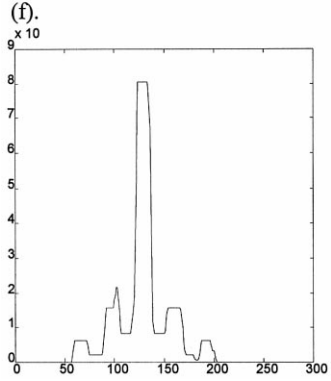
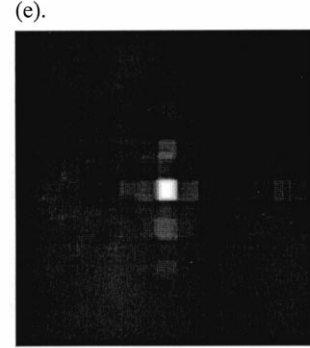
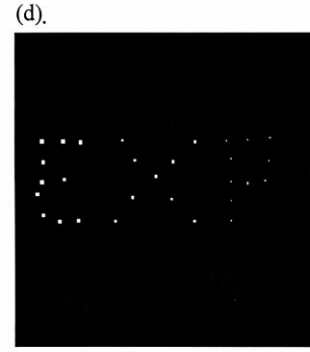
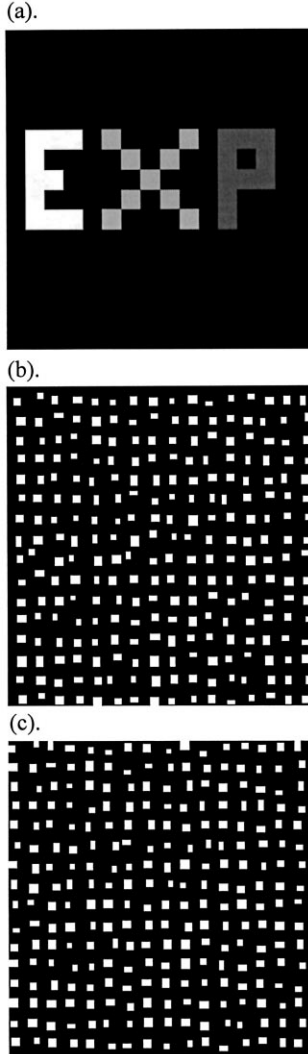


Fig. 3 (continued).

The encoding mask is the sum of its three sections:

$$EM_{n,m}(x,y) = \sum_{i=1}^3 EM_{ni,mi}(x,y). \quad (7)$$

4. Simulations and experiment

In order to test the encoding capabilities of the suggested technique an image consisting of 16×16

Fig. 3. Experimental results: (a) the input image; (b) the encoding mask; (c) the decoding mask; (d) the reconstructed image; (e) the correlation peak; and (f) its cross-section.

pixels was encoded. The image is seen in Fig. 3(a). It has four gray-scale values, equally spaced between zero and unity. The letter 'E' of the image has the gray level of 1, the letter 'X' has the value of $2/3$ and 'P' has a value of $1/3$. The rest of the image has zero gray level. The size of the rectangles was chosen such that the four gray levels could be encoded. The obtained binary encoding and decoding masks are seen in Fig. 3(b) and Fig. 3(c), respectively. Both masks had 256×256 pixels. The digi-

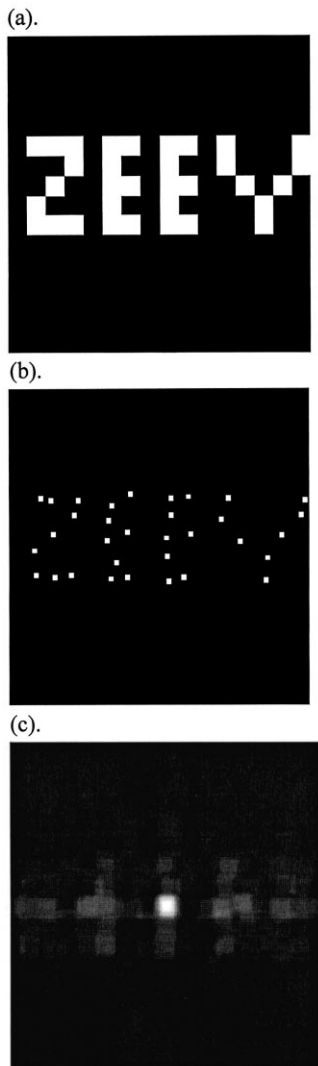


Fig. 4. Additional experimental results: (a) the input pattern; (b) the reconstructed image; and (c) the correlation plane.

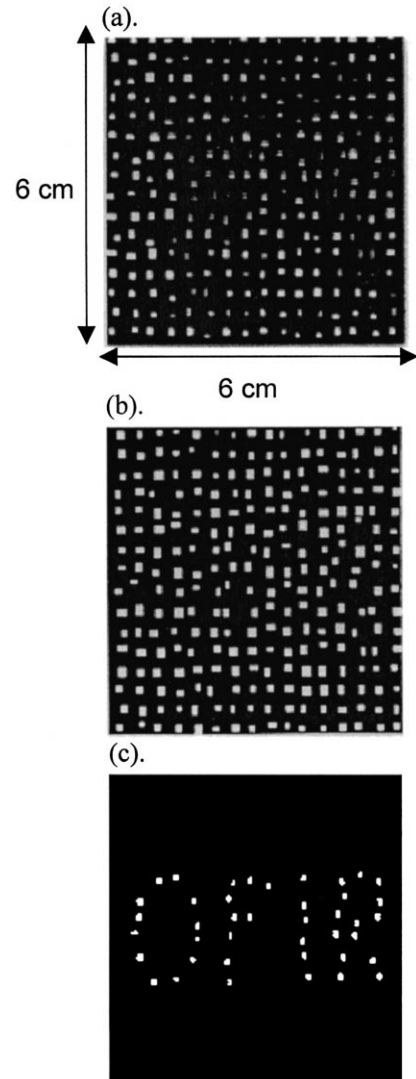


Fig. 5. Optical experiment: (a) the encoding mask; (b) the decoding mask; and (c) the reconstructed image.

tally reconstructed information obtained as a result of attaching (multiplying) the two masks is seen in Fig. 3(d). One may see that the original image was fully reconstructed including its original gray levels (smaller reconstructed rectangles were obtained for the lower gray-scale values of the image). The output detector (a digital detector or a human eye), needs to integrate over each individual (n,m) -pixel to obtain an estimate for a certain gray level. It is clear

however, that for large pixels the random movement might be noticed, which leads to a slightly distorted reconstruction.

The quality of reconstruction was checked by performing a digital correlation test between the original and reconstructed images. This was done using a computer, based on the set up of Fig. 2(a). The correlation plane is presented in Fig. 3(e). The cross-section of the correlation peak is presented in Fig. 3(f). It can be noticed that very sharp peak was obtained, since its width is approximately $256/16 = 16$ pixels (this is the sharpest peak to be obtained for the spatial resolutions presented in this experiment).

A different input image can be seen in Fig. 4(a). A gray level of 1 was used. The image was encoded and decoded using the above-discussed method, and the reconstructed information is seen in Fig. 4(b). The correlation between the reconstructed image and the original one is seen in Fig. 4(c). Note that in this case as well, for images with spatial resolution higher than 16×16 pixels, the rectangles of the reconstructed image will not be seen and their area will be directly translated to the appropriate gray level.

In addition to the above computer simulations, an optical experiment has been carried out based on the set-up presented in Fig. 2(a). The encoded object was the name 'OFIR'. Two 6×6 cm fixed masks with 16×16 pixels were designed and attached to each other. Spatially incoherent white light illumination was used. The encoding and decoding masks can be seen in Fig. 5(a) Fig. 5(b), respectively. The optical reconstruction is shown in Fig. 5(c).

5. Conclusions

To conclude, a novel optical random encoding technique for security systems was presented. The

technique is based upon using two masks: an encoding mask and a decoding mask. Each mask has random information, and therefore the encoded information can be reconstructed only when those two masks are attached together. Although the masks are binary, the encoding of gray level as well as color information is possible. The main advantage of this approach is the fact that it is almost impossible to decode by unauthorized people and has a simplified optical implementation. Experimental results demonstrate the performance of the new technique.

Acknowledgements

The authors wish to thank the Israeli Ministry of Science and the Arts for its support in the framework of the national infrastructure program. Uriel Levy and Gal Shabtay wish to thank the Israeli Ministry of Science and the Arts for the Eshkol fellowship.

References

- [1] T. Nomura, Phase encoded joint transform correlator as an optical encryption decoder, San Diego SPIE Meeting (1998) pp. 246–252.
- [2] L.I. Muravsky, V.M. Fitio, M.V. Shovgenyuk, P.A. Hlushak, Separation of random phase mask in optical correlator for security verification, San Diego SPIE Meeting 3466 (1998) 267–277.
- [3] D.C. Weber, J.D. Trolinger, Novel implementation of non linear joint transform correlators in optical security and validation, San Diego SPIE Meeting 3466 (1998) 290–300.
- [4] P.C. Mogensen, J. Gluckstad, H. Toyoda, T. Hara, Experiments with new phase image encrypting method, SPIE, vol. 3749, ICO18, San Francisco, 1999, p. 274.
- [5] J. Glückstad, L. Lading, H. Toyoda, T. Hara, Lossless light projection, Opt. Lett. 22 (1997) 1373–1375.