Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator

David Abookasis, Ofir Montal, Ohad Abramson, and Joseph Rosen

We describe an electro-optical method of deciphering a watermark from a recently invented encoded image termed a concealogram. The watermark is revealed as a result of spatial correlation between two concealograms, one containing the watermark and the other containing the deciphering key. The two are placed side by side on the input plane of a modified joint-transform correlator. When the input plane is illuminated by a plane wave, the watermark image is reconstructed on part of the correlator's output plane. The key function deciphers the concealed watermark from the visible picture only when the two specific concealograms are matched. To illustrate the system's performance, both simulation and experimental results are presented. © 2005 Optical Society of America

OCIS codes: 090.1760, 070.2580, 070.4560, 050.1950, 070.4550, 100.2810.

1. Introduction

Techniques of information security have received increasing attention recently, as they protect data from unauthorized distribution. Various methods of hiding information[1–5] have been developed by many research groups. One technique to prevent such information burglary is termed digital watermarking[2] and can be useful for preventing illegal duplications. Following the rapid growth of the Internet technologies in early 1990s, digital watermarking and steganography have become major research areas in many applications such as image, audio, and video processing. The goal of these data-hiding techniques[3] is to conceal information such as identification numbers, signatures, and logos within host media, which should not suffer severe degradation. In many proposed methods hiding data entails the use of a secret key that should encrypt and decipher the watermark. This technique must meet several conditions: The embedding of information into images should not alter the visible properties, and the watermark should resist attacks aimed at its removal or modification and should be hard to decipher by an attacker.[4]

Digital watermarking is the process by which a kind of message called a watermark is hidden in a digital file, referred to as the host. However, in most known techniques, when the host file is printed out as a picture, or text, the digital watermark does not survive. The recently invented concealogram[6,7] solves this problem of maintaining watermarks in printed pictures. The concealogram is a method of concealing data in a picture by manipulating the binary representation of continuous-tone images. A binary representation termed halftone coding[8] is commonly used by most printers. The concealed data are not hidden in the paper, ink, or other material used for printing the host picture. The watermark is coded globally by the distances between the dots that compose the complete halftone picture. The watermark is deciphered by cross correlation between the halftone picture and a reference function. The information is hidden in such a way that it prevents the hidden message from being read by unauthorized persons.

In this study we propose a new approach to encrypting watermarks in concealograms and demonstrate a modified electro-optical system for deciphering them. There are three main new elements in this study in comparison with our previous studies.[6,7,9] First, we use an electro-optical correlator as the tool for deciphering watermarks. Electro-optical correlators enable one to decipher pictures in a parallel and fast manner. Of the two main types of electro-optical correlator, the joint-transform correlator[10] (JTC) and the VanderLugt correlator,[11] we chose the former because the JTC requires less restrictive alignment. Second, instead of using phase-only functions[9] as a key with which to decipher the watermark, we use another concealogram. This

The authors are with the Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, P. O. Box 653, Beer-Sheva 84105, Israel. J. Rosen's e-mail address is rosen@ee.bgu.ac.il.

Received 27 February 2004; revised manuscript received 1 June 2004; accepted 7 June 2004.
0003-6935/05/153019-05$15.00/0

means that both binary images in the system are figurative meaningful pictures. The use of binary amplitude holograms enables the correlation to be performed in a simple way by use of simple, low-cost, spatial light modulators (SLMs). Using a figurative key function is an optional feature that opens new applications for the system. Finally, because a JTC is used to read out the watermarks, the encryption method should be modified from the previous methods.[6,7] We use an iterative algorithm called a JTC-based projection onto constraint sets[9] (POCS) for computing two complex functions, which are later encoded to the two concealograms.

The rest of this paper is organized as follows: In Section 2 we discuss the main algorithm for concealing an arbitrary image in a different arbitrary concealogram. Simulation and experimental results are given in Section 3, shown to confirm the proposed method, and followed by concluding remarks in Section 4.

2. Encryption and Deciphering Watermarks

The computation is divided into two stages: (1) Computation of two complex functions, one the encrypted watermark and the other the deciphering function. This computation is guided by an algorithm called JTC-based POCS, described in detail in Ref. 9 and briefly in what follows. (2) Coding the complex functions as two visually meaningful concealograms placed side by side on the JTC input plane.

The first step in our encryption technique is to find a phase function such that, when it is multiplied by the host image and the product is correlated with a particular complex key function, another complex function is generated at the output with a magnitude that is close as possible to the hidden watermark. The POCS algorithm in the present study is based on simulating a JTC in which two phase functions are transformed back and forth between two domains. Appropriate constraints are employed until the functions converge, in the sense that the error between the desired and the obtained images is minimal. The constraints on the JTC input plane are expressed by the need to get two separate, size-limited phase functions; one, the deciphering function, is randomly determined once before the first iteration and the other, the encrypted function, is updated after every iteration. The constraint on the JTC output plane reflects the goal of getting on part of the plane an intensity pattern that is as close as possible to some predefined watermark image. After the iterative procedure is completed, the computer has in its memory two phase functions designed for the specific task of constructing a desired watermark image from the cross correlation between these two functions. The reference key function is fixed during the iterative process and is not related to the first function or to the output watermark image. This function is chosen in the initial step of the iteration and becomes a part of the correlator. Therefore this function does not limit the quantity of host images or watermarks that can be processed by the same key function. To conclude this part of our definition, the first step is accomplished when the correlation between the two phase functions yields a complex function whose magnitude is close enough to the watermark image. A detailed description of the above optimization computation process is found in Ref. 9.

We continue the mathematical description from the point where there are two complex functions, i.e., $g(x, y) = |g(x, y)|\exp[i\theta_g(x, y)]$, the encrypted function, and $h(x, y) = |h(x, y)|\exp[i\theta_h(x, y)]$, the deciphering function, whose phase functions were computed by the JTC-based POCS algorithm, and their magnitudes represent the two chosen figurative images. In the next stage of our process, the goal is to represent the two complex continuous-tone functions by binary valued functions. Following computer-generated hologram techniques,[12] we propose to encode the magnitude within the area of the binary dots and the phase within the dots' positions. Every pixel of the complex gray-tone functions $g(x, y)$ and $h(x, y)$ is replaced by a binary submatrix of size $d \times d$. Inside each submatrix there is a dot represented by some binary value, say, 1, on a background of the other binary value, say, 0. The area of the (k, l)th dot is determined by the value of $|g(x_k, y_l)|$ or $|h(x_k, y_l)|$. The position of the (k, l)th dot inside the submatrix is determined by the value of $\theta_g(x_k, y_l)$ or $\theta_h(x_k, y_l)$. Without loss of generality, we have chosen the shape of the dot as a square, and each dot is translated only along the horizontal axis. Therefore the expression for the binary halftone image becomes

$$\begin{aligned} b(x, y) = {} & \sum\nolimits_{k=-M/2}^{M/2_B} \sum\nolimits_{l=-M/2}^{M/2_B} \\ & \times \mathrm{rect}\left\{\frac{(x - x_1) - d[k + \theta_g(x_k, y_l)/2\pi]}{d[|g(x_k, y_l)|]^{1/2}}\right\} \\ & \times \mathrm{rect}\left\{\frac{(y - y_1) - ld}{d[|g(x_k, y_l)|]^{1/2}}\right\} \\ & + \mathrm{rect}\left\{\frac{(x + x_1) - d[k + \theta_h(x_k, y_l)/2\pi]}{d[|h(x_k, y_l)|]^{1/2}}\right\} \\ & \times \mathrm{rect}\left\{\frac{(y + y_1) - ld}{d[|h(x_k, y_l)|]^{1/2}}\right\}, \end{aligned} \tag{1}$$

where the values of $\theta_g(x_k, y_l)$ and $\theta_h(x_k, y_l)$ are defined in the interval $[-\pi, \pi]$ and the magnitudes range from 0 to 1. The function $\mathrm{rect}(x/a)$ is defined as 1 for $|x| \leq a/2$ and as 0 otherwise. The superscript B in Eq. (1) indicates that the summation is Boolean such that, if two adjacent rect functions overlap, their sum is 1 instead of 2. The two concealograms are displayed side by side; one is around point (x_1, y_1) and the other is around $(-x_1, -y_1)$ on the input plane of the JTC, as shown in Fig. 1.

The two concealograms on the input plane P_1 of the JTC are illuminated by a plane wave and are jointly Fourier transformed by lens L_1 onto focal plane P_2. Following the analysis of the detour-phase computer-generated hologram,[12] the complex amplitude on plane P_2 around point $(f_x, f_y) = (D_x, 0)$, inside a limited

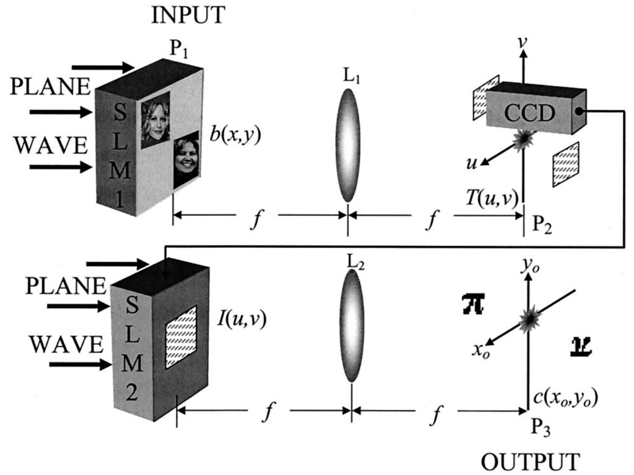

Fig. 1. Schematic of the system for revealing watermarks from concealograms.

frame of the size $\Pi_x \times \Pi_y$, is

$$T(f_x, f_y) \cong \exp\{-i2\pi[(f_x - D_x)x_1 + f_y y_1]\}G(f_x - D_x, f_y) + \exp\{i2\pi[(f_x - D_x)x_1 + f_y y_1]\}H(f_x - D_x, f_y),$$

$$(|f_x - D_x|, |f_y|) \leq \left(\frac{\Pi_x}{2}, \frac{\Pi_y}{2}\right), \quad (2)$$

where $(f_x, f_y) = (u/\lambda f, v/\lambda f)$, u and v are the spatial coordinates of plane P_2, λ is the wavelength of the plane wave, f is the focal length of lens L_1, and the functions $G(f_x, f_y)$ and $H(f_x, f_y)$ are the Fourier transforms of $g(x, y)$ and $h(x, y)$, respectively. The center of the first diffraction order is at point $(\lambda f D_x, 0) = (\lambda f/d, 0)$. The frame size of $\Pi_x \times \Pi_y$ is exactly equal to the bandwidth of the functions $g(x, y)$ and $h(x, y)$, or, in other words, to the size of the functions $G(f_x, f_y)$ and $H(f_x, f_y)$. This size should not exceed the rectangular area $\lambda f/d \times \lambda f/d$.

In our modified JTC, only part of the joint spatial spectrum around point $(f_x, f_y) = (D_x, 0)$ is observed by a CCD that has a limited observation frame equal to the size $\Pi_x \times \Pi_y$. The intensity distribution recorded by the CCD is

$$\begin{aligned} I(\tilde{f}_x, \tilde{f}_y) &= |T(\tilde{f}_x, \tilde{f}_y)|^2 \\ &= \left|\exp\left[-i2\pi(x_1\tilde{f}_x + y_1\tilde{f}_y)\right]G(\tilde{f}_x, \tilde{f}_y) + \exp\left[i2\pi(x_1\tilde{f}_x + y_1\tilde{f}_y)\right]H(\tilde{f}_x, \tilde{f}_y)\right|^2 \\ &= |G(\tilde{f}_x, \tilde{f}_y)|^2 + |H(\tilde{f}_x, \tilde{f}_y)|^2 + \exp\left[-i4\pi(x_1\tilde{f}_x + y_1\tilde{f}_y)\right]G(\tilde{f}_x, \tilde{f}_y)H^*(\tilde{f}_x, \tilde{f}_y) + \exp\left[i4\pi(x_1\tilde{f}_x + y_1\tilde{f}_y)\right]G^*(\tilde{f}_x, \tilde{f}_y)H(\tilde{f}_x, \tilde{f}_y), \end{aligned} \quad (3)$$

where the origin of CCD coordinates $(\tilde{f}_x, \tilde{f}_y)$ is at point $(f_x, f_y) = (D_x, 0)$. The intensity pattern of Eq. (3) is displayed on the second SLM, labeled SLM2 in Fig. 1. This SLM is illuminated by a plane wave such that the Fourier transform of the SLM's transparency is obtained on the back focal plane of lens L_2. Assuming that the focal length of L_2 is identical to that of L_1, the Fourier transform of $I(\tilde{f}_x, \tilde{f}_y)$ yields the following complex amplitude on plane P_3:

$$\begin{aligned} c(x_o, y_o) = {} & g(x_o, y_o) \otimes g(x_o, y_o) + h(x_o, y_o) \otimes h(x_o, y_o) \\ & + g(x_o, y_o) \otimes h(x_o, y_o) * \delta(x_o - 2x_1, y_o - 2y_1) \\ & + h(x_o, y_o) \otimes g(x_o, y_o) * \delta(x_o + 2x_1, y_o + 2y_1), \end{aligned} \quad (4)$$

where $\otimes$ and $*$ denote correlation and convolution, respectively, δ is the Dirac delta function, and x_o and y_o are the coordinates of output plane P_3.

It is evident from Eq. (4) that three spatially separated diffraction orders can be observed. The first two terms are the diffraction zero orders in the vicinity of the origin of the output plane. The third and the fourth terms, at points $\pm 2x_1$ and $\pm 2y_1$, correspond to the cross correlations between the two functions $g(x, y)$ and $h(x, y)$. According to the output results of the POCS algorithm, these cross correlations approximately produce the desired watermark image. Actually, the POCS algorithm computes two phase functions, $\exp[i\theta_g(x, y)]$ and $\exp[i\theta_h(x, y)]$, the cross-correlations between which approximately yield the hidden watermark. However, from many independent experiments we have learned that, as long as the amplitude functions change much more slowly than the phase functions, the amplitude distributions have a negligible influence on the cross-correlation results. Therefore one can retrieve the hidden image by reading it from the vicinity of point $(2x_1, 2y_1)$ or $(-2x_1, -2y_1)$.

It should be emphasized again that our JTC is not the conventional one used for many kinds of pattern recognition.[10] In this JTC we mask the joint spectral plane and process only the first diffraction order in this plane. This procedure enables us to obtain the cross correlation between, effectively, two complex functions, although there are actually two real positive functions in the input plane.

3. Simulation and Experimental Results

The proposed watermark detection was demonstrated first by a computer simulation of the system shown in Fig. 1 and then by an optical experiment with the same system.

In the present simulation the POCS algorithm was tested with an image of the letter π as the hidden watermark pattern. Each of the two gray-tone pictures, one for hosting the watermark and the other for hosting the deciphering key, has a size of 68 × 68 pixels. The convergence of the POCS algorithm to the desired image is evaluated by the average mean-square error between the intensity of the correlation function before and after the corresponding projections (for a definition of this error, see Ref. 9).

After enough iterations of the POCS algorithm have been completed, the computer memory contains two continuous-tone complex-valued matrices, which

Fig. 2. Two concealograms displayed on the simulated modified JTC input plane.

should be binarized according the rule of the concealogram procedure described by Eq. (1). The size of each halftone cell in this study is 11×11 pixels, and the gray-tone image is quantized with 7 levels of magnitude and 11 levels of phase. Both concealograms were located on a larger matrix in a diagonal position, as shown in Fig. 2. The area outside the two concealograms was padded with zeros. The JTC input matrix with the two concealograms was Fourier transformed to the joint spectrum plane shown in Fig. 3; two diffraction orders of the spectral plane, one on either side of the zero order, can be seen in this figure. As only one of these orders is needed, only the squared magnitude distribution, denoted by the white dotted line, is processed further. This intensity was then Fourier transformed again to the output plane. The three orders of the correlation plane containing the letter π in the two first diffraction orders can be clearly seen in Fig. 4, indicating the success of the proposed idea.

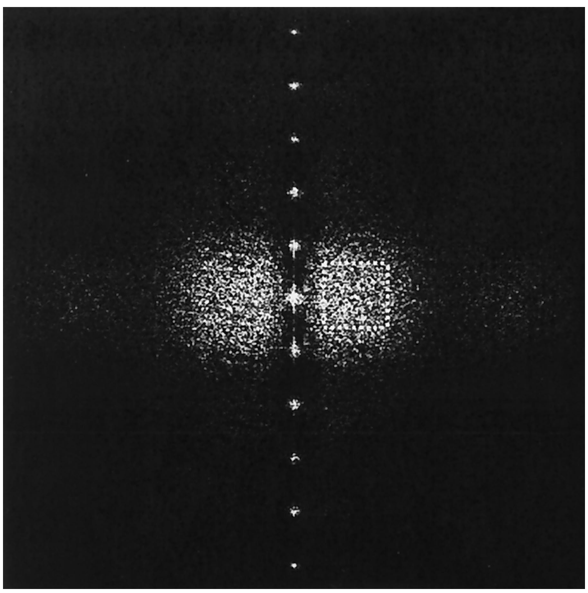

Fig. 3. Simulation results of the joint spectrum plane.

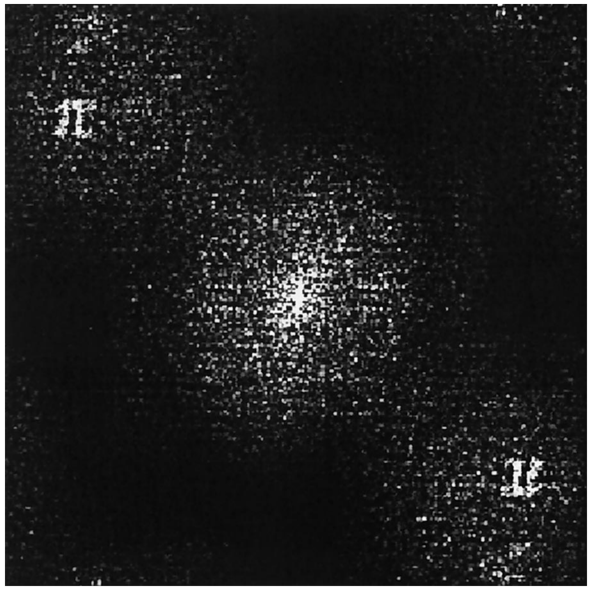

Fig. 4. Simulation results of the JTC output plane in which the hidden watermark was revealed.

The same setup shown in Fig. 1 was used in the optical experiment. The two concealograms were adjusted to be displayed on SLM1 (CRL, Model XGA3; 1024×768 pixels). Both halftone pictures were rotated by 45° on the input plane, as shown in Fig. 5, to avoid the bright tails of the zero diffraction order occurring at the origin of the joint spectrum plane. A collimated beam from a He–Ne laser illuminated SLM1 and created a diffraction pattern of the joint spectrum on the back focal plane of lens L_1 (f = 400 mm, D = 50 mm). The readout image of the entire intensity of the joint spectrum on plane P_2, captured by a CCD, is shown in Fig. 6. Two first diffraction orders, one on either diagonal side of the zero order, can be observed. Because only one of these orders is needed, the CCD records only the intensity distribution inside the area delineated by a white dashed rectangle. The captured image was sampled

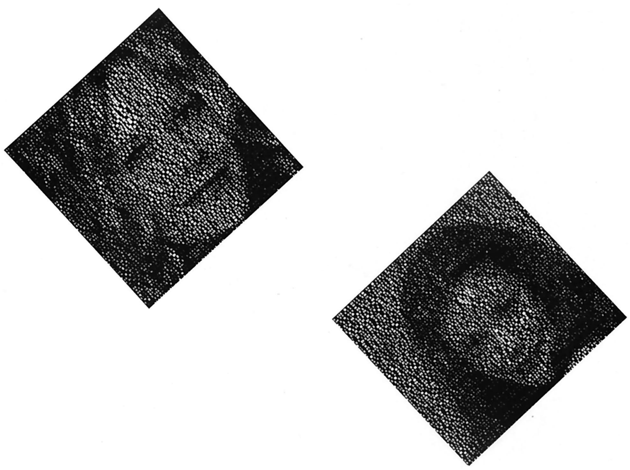

Fig. 5. Two rotated concealograms displayed on SLM1 in the optical experiment.

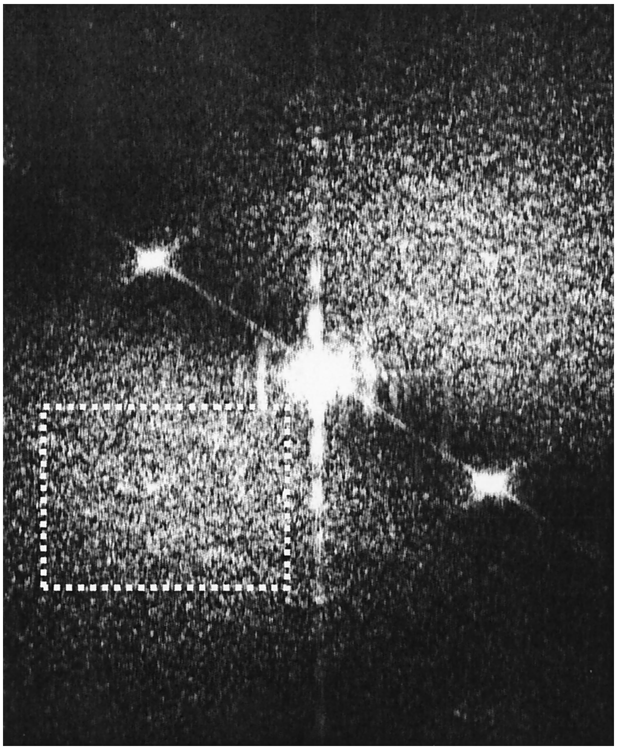

Fig. 6. Experimental results of the joint spectrum plane recorded by the CCD.

into 576 × 768 pixels and was quantized to 256 gray levels. This captured pattern was then displayed on SLM2 (the same SLM as SLM1). Finally, after another Fourier transform by lens L_2, the correlation plane was obtained as shown in Fig. 7. Figure 7 is the watermark reconstructed from optical cross correlation between two input concealograms. Three orders of the correlation plane and the two images of the letter π in the first diffraction orders appear in the figure, demonstrating that the proposed method has reached its goal.

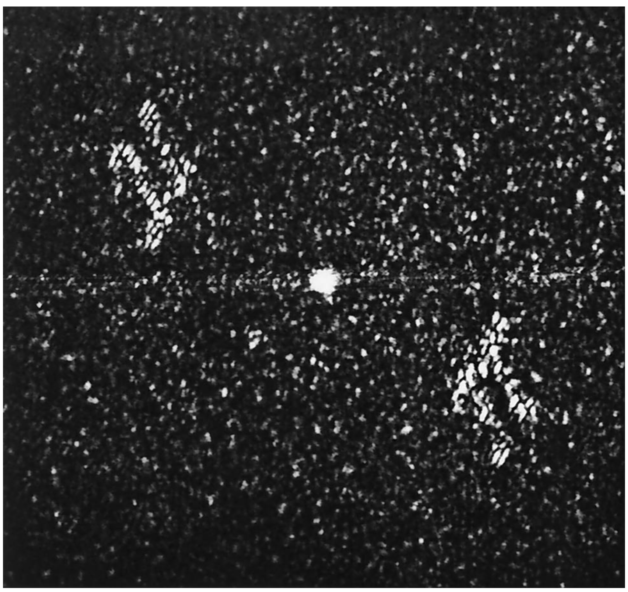

Fig. 7. Experimental results of the reconstructed watermark observed by the CCD on the output plane of the modified JTC.

4. Conclusions

In this paper we have proposed and demonstrated a real-time electro-optical system for embedding and retrieving secured information in hard-copy pictures. In this technique, one conceals an image within another image by manipulating the halftone coding of the host image. The main innovation here is that an electro-optical correlator in a modified JTC configuration deciphers the hidden information. The hidden information is revealed as a result of a spatial correlation between two concealograms. As consequence of the above technique, illegally deciphering the hidden watermark should be practically impossible because the watermark is hidden in the form of complicated phase function. The quality of the reconstructed watermark may be improved by use of another algorithm that is better than the POCS or by use of a SLM with more pixels. Computer simulation and optical experiment have confirmed our proposed technique. Because this watermarking technique can be particularly useful for preventing illegal distribution, and as our proposed method provides the advantages of simple design and alignment with a high degree of security, the technique described above can be a versatile for security applications.

This research was supported by Israel Science Foundation grant 119/03.

References

1. W. Bender, D. Gruhl, N. Morimoto, and L. Lu, "Techniques for data hiding," IBM Syst. J. **35,** 313–336 (1996).
2. D. Grover, "Steganography and watermarking of digital data," Computer Law Security Rep. **17,** 101–104 (2001).
3. N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking—Attacks and Countermeasures,* Vol. 1 of Advances in Information Security, S. Jajodia, ed. (Kluwer Academic, Boston, Mass., 2001).
4. G. C. Langelaar, I. Setyawan and R. L. Lagendijk, "Watermarking digital image and video data. A state of the art overview," IEEE Signal Proc. Mag. **17,** 20–46 (2000).
5. S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden object," Opt. Express **11,** 874–888 (2003), http://www.opticsexpress.org.
6. J. Rosen and B. Javidi, "Hidden images in halftone pictures," Appl. Opt. **40,** 3346–3353 (2001).
7. J. Rosen, B. Javidi, H. Goldenfeld, and S. Moshkovits, "Concealogram: an image within an image," in *Algorithms and Systems for Optical Information Processing VI*, B. Javidi and D. Psaltis, eds., Proc. SPIE **4789,** 44–54 (2002).
8. O. Bryngdahl, T. Scheermesser, and F. Wyrowski, "Digital halftoning: synthesis of binary images," in *Progress in Optics*, E. Wolf, ed. (North-Holland, Amsterdam, 1994), Vol. **33,** pp. 389–463.
9. D. Abookasis, O. Arazi, J. Rosen, and B. Javidi, "Security optical systems based on a joint transform correlator with significant output images," Opt. Eng. **40,** 1584–1589 (2001).
10. C. S. Weaver and J. W. Goodman, "A technique for optically convolving two functions," Appl. Opt. **5,** 1248–1249 (1966).
11. A. VanderLugt, "Signal detection by complex spatial filtering," IEEE Trans. Inf. Theory **IT-10,** 139–146 (1964).
12. A. W. Lohmann and D. P. Paris, "Binary Fraunhofer holograms generated by computer," Appl. Opt. **6,** 1739–1748 (1967).