PRAMANA
— journal of
physics

Vol. 68, No. 3
March 2007
pp. 443–450

Interferometric key readable security holograms with secrete-codes

RAJ KUMAR[1], D MOHAN[2] and A K AGGARWAL[1,*]
[1]Coherent Optics Division, Central Scientific Instruments Organisation, Sector 30, Chandigarh 160 030, India
[2]Department of Applied Physics, Guru Jambheshwar University of Science & Technology, Hisar 125 001, India
*E-mail: aka1945@rediffmail.com

MS received 21 August 2006; revised 27 October 2006; accepted 6 November 2006

Abstract. A new method is described to create secrete-codes in the security holograms for enhancing their anti-counterfeiting characteristics. To imitate these codes is difficult as pure phase objects having complex phase distribution function are used to modulate the object beam that is recorded in conjunction with an encoded interferometric reference beam derived from a key hologram. Lloyd's folding mirror interferometer is used to convert phase variations of the reconstructed wave-front into an intensity pattern for hologram authenticity verification. Creating the secrete-codes through an interferometric reference beam from the key hologram facilitates a multi-stage authenticity verification as well as easy repositioning of the security hologram through a specific Moiré pattern generated during the verification process.

Keywords. Optical security; authenticity verification; security hologram.

PACS Nos 42.40.-i; 42.25.Hz; 42.40.Kw; 42.30.Ms

1. Introduction

Recently, there is a high level of interest in the application of optical techniques in the field of security and product authenticity verification owing to continuous increase in fraudulent cases worldwide. Optical methods offer parallel and real-time processing and provide various dimensions for optical information encryption such as phase, wavelength, polarization etc. in order to deter unauthorized access, copying, or falsification of the valuable products and documents. These parameters of optical waves have been exploited to realize various optical security systems. Representative examples of these systems include image encryption using random phase encoding, optical pattern recognition, fractional Fourier transform, joint transform correlation, phase only encryption etc. [1–4]. The above described systems are excellent in their own right but many of them require accurately fabricated complex masks and fine control of the optical axis alignment and also need specific and

costly equipment to decrypt the encrypted information. Apart from these, several simple encoding schemes such as use of encoded reference beam [5–7], Moiré pattern encoding [8–11], speckle pattern encoding [12] etc. have also been reported for authenticity verification and anti-counterfeit purposes in the embossed holograms.

The present paper reports a simple method for enhancing the anti-counterfeiting ability of security holograms by embedding secrete-codes. Unlike visible holographic security codes [6–8] the secrete-codes, which are in the form of pure phase variations, cannot be detected by an intensity sensitive instrument, thus are extremely difficult for counterfeiting. The desired secrete-codes are created by interfering phase modulated object wave with an interferometric reference wave derived from a specially produced key hologram. During the hologram verification process illumination of security hologram with original reference wave generates a specific Moiré pattern in the observation plane. One of the main characteristics of this Moiré pattern is that it disappears on perfect repositioning of the genuine security hologram only. The chief security feature of these holograms (in addition to Moiré pattern and reconstruction of sharp focused spots at predetermined positions [11]) is that the secrete-codes remain concealed even for a perfectly repositioned security hologram until a decoding process is performed on the reconstructed wave-front to convert their phase variations into intensity variations. The paper reports the use of the simplest known interferometric scheme 'the Lloyd's mirror interferometer' to convert the invisible phase variations of the reconstructed wave-front into detectable intensity pattern for hologram authenticity verification.

2. Principle of the method

The method reported in this paper is based on the formation of a key hologram KH [11] having some unique characteristics and the security hologram in two recording steps. In the first recording step, the key hologram is formed by two holographic exposures on the same recording plate. In the first exposure a convergent beam O_1 is combined with a collimated reference beam R, while in the second exposure another convergent beam O_2, slightly different from O_1 is combined with the same reference beam R. Upon illumination of the processed KH with R, the reconstructed field R_1, which is a combination of O_1 and O_2, serves as an encoded interferometric reference wave to create the secrete-codes on the security hologram SH in the second recording step. Reading of SH through KH generates a specific Moiré pattern at the observation plane OP. Proper repositioning of SH results in the disappearance of these Moiré fringes. The secrete-code information is still invisible and a demodulating process is required to convert the invisible phase information into a visible intensity pattern. This could be accomplished by placing a Lloyd's mirror in proximity with one of the reconstructed focus spots and this is a quite simpler process than the earlier described methods of phase contrast [2] and Mach–Zehnder interferometer [3] to convert phase variations into intensity pattern in the phase-only encryption systems.

Let complex amplitude distributions of the beams O_1, O_2 and R are:

$$O_1 = (A_0/r_1)\exp(-j\phi_1),$$
$$O_2 = (A_0/r_2)\exp(-j\phi_2),$$

and

$$\mathrm{R} = A_\mathrm{r} \exp(j\phi_r), \tag{1}$$

where $\phi_1 = k\mathbf{n}_1 \cdot r_1$, $\phi_2 = k\mathbf{n}_2 \cdot r_2$, $\phi_\mathrm{r} = k\mathbf{n} \cdot r$; and $\mathbf{n}_1$, $\mathbf{n}_2$, $\mathbf{n}$ are unit vectors along the directions of propagation of beams O_1, O_2 and R respectively; $k = 2\pi/\lambda$, λ is the wavelength of the light used and $j = \sqrt{-1}$. A_r and A_0 are the amplitude distributions of the corresponding beams. The processed KH upon illumination with R provides an encoded interferometric reference wave R_1 subsequently to be used for the formation of SH, given by [11]

$$\mathrm{R}_1 \sim \ \mathrm{O}_1 + \mathrm{O}_2. \tag{2}$$

Equation (2) represents a sinusoidal grating pattern with transmittance function

$$g(x, y) = |\mathrm{R}_1|^2 \sim 1 + \cos \Delta\phi, \tag{3}$$

where

$$\Delta\phi = \phi_2 - \phi_1 = 2\pi x/d,$$

and $d = \lambda/[2 \sin(\delta\alpha/2) \cos\{(2\alpha + \delta\alpha)/2\}]$ represents its spatial period (for $z = 0$ position) and α and $\alpha + \delta\alpha$ are the angles made by the directions of beams O_1 and O_2 respectively with the z-axis, i.e. with the direction of the reference beam R. The grating elements/lines run parallel to the y-axis. This encoded reference wave R_1 is used in conjunction with object wave $\mathrm{O} = (A_\mathrm{o}/r_\mathrm{o}) \exp[-j\{\phi_\mathrm{o} + \psi(x, y)\}]$ (where $\psi(x, y)$ is the phase distribution function of the pure phase object $S = \exp\{j\psi(x, y)\}$ to be concealed and $\phi_\mathrm{o} = k\mathbf{n}_\mathrm{o} \cdot r_\mathrm{o}$; $\mathbf{n}_\mathrm{o}$ is the unit vector along O) propagating at an angle β with the z-axis for making the concealed coded security hologram SH. Keeping the term of interest, the transmitted field from processed SH upon illumination by interferometric reference wave R_1 is

$$t(x, y) \sim |\mathrm{R}_1|^2 \cdot \mathrm{O}. \tag{4}$$

In the final reading process, if SH is slightly mis-positioned (say tilted by an angle θ with respect to the y-axis, and displaced longitudinally by a distance Δz from the original position) the transmittance function will be

$$t'(x, y) \sim \mathrm{O}[1 + \cos 2\pi(x \cos\theta - y \sin\theta)/d']. \tag{5}$$

The intensity distribution in the observation plane due to illumination of mis-positioned SH with R_1 is given by the product of transmittance functions $g(x, y)$ and $t'(x, y)$ [13,14]

$$\begin{aligned} I(x, y) &= g(x, y) \cdot t'(x, y) \\ &= O[1 + \cos(2\pi x/d) + \cos[2\pi(x \cos\theta - y \sin\theta)/d'] \\ &\quad + \cos(2\pi x/d) \cos[2\pi(x \cos\theta - y \sin\theta)/d'], \end{aligned} \tag{6}$$

where d' is the effective period of grating pattern recorded on the mis-positioned SH. The first term in eq. (6) is a DC term, second and third terms are proportional

to the superimposing periods and the last term represents the Moiré pattern (figure 1) between these sinusoidal gratings. The last term is of our interest and can be rewritten with standard trigonometric relations as

$$\sim (\mathrm{O}/2)\cos[2\pi\{x[(1/d)+\cos\theta/d']-y\sin\theta/d'\}]$$
$$+(\mathrm{O}/2)\cos[2\pi\{x[(1/d)-\cos\theta/d']+y\sin\theta/d'\}]. \quad (7)$$

In eq. (7) the first term generates a sum Moiré pattern, which has fine period, while the second term generates the difference Moiré pattern. The spatial period of this Moiré pattern is

$$d_{\mathrm{m}} = dd'/(d^2+d'^2-2dd'\cos\theta). \quad (8)$$

It is obvious from eq. (8) that the period of Moiré pattern becomes infinite when $d = d'$ and $\theta = 0$, i.e. when SH is perfectly repositioned. At this position the amplitude distribution of the reconstructed wave-front is given by eq. (4), which makes it clear that in the intensity recording of a pure phase modulated wave-front all information about phase distribution function $\psi(x, y)$ is lost completely, i.e. information of a pure phase object used as a secrete-code remains concealed. A Lloyd's mirror positioned in proximity with one of the reconstructed focused spots (other spots are filtered out) of the converging beams converts the phase

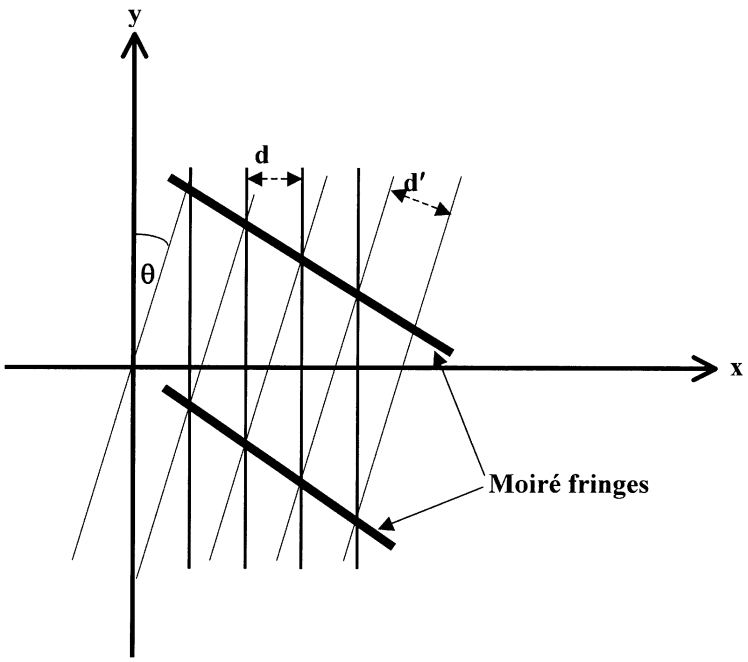

Figure 1. Geometry depicting Moiré fringe formation due to superposition of interferometric encoded reference beam R_1 and grating pattern recorded on security hologram for slightly misaligned positions.

information of secrete-codes into an intensity pattern by generating a two-beam interference fringes:

$$I_2(x, y) = I_0(x, y)[1 + V(x, y) \cos \psi(x, y)], \tag{9}$$

where $I_0(x, y)$ is the average intensity and $V(x, y)$ is the fringe contrast. This interference pattern provides information about the phase distribution function $\psi(x, y)$ in the form of intensity variations which could be used for visual inspection to verify the authenticity of the security hologram.

3. Experiment and results

The experimental set-up for the formation of KH, SH and their reconstruction is schematically shown in figure 2. He–Ne laser at 632.8 nm wavelength was used as the light source. The thin laser beam was split into three parts as beams 1, 2 and 3 using variable beam splitters BS_1 and BS_2. Beam 1 was used as a plane reference beam R while beam 2 was used to generate convergent beams O_1 and O_2 to make the KH. Beam 3 was used as the object beam in conjunction with encoded interferometric reference beam R_1, reconstructed from KH, to make the security hologram SH. Lens L_1 (f/4) in conjunction with beam expander BE_1 generates a collimated beam of 50 mm diameter. Lens L_2 (f/4, 50 mm diameter) in conjunction with beam expander BE_2 was used for the generation of convergent beams O_1 and O_2. Lens L_3 (f/4) in conjunction with beam expander BE_3 generates a 100 mm diameter collimated beam and lens L_4 (f/4, 100 mm diameter) converges this collimated beam. Here f/4 denotes the f-number of the lenses. S_1–S_3 are shutters in the beams 1–3 respectively. During the formation of KH, shutters S_1 and S_2 were opened while S_3 was kept closed. Before making second exposure for KH on the same recording plate, the converging lens L_2 was given a minute movement ($\sim$400 μm) in the transverse direction to generate another convergent beam O_2. For the formation of SH, processed KH was placed back in its original position and a pure phase object S was introduced into a portion of the one half width of collimated beam O, between lenses L_3 and L_4 to create the secrete-codes on SH. During the exposure for the formation of SH, shutters S_1 and S_3 were opened while S_2 was kept closed. In the final reading process, processed KH and SH were repositioned at their original positions and only shutter S_1 was open. A precise manual translation stage was used in our experimental set-up to reposition the processed SH for verification. A spatial filtering process was used to enhance the contrast of the Moiré pattern. A front coated plane mirror M (20 mm $\times$ 40 mm $\times$ 2 mm, SiO_2 protected, front surface silver coated, reflectivity $\sim$94%) was kept in proximity of one of the reconstructed focused spots of the object beam O to convert the invisible phase information of the secrete codes into verifiable intensity pattern. Exposure time of 600 ms was used for the first two exposures for the formation of KH while an exposure time of 350 ms was used for the formation of SH to supply the optimum energy of 130 μJ to the recording medium. Slavich PFG-01 holographic recording plates of sizes 63 mm $\times$ 62 mm for KH and 25 mm $\times$ 31 mm for SH were processed in standard Kodak D-19 developer and R-9 bleach bath solutions. As is well-known, vibration isolation is an essential requirement to record a hologram

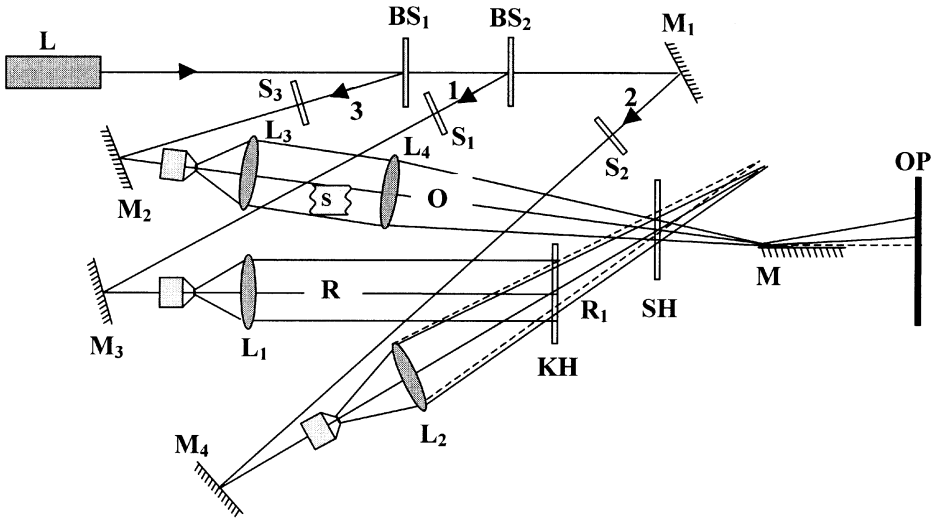

Figure 2. Schematic configuration of the experimental set-up.

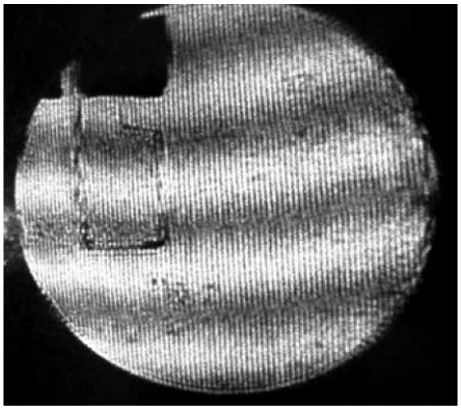

Figure 3. Photograph of a typical finite mode Moiré pattern.

and vibrations with amplitude greater than $\lambda/2$ could disturb the recording. Thus a mechanical stability of the order of $\lambda/2$ is needed during the recording process of the hologram. For this reason, floating vibration isolation table and an enclosure to reduce air currents was used. The results presented have been recorded using S-50 Power-Shot Cannon digital camera in white balance settings.

Figure 3 shows a specific Moiré pattern formed in the observation plane OP due to slight misalignment of SH in its repositioning. This Moiré pattern disappears on proper repositioning of SH and a typical null mode Moiré pattern is obtained as shown in figure 4. It may be noted that this finite Moiré to null Moiré transition takes place only for genuine SH. The information of secrete-codes is still hidden and a Lloyd's mirror interferometer is used to convert this phase information into

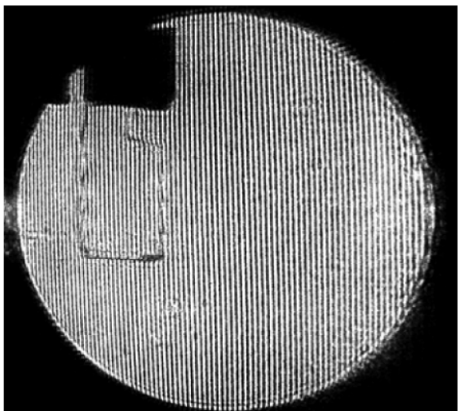

Figure 4. Photograph of a typical null mode Moiré pattern.

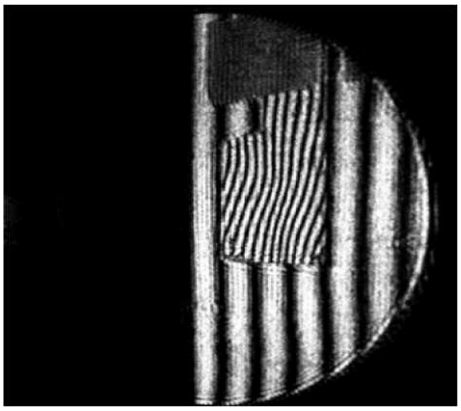

Figure 5. Reconstructed image of a phase object (a glass plate with a small broken portion) from the security hologram using Lloyd's mirror interferometer for hologram authenticity verification.

an intensity pattern. Typical test results of the reconstructed secrete-codes (phase object) are shown in figure 5, which verifies the hologram authenticity.

4. Conclusions and discussions

A simple method is described for generating security holograms with secrete-codes. A specially created key is used for the recording and reconstruction of the security hologram. In the reading process, a slight misalignment in repositioning of security hologram generates Moiré fringes that would vanish on proper repositioning, only for genuine security hologram. It may be noted that key hologram plays dual role – in repositioning security hologram as well as in its authenticity verification. The reconstruction of sharp focused spots at pre-determined fixed positions (angularly and azimuthally) serves as an additional anti-counterfeiting feature and may

also be used for machine inspection. The final verification of security hologram requires an interferometric process on the reconstructed wave-front to convert the phase information of secrete-codes into verifiable intensity pattern. This has been accomplished using Lloyd's mirror interferometer, which is quite elegant compared to the earlier used set-ups for phase-only encryption methods. Counterfeiters may find it more difficult if we use strong (highly refracting) phase objects for creating secrete-codes. A further step is needed for retrieving complete information for such an object, where a grating is used at a specific distance from the focused spots to generate the null mode information [14]. Alternatively, a knife-edge [15] or mirror-edge [16] could also be used for easy verification, but it will reduce the contrast of the resulting pattern.

Acknowledgements

The authors are grateful to The Director, CSIO, Chandigarh for his constant encouragement, support and for permission to publish this work. They wish to thank Mr D P Chhachhia for his kind help in performing the experiments and Mr Sushil K Kaura and Mr Amit K Sharma for helpful discussions held with them. The financial support by Council of Scientific & Industrial Research (Emeritus Scientist Scheme) is greatly acknowledged.

References

[1] B Javidi (ed), *Optical and digital techniques for information security* (Springer-Verlag, Berlin, 2005)
[2] P C Mogensen and J Gluckstad, *Opt. Lett.* **25**, 566 (2000)
[3] D H Seo and S J Kim, *Opt. Lett.* **28**, 304 (2003)
[4] M S Millán, E Pérez-Cabré and B Javidi, *Opt. Lett.* **31**, 721 (2006)
[5] S Lai, *Opt. Eng.* **35**, 2470 (1996)
[6] A K Aggarwal, S K Kaura, D P Chhachhia and A K Sharma, *J. Opt. A: Pure Appl. Opt.* **6**, 278 (2004)
[7] A K Aggarwal, S K Kaura, A K Sharma, R Kumar and D P Chhachhia, *Ind. J. Pure Appl. Phys.* **42**, 816 (2004)
[8] S Liu, X Zhang and H Lai, *Appl. Opt.* **34**, 4700 (1995)
[9] X Zhang, E Dalsgaard, S Liu, H Lai and J Chen, *Appl. Opt.* **36**, 8096 (1997)
[10] A K Aggarwal, S K Kaura, D P Chhachhia and A K Sharma, *Opt. Laser Technol.* **38**, 117 (2006)
[11] S K Kaura, D P Chhachhia and A K Aggarwal, *J. Opt. A: Pure Appl. Opt.* **8**, 67 (2006)
[12] S L Yeh, *Opt. Eng.* **43**, 573 (2004)
[13] R S Sirohi and F S Chau, *Optical methods of measurement* (Dekker, New York, 1999) p. 227
[14] R Kumar, D P Chhachhia and A K Aggarwal, *J. Opt. A: Pure Appl. Opt.* **8**, 747 (2006)
[15] R Kumar, S K Kaura, A K Sharma, D P Chhachhia and A K Aggarwal, *Opt. Laser Technol.* **39**, 256 (2007)
[16] R Kumar, D P Chhachhia and A K Aggarwal, *Appl. Opt.* **45**, 6708 (2006)