PRAMANA © Indian Academy of Sciences Vol. 70, No. 1
— journal of January 2008
physics pp. 131–139

Dual beam encoded extended fractional Fourier transform security hologram with in-built repositioning

AMIT K SHARMA[1,3], D P CHHACHHIA[1], C G MAHAJAN[2]
and A K AGGARWAL[1,*]
[1]Coherent Optics Division, Central Scientific Instruments Organisation,
Sector 30, Chandigarh 160 030, India
[2]Department of Physics, Panjab University, Chandigarh 160 014, India
[3]Present address: Department of Applied Science, IIMT Engineering College,
Meerut 250 001, India
[*]Corresponding author. E-mail: aka1945@rediffmail.com

MS received 16 January 2007; revised 21 August 2007; accepted 28 August 2007

Abstract. This paper describes a simple method for making dual beam encoded extended fractional Fourier transform (EFRT) security holograms. The hologram possesses different stages of encoding so that security features are concealed and remain invisible to the counterfeiter. These concealed and encoded anticounterfeit security features in the security hologram can only be read through a key hologram. Key hologram also facilitates in-built repositioning of security hologram. The method of fabrication, the principle of reconstruction and the experimental results are presented.

Keywords. Holograms; security holograms; optical security; extended fractional Fourier transforms.

PACS Nos 42.40.-i; 42.40.My; 42.40.Ht

1. Introduction

Holograms are widely used as security seals on various products and documents to protect them against forgery. But, in recent years, with rapid technological advances, the conventional holography is facing serious problems from counterfeiters as holographic images from hologram can be captured easily with advanced opto-electronic tools and a new look-a-like hologram can be synthesized. To prevent counterfeiting of these security holograms, researchers have developed various optical methods that are based on Moiré pattern encoding [1–4], random phase encoded holograms [5,6], speckle pattern encoding [7], fractional Fourier transform holograms [8,9] etc. These methods are excellent in their own right and have their own advantages and disadvantages. When we were looking for a simplified and cost-effective scheme for the development of security hologram, we noticed that two reference beams holography [10] can play an important role in enhancing the anti-counterfeit ability of security hologram, where two states of an object are recorded individually with two different reference beams. Two-reference beams holography is a well-known phenomenon used in high resolution holographic interferometry for nondestructive testing where two images have their own reconstruction beams, each has access to the other image separately, as well as to its mutual interference pattern. Additionally, to maximize the security potential of the hologram we apply dual beam encoding with extended fractional Fourier transform (EFRT) [11]. The significant feature of extended fractional Fourier domain optical image encryption benefits from its additional parameters compared to conventional fractional Fourier transform (FRT). In conventional FRT two planes are located symmetrically with respect to lens whereas in extended fractional Fourier transform (EFRT), two planes are located asymmetrically with respect to lens. Furthermore, in our scheme these two reference beams have been recorded separately as a key hologram, which further enhances the anticounterfeit measure of the security hologram. In most of the key–security hologram pair systems, correct mutual repositioning is a critical issue. In this method repositioning problem is solved by making key–security hologram-based interferometric scheme such that key hologram itself works as a guiding tool to reposition the security hologram. The security features which are in the form of interferometric verification fringes on the objects can only be decoded when each object state is addressed individually through both reference beams, and reconstructed wavefronts propagate through such extended fractional Fourier transform system whose parameters are secret and set by the designer. Thus decoding of verification feature is sensitive not only to the two reference beams but also to the parameters of extended fractional Fourier transforms.

2. Principle of the method

The method reported in this paper, for the formation of key–security hologram pair system, is based on the principle of dual reference beam encoding of security hologram in addition to extended fractional Fourier transform. The two reference beams $\mathrm{R}_1$and R_2 have been recorded separately at two different places on the same recording plate in conjunction with a common collimated beam to form the key hologram. This key hologram, when illuminated with collimated beam provides two recorded reference waves for the recording of security hologram.

The schematic for the formation of interferometric encoded security hologram is shown in figure 1, where L_1 is a transform lens placed at the zero of z-axis. Suppose the object $U(x_0) = U\exp\{(j2\pi/\lambda)\phi\}$ is located perpendicular to z-axis. Coherent light modulated by object $U(x_0)$ propagates through distances d_1, passes through lens L_1 and further propagates the distances d_2 to reach the hologram plane where this is captured with beam R_1 in the lower half portion of the recording plate while the upper half portion of the plate remains covered with a stop (figure 1). For incorporation of security verification features (which are in the form of fringe patterns of random profiles on the objects) in the security hologram, two states of the object are recorded employing a two-beam double-exposure holographic interferometric

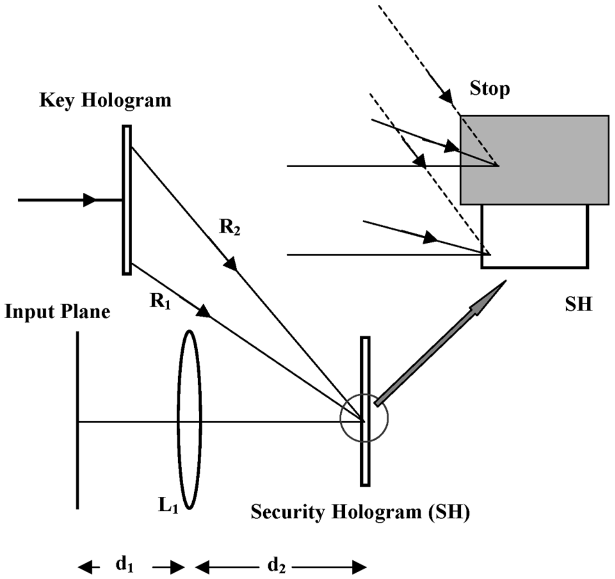

Figure 1. Schematic of experimental lay-out for recording dual beam encoded extended fractional Fourier transform security holograms. Close view around the security hologram is shown by encircled area.

technique. For this, a glass plate is attached with the object during the second exposure where the modified object state is represented by $U'(x_0) = U\exp\{(j2\pi/\lambda)\phi'\}$ and is recorded on the same portion of the plate by beam R_2. For in-built repositioning of security hologram, an interference between beams R_1 and R_2 is also recorded in the upper half portion on the security hologram whereas earlier recorded lower half portion is kept covered by an aperture (figure 2).

Let the distribution of the object $U(x_0)$ in the hologram plane is denoted by $U(x_1)$ where x_0 and x_1 are the coordinates in the input and hologram plane respectively.

$$\begin{aligned} U(x_1) &= \int U(x_0)\exp[j\pi\{(a)^2(x_0)^2 + (b)^2(x_1)^2\}/\tan\phi - j2\pi(abx_0x_1/\sin\phi)]\mathrm{d}x_0 \\ &= u[U(x_0)|a,\alpha,b|(x_1)]. \end{aligned} \tag{1a}$$

Similarly, the distribution of the changed object state $U'(x_0)$ in the hologram plane is denoted by $U'(x_1)$.

$$U'(x_1) = u[U'(x_0)|a,\alpha,b|(x_1)], \tag{1b}$$

where a, α and b are the three parameters of extended fractional Fourier transforms which are equivalent to expanding a function a times, performing FRT of order α [12] and contracting the resultant distribution b times. The parameters a, α and b are related to distances d_1, d_2 and the focal length f of the lens through the expressions

$$a^2 = (1/\lambda)\left[\left\{\frac{(f-d_2)^{1/2}}{(f-d_1)^{1/2}}\right\}\left\{\frac{1}{[f^2-(f-d_1)(f-d_2)]^{1/2}}\right\}\right],$$

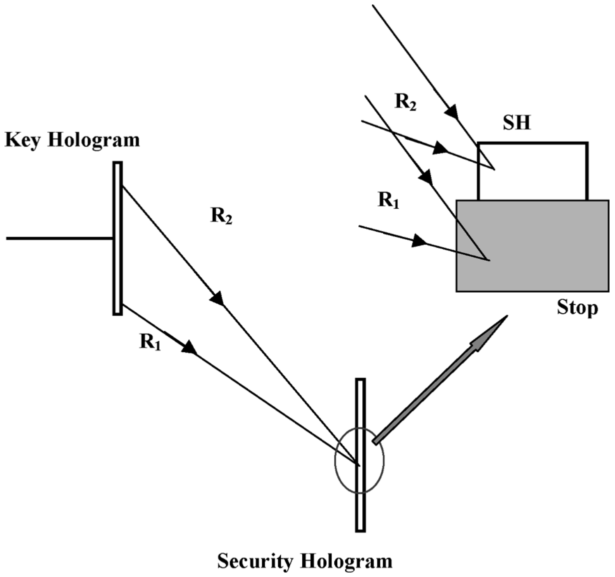

Figure 2. Schematic of experimental lay-out for recording holographic interferometer used for repositioning alignment of security holograms. Close view around the security hologram is shown by encircled area.

$$\alpha = 2/\pi \text{arcos}[(f-d_1)^{1/2}(f-d_2)^{1/2}/f],$$
$$b^2 = (1/\lambda)\left[\left\{\frac{(f-d_1)^{1/2}}{(f-d_2)^{1/2}}\right\}\left\{\frac{1}{[f^2-(f-d_1)(f-d_2)]^{1/2}}\right\}\right], \tag{2}$$

where λ is the recording wavelength. Under the linear recording conditions, the amplitude transmittance of the lower half portion of the plate can be considered as

$$t \sim |U(x_1)+R_1|^2 + |U'(x_1)+R_2|^2, \tag{3}$$

where $U(x_1)$ and $U'(x_1)$ are the object distributions and R_1 and R_2 are respective recording beams. When the processed hologram is illuminated with original beams R_1 and R_2 distributions $U(x_1)$ and $U'(x_1)$ are reconstructed. To verify the hologram security feature, the extended FRT operation with fractional order β should be performed where distributions $U(x_1)$ and $U'(x_1)$ propagate distance d_3 and pass through lens L$_2$ and further propagate distance d_4. The amplitude components on the output plane can be expressed as $U(x_2)+U'(x_2)$ where

$$\begin{aligned} U(x_2)+U'(x_2) &= u[u\{|R_1|^2\{U(x_1)\}|c,\beta,d|(x_2)\}] \\ &\quad + u[u\{|R_2|^2\{U'(x_1)\}|c,\beta,d|(x_2)\}]. \end{aligned} \tag{4}$$

One can obtain the expressions that relate the parameters c,β and d to distances d_3 and d_4 by replacing a,α,b,d_1 and d_2 with c,β,d,d_3 and d_4 respectively in eq. (2). Applying condition of additive operation for the EFRT, i.e. if $b=c$ then

$$\begin{aligned}U(x_2) + U'(x_2) &= u[u\{|R_1|^2\{U(x_1)\}|a, \alpha + \beta, d|(x_2)\}] \\ &\quad +u[u\{|R_2|^2\{U'(x_1)\}|a, \alpha + \beta, d|(x_2)\}] \\ &= U(-x_0) + U'(-x_0), \qquad (5)\end{aligned}$$

where $\alpha + \beta$ is analogous to order matching condition used in general FRT with two additional parameters. Here the reconstructed wavefront is the corresponding object wavefront by coordinate inversion. Intensity pattern will be

$$I = |U(x_0) + U'(x_0)|^2 = 2|U|^2[1 + \cos(\phi' - \phi)], \qquad (6)$$

where $2|U|^2$ represents the light from the image of the objects. The terms in square brackets describes the fringes on the objects and $(\phi' - \phi)$ is the change in optical phase due to change in optical position between exposures.

In most of the key–security hologram pair systems, correct mutual repositioning is a critical issue. It is to be noted that translation and angular errors in the repositioning of security hologram results in immeasurable verification feature. The degree of accuracy on the replacement of the security hologram to its original recording position should be much better than the wavelength of the radiation in use. The tolerance range for correct repositioning is much tight. Micro-positioning adjustments are usually conducted on trial and error basis, which could become a lengthy and non-optimized operation. In our method an interferometric technique is also described, which offer an accurate and monitored method of hologram repositioning. For this, interference patterns between beams R_1 and R_2 coming out from key hologram is recorded in the upper half portion of the security hologram (figure 2). In reading process, when security hologram is simultaneously illuminated with beams R_1 and R_2 it also forms a holographic interferometer [13] where the undiffracted beam R_1 and the diffracted beam R_1 (generated due to beam R_2) are propagating in the same direction and form interferometric fringes. Similarly, undiffracted beam R_2 and diffracted beam R_2 (generated due to beam R_1) also produces interferometric fringes (figure 3). These spatially separated superimposed beam pairs provide two separate interferograms at two different locations. The interferometric fringes of any of the interferogram can be used to realign the security hologram. The hologram is at the nearest position of alignment when these interferometric fringes vanish and sharp verification fringes appear on object reconstruction plane.

3. Experimental details

In our experimental arrangement, a He–Ne laser (coherent model 31-2140, 35 mW output power, 632.8 nm wavelength) was used to record key hologram, the security hologram and in the final reading process of security hologram. Dual beam encoded extended fractional Fourier transform hologram was formed in conjunction with a key hologram which generates two different kinds of reference beams for security hologram recording. The object used in our experiment is a diffuser that contains a character ‘A’. We have used two lenses having focal length 160 mm for recording and 200 mm for reconstruction. The angle between the reference wave R_1 and the object waves was 25° and reference wave R_2 and the object waves was 35°.

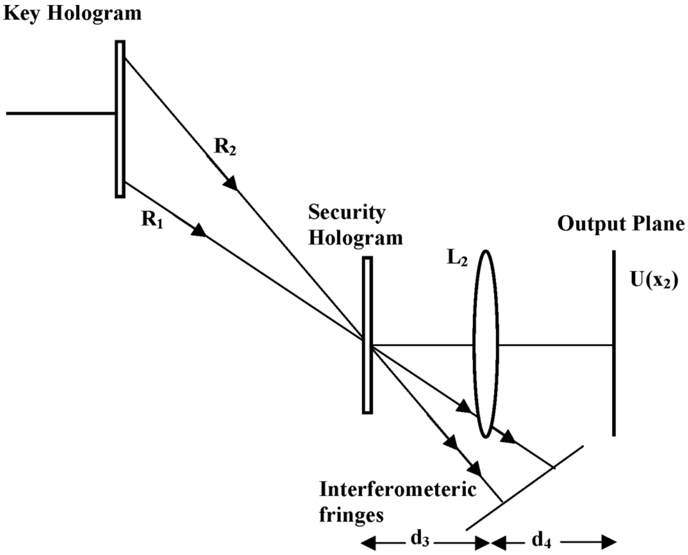

Figure 3. Schematic of experimental lay-out for reconstruction of proposed security holograms with repositioning guiding tool.

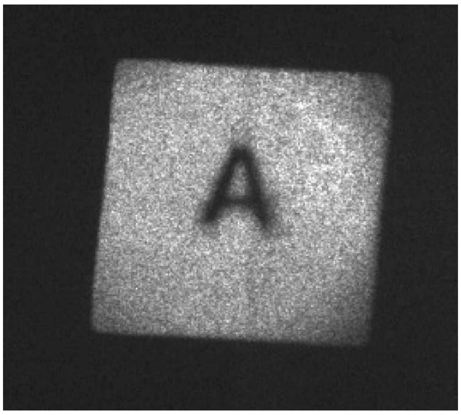

Figure 4. Photograph of typical results obtained due to the reconstructed object 'A' when security hologram is illuminated with one beam and after suitable EFRT.

The asymmetrical distances on two sides of recording lens used for encoding the first object were kept as $d_1 = 118$ mm and $d_2 = 135$ mm, resulting in extended fractional Fourier transform parameters $a = 2.79$ mm^{-1}, $\alpha = 0.87$ and $b = 3.62$ mm^{-1}. To calculate the parameter for reconstruction, knowledge of the concealed recording EFRT parameters (i.e. a, α and b) are necessary. In our case, reconstruction parameters for keeping unit magnification (i.e. $\alpha + \beta = 2$) of the object are $\beta = 1.13, d_3 = 225.03$ mm, $d_4 = 265.70$ mm. Standard Kodak D-19 developer and R-9 bleach bath solutions are used with Slavich PFG-01 plates to give high efficiency

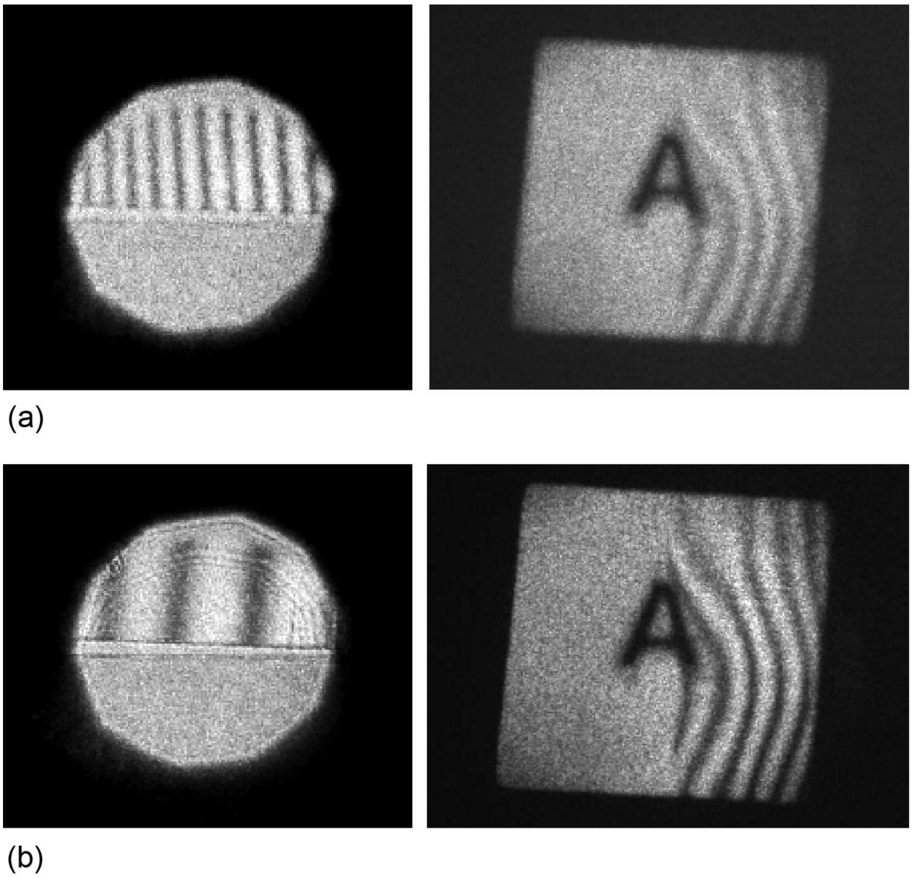

Figure 5. (**a**) Photograph of typical results obtained due to the reconstructed object ‘A’ with faint verification fringes when security hologram is not properly repositioned and suitable EFRT performed. (**b**) Photograph of typical results obtained due to the reconstructed object ‘A’ with sharper verification fringes when security hologram is near to repositioned state and suitable EFRT performed.

and low noise encoded key and security holograms. The experimental lay-out for the final reading process of these security holograms is shown in figure 3. Here a collimated beam is used to illuminate the key hologram, which further generates two different beams R_1 and R_2. When security hologram is simultaneously illuminated with reference beams R_1 and R_2, and thereby reconstructed wavefronts $U(x_1)$ and $U'(x_1)$ undergo through preset extended fractional Fourier transform, reconstruct the image of the object with verification fringes. When hologram is illuminated with single beam, verification fringes on the object cannot be depicted. Figure 4 shows the reconstructed object when hologram is illuminated with one beam. Typical results having verification fringes using proposed two-beam double-exposure holographic interferometric technique are shown in figure 5. Figures 5a and 5b show repositioning of security hologram and corresponding verification fringes. In these figures, left-hand side (LHS) fringes are interferometric fringes and could be used to align the security hologram whereas right-hand side (RHS) fringes on the object are verification fringes. It may be noted that the contrast of the verification fringes on the object depends on the repositioning as is evident in figure 5 where the contrast of these fringes gets enhanced as the security hologram is properly repositioned.

4. Conclusion

This paper presents a simple and cost-effective method for making security holograms, which is based on the particularity of two-beam interferometric encoding and extended fractional Fourier transform of the object through a key hologram. In the final reading process, key hologram is used to decode the object and the verification features. The image of recorded object along with specific verification fringes can be observed at the output plane of the reconstructed EFRT systems. Object cannot be reconstructed if EFRT parameters are unknown. Here key hologram is not only used to decode the verification features but also worked as an alignment tool to reposition the security hologram. However, the hologram recorded at the upper half of the security hologram (interference between R_1 and R_2) is insensitive to translation of the hologram in a direction perpendicular to the grating vector, because R_1 and R_2 are plane beams. The security hologram contains many secret parameters such as parameters of recording systems, specific wavefront generated from HOE key hologram and random shape and size interferometric fringes on the object in addition to angular encoding of object, which are impossible to guess for any counterfeiter, and so the proposed hologram could be considered as high security hologram.

Acknowledgement

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 S K Kaura and Mr Raj Kumar for helpful discussions throughout the work and to CSIR, New Delhi for their financial support.

References

[1] S Liu, X Zhang and H Lai, *Appl. Opt.* **34**, 4700 (1995)

[2] X Zhang, E Dalsgaard, S Liu, H Lai and J Chen, *Appl. Opt.* **36**, 8096 (1997)

[3] A K Aggarwal, S K Kaura, D P Chhachhia and A K Sharma, *Opt. Laser Technol.* **38**, 117 (2006)

[4] S K Kaura, D P Chhachhia and A K Aggarwal, *J. Opt. A: Pure Appl. Opt.* (*UK*) **8**, 67 (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.* (*UK*) **6**, 278 (2004)
[7] S L Yeh, *Opt. Eng.* **43**, 573 (2004)
[8] Y Zeng, Y Guo, F Gao and J Zhu, *Opt. Commun.* **215**, 53 (2003)
[9] W Jin, L Ma and C Yen, *Opt. Commun.* **259**, 513 (2006)
[10] R Dandliker, E Marom and F M Mottier, *J. Opt. Soc. Am.* **66**, 23 (1976)
[11] J Hua, L Liu and G Li, *J. Opt. Soc. Am.* **A14**, 3316 (1997)
[12] A W Lohmann, *J. Opt. Soc. Am.* **A10**, 2181 (1993)
[13] A K Aggarwal, Sushil K Kaura, D P Chhachhia and A K Sharma, *Opt. Laser Technol.* **36**, 545 (2004)