Indian Journal of Pure & Applied Physics
Vol. 42, November 2004, pp. 816-819

Interferometry based security hologram readable with an encoded key hologram

A K Aggarwal, Sushil K Kaura, Amit K Sharma, Raj Kumar & D P Chhachhia
Coherent Optics Division, Central Scientific Instruments Organisation,
Sector 30, Chandigarh 160 030

Received 19 April 2004; accepted 18 August 2004

A simple and cost-effective method for making security holograms has been presented, which incorporates holographic interferometry as verification feature in addition to spatially separated sharp focus spots. When the security hologram is illuminated with decoding reconstructing beam generated from an encoded key hologram, two spatially separated sharp focus spots emerge at the predefined positions and can be read through a photoelectric detector array. In addition, these focused spots upon divergence in longitudinal direction further generate specific kind of interferometric fringe patterns of random profile contained in them, which are suitable for further visual inspection. These machine-readable and visual verifiable features can be used for better counterfeit-resistant security codes in embossed holograms. Recording schemes for the formation of such security holograms and typical experimental results have been presented.

[Keywords: Security holograms, Holograms, Optical security]
IPC Code: G 02B 5/32

1 Introduction

Since the earliest days of market trade, counterfeit goods have existed. In order to deter the counterfeiting of currency, passports, drivers licenses, brand name products, and other instruments of value etc; various optical security techniques based on double random phase encoding and joint transform correlation have been widely investigated[1-5]. These techniques though excellent in their own right, are inherently complex and need specific and costly equipments to visualize or verify their security features. Embossed holograms, extensively used as security seal on various products and documents, offer a simple and cost effective approach to guard these against duplication and forgery[6]. Moiré patterns[7,8] are successfully used for visual verification in security holograms but are not suitable for automatic inspection. For machine-readable security holograms, encoded reference wave generated through random phase mask/key hologram is commonly employed[9,10]. Recently a method has been proposed in which both machine-readable and visual verifiable features are incorporated to increase the anti-counterfeit ability of the security holograms[11]. During verification of these holograms, two spatially separated sharp focus spots emerge which upon divergence further generates linear or circular fringes contained in them. Though this method increases the level of difficulty for counterfeiter but still there is a possibility that by knowing about the shape and number of fringes, these holograms could be regenerated. In order to further enhance the anti-counterfeit ability of these security holograms, we propose a simple and cost-effective method with improved security verification elements in the form of multiple focusing spots that additionally contain fringe patterns of random profiles instead of that of definite shaped fringes. These fringes are random in nature and the chances of their regeneration are almost negligible and so these types of security holograms have features that cannot be copied and thus further enhance their anti-counterfeit ability. Double-exposure hologram interferometric techniques have successfully been used for generation of these encoded random profile fringes.

2 Experimental Details

The method reported in this paper is based on the formation of an encoded key hologram and the security hologram separately in two recording steps. In the first recording step, an encoded key hologram is formed by combining an object wave generated through a random phase plate with a collimated reference beam. This encoded key hologram, when illuminated with a collimated beam, provides an encoded reference wave R for the second recording step. In the second recording step, the so generated encoded reference wave R is used, for making two

separate holographic recordings in conjunction with two spatially separated convergent object waves O_1 and O_2 respectively, for the formation of the security hologram. For further incorporation of enhanced security verification features (in the form of fringe patterns of random profiles[12,13]) in these security holograms, each of these holographic recordings in turn employs double-exposure holographic interferometry where two separate holographic exposures are given independently and on the same recording plate. In the first recording case, a soldering gun (SG) is inserted between the collimating lenses C_1 and C_2 (used for the generation of convergent object wave O_1), which is kept switched-off during the first exposure and is switched-on during the second exposure. In the second recording case, the first exposure is made by using R and the convergent object wave O_2, while during the second exposure a glass plate (GP) is inserted between the collimating lenses C_3 and C_4 (used for the generation of convergent object wave O_2). In the reading process of these security holograms, the encoded key hologram (facilitating the generation of decoding reconstructing wave R) is used and two spatially separated sharp focus spots are reconstructed on the respective convergent points. In addition, these focused spots upon divergence in the longitudinal direction further generate specific interferometric fringe patterns of random profile contained in them.

The experimental layout for the first recording step is schematically shown in Fig. 1. Light from a He-Ne laser (L) is split by a variable beam splitter (BS) into two components. The transmitted beam is used to generate a collimated reference beam through a beam expander (BE_1) and a collimating lens (C_1). The reflected beam, used for the generation of an object wave, is expanded and collimated by using a beam expander (BE_2) in conjunction with a collimating lens (C_2). The so generated plane wave is further modulated through a random phase plate (RP). The scattered light from RP is made to interfere with the reference beam on the holographic recording plate to form an encoded key hologram (KH). The experimental layout for the second recording step of making security holograms is schematically shown in Fig.2. Light from a He-Ne laser (L) is split into two components by using a variable beam splitter (BS_1). The transmitted component is further split into two parts by another variable beam splitter (BS_2). The reflected component from BS_2 is used for the generation of a convergent object wave O_1 on the hologram recording plate SH through a beam expander (BE_1) in conjunction with a combination of two collimating lenses (C_1 and C_2). The reflected component from BS_1 is used for the generation of another convergent object wave O_2 on the hologram recording plate SH through a beam expander (BE_2) in conjunction with a combination of two collimating lenses (C_3 and C_4). The transmitted component from BS_2 is used for the generation of a conjugate reference beam for the KH through a beam expander (BE_3) in conjunction with a collimating lens (C_5). The real image derived from the KH serves as the encoded reference wave R for making the security hologram. The so generated encoded reference wave R is used, for making two separate holographic recordings in conjunction with two spatially separated convergent

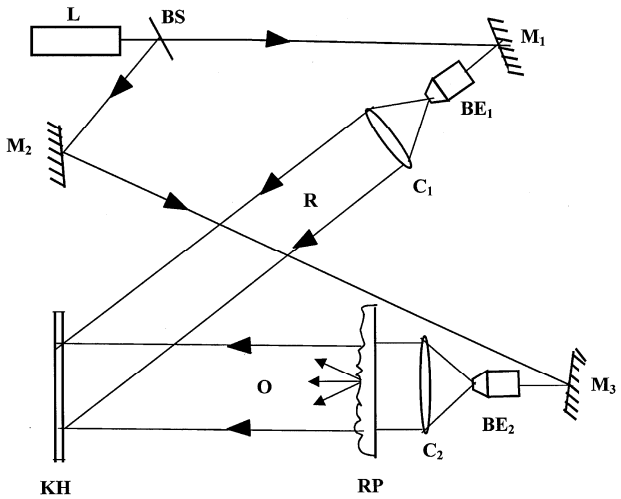

Fig. 1—Schematic of experimental layout for recording encoded key holograms

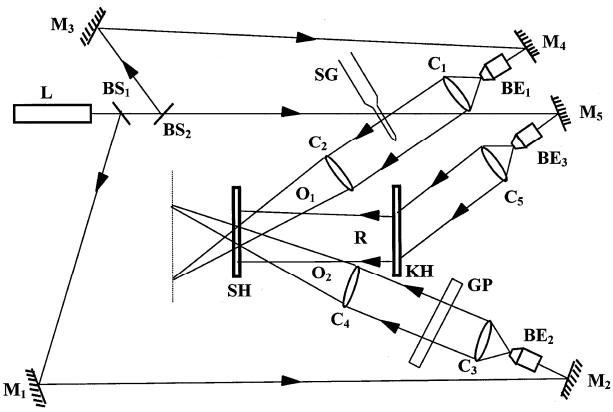

Fig. 2—Schematic of experimental layout for recording security holograms

object waves O_1 and O_2 respectively, for the formation of the security hologram. However, each of these holographic recordings in turn employs double-exposure holographic interferometry where two separate holographic exposures are given independently and on the same recording plate. In the first recording case, a soldering gun (SG) is inserted between the collimating lenses C_1 and C_2, which is kept switched-off during the first exposure and is switched-on during the second exposure. In the second recording case, the first exposure is made by using R and the convergent object wave O_2, while during the second exposure a glass plate (GP) is inserted between the collimating lenses C_3 and C_4. Standard Kodak D-19 developer and R-9 bleach bath solutions are used with Agfa-Gevaert 8E75HD plates to give high efficiency and low noise encoded key holograms and security holograms.

The experimental layout for the final reading process of these security holograms is schematically shown in Fig. 3. Light from a He-Ne laser (L) is expanded and collimated by using a beam expander (BE) in conjunction with a collimating lens (C). This collimated beam is used as a conjugate reference beam to illuminate the KH, where KH is placed at a predetermined fixed position. The real image derived from KH serves as a decoding reconstructing beam for reading the SH and two spatially separated sharp focus spots (bright spots) are reconstructed on the convergent points of the original object waves O_1 and O_2 in the observation plane (OP). In addition, these focused spots upon divergence in the longitudinal direction further generate specific interferometric fringe patterns of random profile contained in them.

The typical results obtained with these studies are shown in Figs 4 and 5. Fig. 4 depicts the reconstructed focus spot images, as obtained, by using SH in the final reading process (Fig. 3). Figure 5 depicts typical specific interferometric fringe patterns of random shape as obtained upon divergence from these focused spots. For final reading of these holograms, both SH and KH are required to be kept at the same position at which they were placed in the second recording step. It is observed that the sensitivity in the placement of the KH and the SH (Fig. 3) mainly depends on the randomness (phase distribution) of the phase plate used for the formation of the key hologram in the first recording step. Thus as the randomness of the phase plate is increased, the sensitivity requirement in positioning of both the KH and SH also becomes more critical. The advantage of making KH in our method lies in the fact that a large number of key holograms (KHs) can be made, for distribution to the inspectors, either by directly using the experimental set-up as described in Fig. 1 or holographic copies of the KH can be generated by using hologram-copying techniques[14]. In our experimental studies, it was observed that if SH or KH (Fig. 3) is moved by more than 0.7mm or rotated by more than 3 degree in the reading process, the reconstructed focus spots disappear. In the final verification process, the sharp focus spots, which display specific interference fringe patterns of random profile upon divergence in the longitudinal direction, are reconstructed only when the SH is illuminated by the decoding reconstructing beam generated from the KH. Thus, in these security holograms the level of difficulty for counterfeiting them have been increased manifold as they contain enhanced security features in

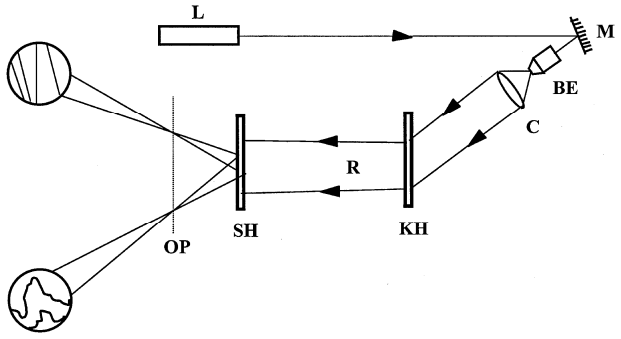

Fig. 3—Schematic of experimental layout for reading security holograms

Fig. 4—Photograph of typical results obtained due to the reconstructed focus spot images

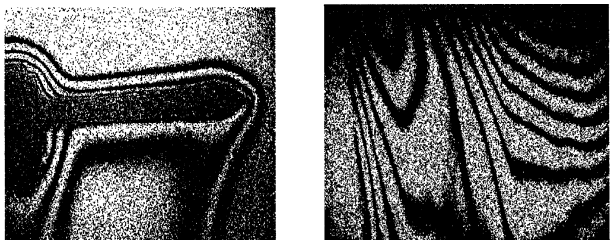

Fig. 5—Photograph of typical results obtained due to specific interferometric features contained in these focused spots

the form of visually verifiable specific interference fringe patterns of random profile in addition to the machine-readable sharp focus spots which can be read only by using the KH in the reading process and is virtually impossible to regenerate.

3 Conclusion

This paper presents a simple and cost effective method for making security holograms, which employs holographic interferometry in addition to an encoded reference beam. In the verification process, specific interferometric fringe patterns of random profile emerge as additional visual verifiable feature due to divergence in machine-readable sharp focus spots, only when security hologram is illuminated by decoding reconstructing beam generated through the key hologram. Because the fringe patterns that are random in nature and would be almost impossible to regenerate them even by an expert holographer, the proposed holograms incorporating these types of features are immune to the counterfeiting and could be considered as high security holograms.

Acknowledgement

The authors are grateful to Dr R P Bajpai, Director, CSIO, Chandigarh for his constant encouragement, support and for permission to publish this work. They wish to thank the Department of Science and Technology, Govt. of India, New Delhi for the financial support for carrying out this work. They also wish to thank Mrs Madhu Mehta, Sr Stenographer for typing the manuscript of the paper. One of the authors (AKS) also wishes to thank the CSIR for the fellowship offered to him for the pursuit of this research.

References

1 Wang R K, Watson I A & Chatwin C, *Opt Eng*, 35 (1996) 2464.
2 Refregier P & Javidi B, *Opt Lett*, 20 (1995) 767.
3 Neto L G & Sheng Y, *Opt Eng*, 35 (1996) 2459.
4 Javidi B & Horner J L, *Opt Eng*, 33 (1994) 1752.
5 Weber D & Trolinger J, *Opt Eng*, 38 (1999) 62.
6 Lancaster I (Ed), *Holopack Holoprint Guidebook* (Reconnaissance International Publishers and Consultants, Leatherheads, Surrey, UK), 2000.
7 Liu S, Zhang X & Lai H, *Appl Opt*, 34 (1995) 4700.
8 Zhang X, Dalsgaard E, Liu S, Lai H & Chen J, *Appl Opt*, 36 (1997) 8096.
9 Lai S, *Opt Eng*, 35 (1996) 2470.
10 Kaura S K, Chhachhia D P, Sharma A K & Aggarwal A K, *Indian J Pure & Appl Phys*, 41 (2003) 696.
11 Aggarwal A K, Kaura S K, Chhachhia D P & Sharma A K, *J Opt A: Pure & Appl Opt*, 6 (2004) 278.
12 Aggarwal A K, Kaura S K, Chhachhia D P & Sharma A K, *Opt & Laser Tech*, 36 (2004) 545.
13 Aggarwal A K, Kaura S K, Chhachhia D P & Sharma A K, *Indian J Pure & Appl Phys*, 42 (2004) 326.
14 Caulfield H J (Ed), *Handbook of optical holography*, (Academic Press, New York, USA), 1979.