Volume 66, Issue 3, 2022

Journal of Scientific Research

of

The Banaras Hindu University

Retrieving Codes in Security Hologram Using Encoded Dual Beam

Amit Kumar Sharma[*1], Roopesh Kumar[2]

[*1]Department of Physics, D.A.V. (PG) College, Dehradun, (aoemit@rediffmail.com)
[2]SDepartment of Physics, D.B.S. (PG) College, Dehradun (roopeshdbs@gmail.com)

Abstract: **A simplistic approach for hiding and retrieving security codes in hologram is described here. Retrieval of these codes requires encoded dual beam which are recorded in a key hologram. In the reading process, spatially separated focus spots are formed which on divergence form moiré fringes in the observation plane. The nulling of moiré fringe in repositioning security hologram is possible only in case of genuine security and key hologram pair. The retrieval of hidden codes in the security hologram further needs spatial filtering of focus spots.**

Index Terms: **hologram, security hologram, concealed code, encoded hologram, optical security.**

I. Introduction

Holograms are among most popular means used for securing valuable commercial products and documents [1-4]. The information stored holographically is considered to be secure for unauthorized access as hologram works on the principle of diffraction unlike others means which usually work on reflection. But with rapid growth of technology there exists a possibility to counterfeiter a hologram. Thus, security of information stored in hologram is an important issue. To prevent falsification or copying, many different optical systems utilizing phase encoding and correlation techniques have widely been reported [1]. These systems are marvelous and capable to deter counterfeiting but are inherently complex which requires highly sophisticated and costly equipment. Besides these techniques, various cost effective and simplified encoding schemes in embossed holograms namely use of encoded reference beam [5-8]; moiré pattern encoding [9-11], speckle pattern encoding [12] etc. have also been reported in literature for authenticity verification and anti-counterfeiting purposes. In the techniques using encoded reference beam, a converging beam is captured with the reference beam derived from a random phase plate. During verification, on proper repositioning of the security hologram a sharp focused spot is reconstructed at predetermined position as an authenticity verifiable feature. A machine placed at this position verifies the authenticity of the security hologram. The repositioning of security hologram is simplified by using the concept of key hologram, where the random reference beam is frozen on a recording plate using a plane reference beam. Illumination of key hologram with plane wave reconstructs the random wavefront serving as reference beam for the security hologram. Putting additional interferometric codes in the security hologram further enhances the level of difficulty. In another development for security holograms moiré patterns are encoded which generate specific artistic effects during hologram verification. Here one periodic pattern is recorded as a phase object on the security hologram while second periodic pattern works as the key to generate the desired moiré pattern. In most of these encoding techniques either repositioning of security hologram is tedious or by conversely reading of security hologram, there are some chance to regenerate copy of the key hologram.

In this paper we propose encoded dual beam, generated from a key hologram to create security features, which not only reduces alignment related difficulties (in verification process) greatly but also immensely increase the level of security. The key hologram upon illuminating with reference beam generates both beams simultaneously to serve complex interfering encoded dual beam which further used as reference beam for the generation of security hologram. Due to random nature of interferometric encoded dual beam, it becomes nearly impossible for any counterfeiter to conversely regenerate it. During reconstruction of the security hologram, a few spatially separated sharp focused spots are reconstructed at predetermined positions. These spots upon divergence generate moiré fringes in the observation plane. These moiré fringes appear because of overlapping of complex sinusoidal phase diffraction grating of

[*]Amit Kumar Sharma

DOI: DOI: 10.37398/JSR.2022.660330

high frequencies generated from key hologram and those recorded in security hologram. Here pure phase codes could be concealed in the security hologram using this encoded dual reference beam. Retrieving of these codes requires transition of phase information into the verifiable intensity pattern which is performed by perfectly repositioned the security hologram and filtering focus spots.

II. Principle of the Method

The method described in this paper is rests on the formation of a key hologram (KH) and the security hologram (SH) in different recording steps where key hologram has some specific characteristics which authenticates and retrieves the hidden codes in security hologram. Figure 1 shows a schematic for recoding the key hologram (KH) where encoded dual beam (R_1) is captured with a collimated beam (R). Now when the processed KH is illuminated with plane reference beam R, the beam R_1 (which is combinatory of beams O_1 and O_2) is reconstructed, which serves as an encoded special reference wave to create the concealed codes on the security hologram SH in conjunction with phase (S) modulated object beam (O). Schematic for recording this security hologram is exhibited in figure 2. The Security hologram SH can only be read through genuine key hologram KH. In final reading process a few spatially separated focus spots are generated, which on divergence, overlap and produce moiré fringes at the observation plane OP (figure 3). It should be marked that finite moiré to null moiré transition in repositioning the security hologram can only be taking place for genuine key and security hologram pair. The concealed phase information requires a demodulation process to convert into verifiable visible intensity patterns. This could be achieved by spatial filtering of these spots placing an opaque screen and only one spot is allowed to pass results sharp verifiable pattern in observation plane.

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

$$O_1 = \left(\frac{A_1}{r_1}\right) exp(-j\phi_1),$$

$$O_2 = \left(\frac{A_2}{r_2}\right) exp(-j\phi_2) \text{ and}$$

$$R = A_r exp(-j\phi_r) \qquad (1)$$

Where $\phi_1 = k\,\boldsymbol{n_1}.r_1$, $\phi_2 = k\,\boldsymbol{n_2}.r_2$, $\phi_r = k\,\boldsymbol{n}.r$; and $\boldsymbol{n_1}, \boldsymbol{n_2}, \boldsymbol{n}$ are unit vectors in the directions of propagation of beams $O_1,\ O_2\ and\ R\ are$ respectively; $k = 2\pi/\lambda$, λ is wavelength of the laser light used and $j = \sqrt{-1}$. A_1, A_2 and A_r are the amplitude distributions for the beams used. The processed key hologram (KH) when illuminating with beam R, generates encoded beam R_1 which is later on used for the formation of security hologram (SH), given by [10]

$$R_1 \sim O_1 + O_2 \qquad (2)$$

having transmittance function

$$g(x,y) = |R_1|^2 \sim 1 + \cos(2\pi x/d) \qquad (3)$$

where $d = \lambda/[2\sin(\delta\alpha/2)\cos\{(2\alpha+\delta\alpha)/2\}]$ is the spatial period for sinusoidal grating pattern formed and α and $\alpha + \delta\alpha$ represents the angles made by the beams O_1 and O_2 respectively with the direction of reference beam R. This encoded reference wave R_1 is used in conjunction with object wave O = (A_o/r_o) exp $[-j\{\phi_o + \xi(x,y)\}]$, (where $\xi(x,y)$ is the distribution function of the phase object S = $\exp\{j\xi\ (x,y)\}$ and $\phi_o = k\ \mathbf{n_o}.r_o$; $\mathbf{n_o}$ is unit vector along the beam O forming the security hologram SH having concealed codes. The processed security hologram SH when illuminated with encoded beam R_1 (which is generated from the key hologram) have transmitted field

$$t(x,y) \sim |\, R_1|^2.O \qquad (4)$$

In the illumination process, if the security hologram is misaligned (whether it is angular or positional misalignment), the transmittance function will be [13]

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

where θ is the angular misalignment in repositioning of the security hologram. Then the intensity distribution in the observation plane due to illumination of misaligned SH can be represented by product of transmittance functions g(x,y) and t'(x,y)

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

where d' is the effective period for the grating pattern on the misaligned SH. The first term of Eq (6) represents formation of sum moiré fringes, while the second term is depicting formation of the difference moiré fringes. The spatial period for these moiré fringes is

$$d_m = dd'/(d^2 + d'^2 - 2\ dd' \cos\theta) \qquad (7)$$

It becomes obvious from Eq. 7 that the proper repositioning of SH can only be achieved when d= d' and θ = 0, which could happen only when the key and security holograms are genuine. In this condition the amplitude distribution function of the reconstructed wave front is given by Eq. (4), where the information about phase distribution function $\xi(x,y)$ is modulated with intensity of recording beam and the information of the concealed phase code is not clearly visible. A spatial filtering tool is positioned in propinquity of any of the reconstructed spots and rest others spots are filtered out, of the converging beams which converts the concealed phase codes into verifiable intensity pattern, which is suitable for visual inspection for the authenticity of the security hologram.

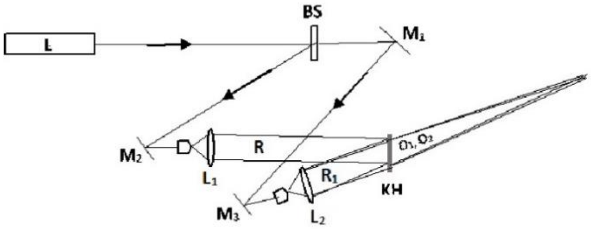

Fig.1- Schematic diagram for the formation of key hologram

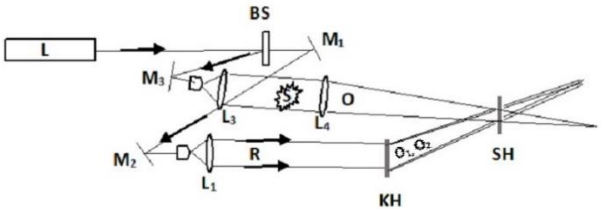

Fig.2- Schematic diagram for the formation of security hologram

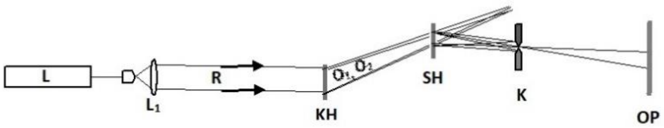

Fig.3- Schematic diagram for the reading of security hologram

III. Experiment and Results

The experimental setup for the construction of KH, SH and the retrieval of security code in reconstruction have been schematically shown in Figures 1, 2 and 3 respectively. Here, Silver halide plates were used for creating KH and SH. The light source used in experiment was a He-Ne laser having wavelength 632.8 nm. For the formation of KH, light beam was split in two beams with help of beam splitter (BS) and the convergent beam O_1 is recorded on plate KH in conjunction with collimating beam R. Now the transverse movement is given to the lens L_2, which generates the convergent beam O_2 that also got recorded on plate KH in conjunction with the same collimating beam R. For the formation of security hologram (SH), the processed KH when illuminated with beam R it serves the encoded beam R_1 which is used conjunction with beam O having phase object S into a portion between lenses L_3 and L_4 (Fig.2) In the final reading process, the processed KH and SH are repositioned at their original positions and KH is illuminated with a collimating beam. This results in multiple focus spots on predeterminant positions (Fig.4), which on divergence produce moiré pattern in the observation plane, which are due to the misalignment of SH in repositing process (Fig. 5). When SH is perfectly repositioned, which is possible only for the case of genuine KH and SH pair, these moiré fringes disappear (Fig.6). The information of secret codes (phase object) is still unreadable. A spatial filtering tool (K) was kept in propinquity of any of the reconstructed focused spots to convert the concealed phase codes into verifiable intensity pattern. Typical test results of the reconstructed concealed codes by spatial filtering are shown in Fig. 7, which ensure the hologram authenticity.

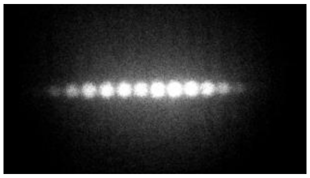

Fig.4- Photograph of multiple focus spots

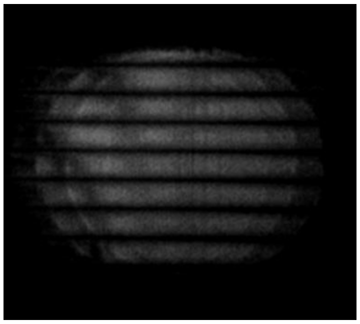

Fig. 5- Photograph of moiré pattern

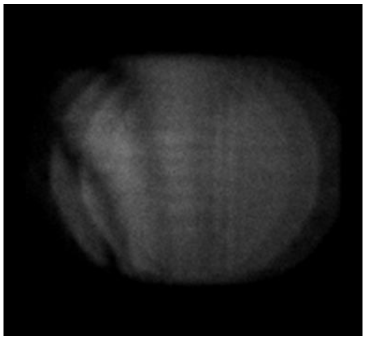

Fig.6- Photograph of null mode moiré pattern

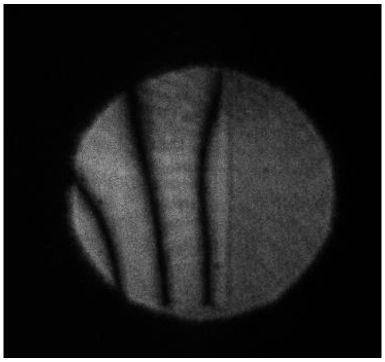

Fig.7- Retrieving phase code from the security hologram after spatial filtering

Conclusion and Discussion

A simple method for generating and retrieving concealed codes in security holograms using specially encoded dual beam is described here. In the research reported here, both encoded beams are convergent in nature. In order to enhance security multifold, this encoded dual beam recorded in key hologram could be chosen of enormously diverse forms with varying angular encoding. Because of different nature of both the beams, it makes counterfeiting or regenerating key hologram more difficult. Here key hologram plays dual role, making repositioning of security hologram easy as well as verifying its authenticity. Only in case of genuine key hologram, moiré fringes in observation plane can be disappeared and formed null moiré. As these focused spots are reconstructed at some fixed positions (angularly and azimuthally), they serve an additional anti-counterfeiting feature which may also be exploited for machine inspection. The final verification of security hologram involves a spatial filtering of the reconstructed focus spots which convert the phase codes into verifiable intensity information.

Acknowledgment

The authors are indebted to anonymous reviewer for invaluable comments and suggestions that improved the quality of the manuscript.

References

1) Javidi B. (Ed.). (2005) Optical and Digital Techniques for Information Security**,** *Springer-Verlag*, Berlin

2) Li X., Zhao M., Zhou X. and & Wang Q. H. (2018). Ownership protection of holograms using quick response encoded plenoptic watermark. *Optics Express* 26 (23), 30492-30508.

3) Wlodarczyk K. L., Ardron M., Weston N. J. & Hand D. P. (2019). Holographic watermarks and steganographic markings for combating the counterfeiting practices of high value metal products. *Journal of Materials Processing Tech.* 264, 328-335

4) Kolyuchkin V. V., Odinokov S. B., Tsyganov I. K. &Zlokazov E. Yu. (2015). The quality inspection method for master matrices of security holograms. *Physics Procedia*, 73, 313-319.

5) Lai S. (1996) Security holograms using an encoded reference wave. *Optical Engineering*, 35 (9), 2470-2472 .

6) Kaura K. K., Chhachhia D.P., Sharma A.K. & Aggarwal A. K. (2013) Security holograms readable with an encoded key hologram.*Indian Journal of Pure & Applied Physics*, 41, 696-699.

7) Aggarwal A K, Kaura S.K., Chhachhia D. P. & Sharma A. K. (2004) Encoded reference wave security holograms with enhanced features. *Journal of Optics A: Pure and Applied Optics*, **6,** 278-281.

8) Aggarwal A. K., Kaura S K., Sharma A. K., Kumar R, &Chhachhia D.P. (2004). Interferometry based security hologram readable with an encoded key hologram. *Indian Journal of Pure & Applied Physics*, 42, 816-819.

9) Aggarwal A. K., Kaura S. K, Chhachhia D.P.& Sharma A. K. (2006). Concealed Moire pattern encoded security holograms readable by a key hologram’ *Optics & Laser Technology*, 38, 117-121.

10) Sharma A. K., Chhachhia D. P. & Aggarwal A. K. (2008). Moiré pattern encoded extended fractional Fourier transform security hologram. *Journal of Modern Optics*, 55 (3), 351-359.

11) Zhang X., Dalsgaard E, Liu S., Lai H. & Chen J. (1997). Concealed holographic coding for security applications by using a moiré technique. *Applied Optics*, 36, 8096-8097.

12) Yeh S. L. (2004). Light diffusion mark constituted with two dimensional speckle patterns for enhancing hologram anticounterfeiting characteristics. *Optical. Engineering*, 43, 573-579.

13) Kaura S.K., Virdi S. P. S. & Aggarwal A. K. (2006) Holographic optical elements encoded security holograms with enhanced features. Indian Journal of Pure & Applied Physics, 44, 896-902.

***