International Research Journal of Natural and Applied Sciences
ISSN: (2349-4077)
Impact Factor 5.46 Volume 5, Issue 03, March 2018
Website- www.aarf.asia, Email : editor@aarf.asia , editoraarf@gmail.com

# Embossed Holograms: An Anticounterfeit Device for Documents Protection

Amit Kumar Sharma[a]*, Roopesh Kumar[b]

[a]Department of Physics, D.A.V. (PG) College, Dehradun
*aoemit@gmail.com

[b]Department of Physics, D.B.S. (PG) College, Dehradun

**This paper presents various cost-effective methods for realizing counterfeit-proof high security holograms. The proposed high security hologram with low-cost security verification system is primarily based on the optical encoding with either pseudo-randomly generated phase masks or other pre-designed optical phase arrays (such as moiré, holographic optical elements and complex diffraction gratings) so that their inspection by performing visual as well machine readable device is straight forward.**

**Keywords:** Hologram, Optical security, Anticounterfeit device

## Introduction

Since the earliest days of market trade, counterfeit goods have existed. In order to deter the counterfeiting of currency, passports, driver's licenses, branded products, and other instruments of value; sophisticated technologies, including holography, are currently being employed in their manufacture and production[1]. It is the objective of any security device to be able to reliably differentiate the counterfeit from the authentic good. Nevertheless, the 21st century counterfeiter can counterfeit almost all of these technologies. Rapid technological progress, especially in computers, CCD technology, color printers and scanners has made forgery and counterfeit of identification documents such as credit cards, or other important objects, increasingly simple. Anti-counterfeit security is not a product or a technique; it is a dynamic, evolving system gelled with host of

technologies. Anti-counterfeit security is an attempt to prevent valuable products or documents from being copied or falsified. Anti-counterfeit technologies are (or should be) designed to ensure that counterfeiting is too expensive to be profitable because of risk of getting caught and/or the cost of overcoming the anti-counterfeiting technologies is too prohibitive. On the other hand, advances we foresee in recording materials, hologram recording systems and embossing substrate materials, it should increase the security value of holograms in the near future[2]. At the same time, the currently available so called "security holograms" have a disadvantage because a skilled holographer can make look alike optical copies of these holograms that are very difficult to distinguish from the originals. Current techniques such as the embossed hologram with the available features on credit cards etc. are thus being defeated, and there is a strong need for a continuous development of new optical methods to be incorporated in high security embossed hologram applications so as to stay ahead of counterfeiters. In order to deter the counterfeiting, various optical validation and security verification techniques based on double random phase encoding and joint transform correlations have been widely investigated[3-7]. These techniques though excellent in their own right, are inherently complex and need specific and costly equipment to visualize or verify their security features. In order to look for simplified and cost effective solution to generate security holograms, concealed security (covert) features are introduced where the reference wave is generally encoded either through a random phase mask[8] or a key hologram[9]. When these security holograms are viewed or inspected through such a random phase mask/key hologram the verification pattern (normally a bright spot) is made available, which can conveniently be seen by an inspector or be read through a relatively simple machine-readable device. The use of an encoded reference beam though enhances the security feature immensely but could be reproduced by a hit and trial method[10]. Encoding through moiré patterns[11,12] have also been exploited successfully toenhance the anticounterfeit ability of security holograms for visual inspection. The concealed part (one of the periodic pattern) of these moiré pattern security holograms is directly recorded as a secret phase code superimposed on a pre-designed holographic image, which is read by another periodic pattern (used as a decoder) to form the moiré images. Though the concealed part is in the form of a phase pattern, but with the advanced phase reading and recording devices, such as phase contrast microscopy, optical scanning microscopy, etc, a possibility of copying them always exist.

In order to overcome these problems, various methods of making enhanced feature security holograms are described, where additional security elements have been incorporated in the verification pattern in conjunction with encoded reference beam[10,13,14]. These additional security elements are in the form of multiple focusing spots containing either interferometric or moiré features. In these security holograms the level of difficulty for counterfeiting have been increased manifold as they contain enhanced security features in 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. Further, the relative repositioning of key and security holograms is made easy by making key hologram in the form of specially encoded complex holographic optical element.

## Encoded Key Hologram

The methods reported in this paper are based on the formation of an encoded key hologram (KH) and the security hologram (SH) separately in two recording steps. The key hologram is formed by combining the wave generated through a random phase plate (RP) with a collimated beam [Fig.1]. This encoded key hologram, when illuminated with a collimated beam, provides an encoded reference wave for recording and reading the security holograms.

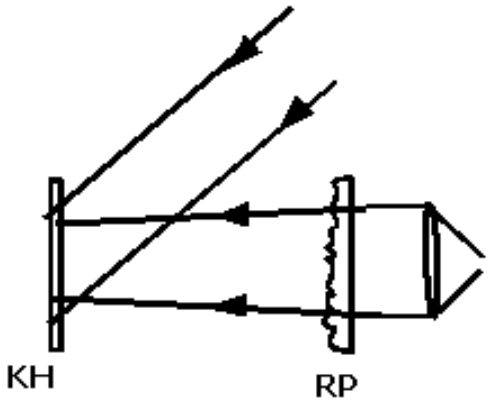



Fig. 1 – Schematic for recording diffuse key holograms

## Enhanced Feature Security Holograms

These security holograms contain enhanced security features in addition with angular and azimuth encoding[13,14], which can only be read through an encoded key hologram. In the final reading process, two spatially separated sharp focus spots (bright spots) emerge only when the security hologram is illuminated by the decoding, reconstructing beam, generated from the encoded key hologram. These bright focused spots, used as verification feature, can conveniently be read through a relatively simple machine-readable device. In addition these focused spots upon divergence in the longitudinal direction further generate either regular interferometric patterns, i.e. circular and/or linear fringes or random interferometric patterns, i.e. irregular profile fringes [Fig.2]. These variable interferometric patterns further facilitate in the visual inspection of these additional/enhanced security verification features contained in these security holograms. These security holograms are suitable for both visual as well as machine inspection. If photoelectric detectors are placed at the reconstructed focus spots and threshold circuit is used, the authentic security hologram can be identified / verified automatically through machine inspection. The additional variable interferometric features contained in these focused spots can be used for visual inspection for further verifying the authenticity of these

holograms and also make these security holograms virtually impossible to counterfeit.This type of holograms can also be used as security codes for better protection against counterfeiting in the embossed holograms.

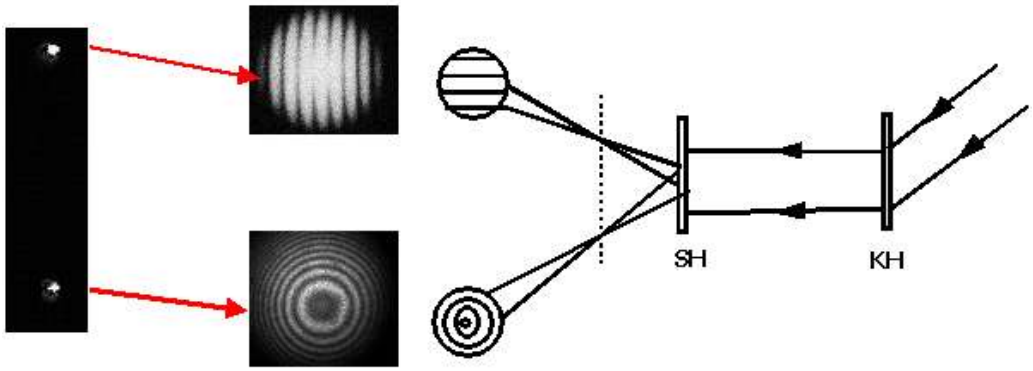



Fig. 2 – Schematic for reading security holograms containing variable interferometric features in the reconstructed focus spot images

It is observed that the sensitivity in the placement of the key and the security hologram mainly depends on the randomness of the wavefront generated from the key hologram. As the randomness of the wavefront is increased, the sensitivity requirement in positioning of both the key and security hologram also becomes more critical. Using a special encoded complex holographic optical element (containing pre-designed interferometric wavefront) instead of hologram having diffuse and distorted wavefront as a key, alignment problem can be greatly reduced.

## Interferometric Holographic Key Encoded Security Holograms

A specially encoded complex holographic optical element, which produces a pre-designed interferometric wavefront, is used as key hologram (IHK) [Fig.3] to encode security holograms. When security holograms are read through this specially formed encoded key hologram, specific moiré-like fringe pattern is formed in the case of an authentic security hologram.These moiré-like fringe patterns,observedon the security hologram, are formed due to superposition of complex holographic interferometric sinusoidal phase patterns generated from key hologram and those recorded in security hologram.

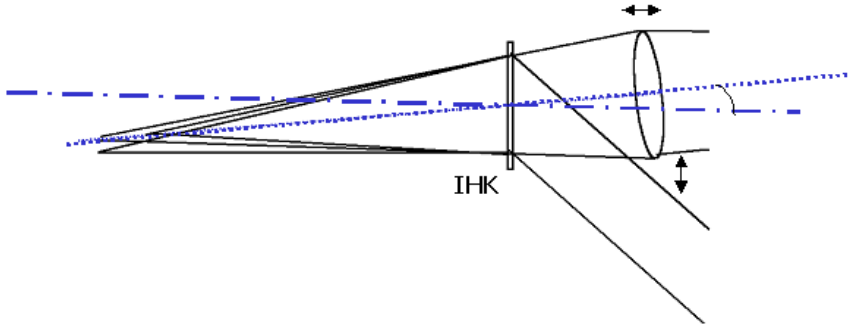



Fig.3 – Schematic for recording interferometric encoded key holograms

The complex amplitude distribution at security hologram due to misalignment θ is

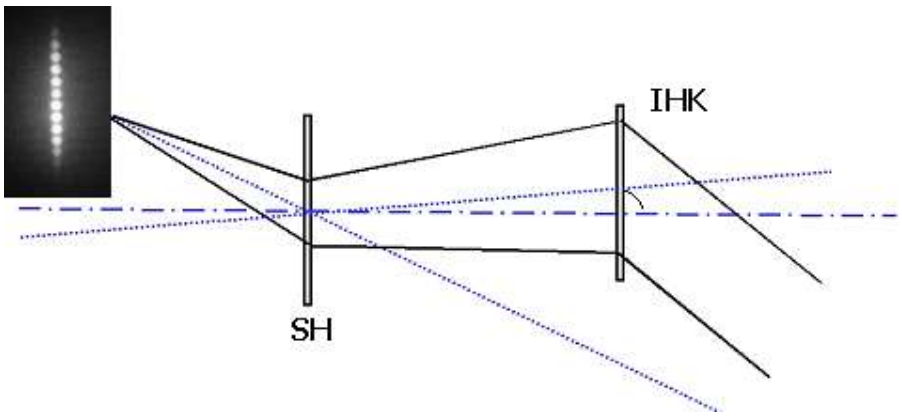
$t(x,y) \sim 1 + \cos 2\pi(\mu x - \nu y) + \cos 2\pi (a - b)(\mu x - \nu y) + \cos 2\pi (a + \varepsilon - b)(\mu x - \nu y)$

$+ \cos 2\pi\mu_0 x + \cos 2\pi\mu_0 x \cos 2\pi(\mu x - \nu y) + \cos 2\pi\mu_0 x \cos 2\pi (a - b)(\mu x - \nu y)$

$+ \cos 2\pi\mu_0 x \cos 2\pi (a + \varepsilon - b)(\mu x - \nu y)$ ----------(1)

where $\mu = \cos\theta / d$ , $\nu = \sin\theta / d$ and $\mu_0 = 1/d$ ; 'd' is the fringe spacing in key and security holograms, 'a' is wave propagation vector and 'ε' is the difference between two waves recorded in IHK and 'b' is the wave propagation vector in security hologram. In the right hand side of Eq. (1), 6$^{th}$ term denotes the presence of a complex moiré-like fringe pattern on the security hologram.

These complex holographic interferometric sinusoidal phase patterns are very resistant against counterfeitingthrough conventional copying methods. These specific moiré-like fringe patterns are used for visual inspection of the security hologram. Further, several spatially separated bright focused spots gets generated from the security hologram. These bright spots, formed at predetermined fixed positions, may be exploited for machine inspection. By making slight adjustments in the security hologram, this specific moiré-like fringe pattern disappears only for an authentic security hologram, when the complex holographic interferometric sinusoidal phase patterns generated from key hologram and those recorded in security hologram completely overlap each other [Fig.4].



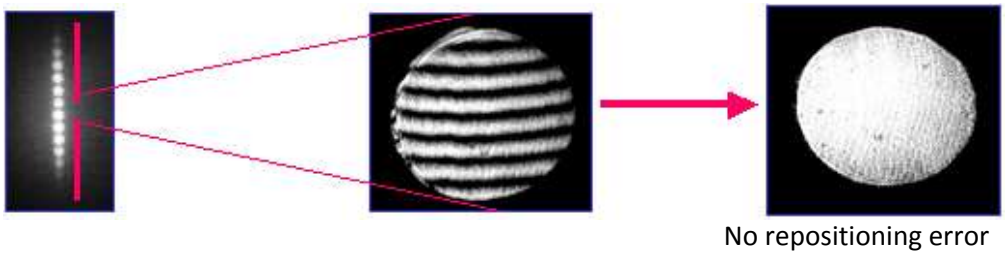



Fig. 4 – Schematic for reading security holograms having moiré fringe patterns

These security holograms contain three fold concealed and encoded anti-counterfeit security features which can only be decoded by using an encoded HOE key in the reading process. Since the visually verifiable moiré-like fringe pattern formed on the security hologram and in the observation plane are in addition to the sharp focus spots, this type of security holograms are suitable for both visual and as well as machine inspection. Further, as these security holograms contain complex holographic interferometric sinusoidal phase patterns rather than a binary pattern, this makes these security holograms virtually impossible to counterfeit. Also the sensitivity requirement in positioning of the security hologram in reading process is not critical as wavefront generated from key is not diffuse.

## Conclusion

This paper presents various simple and cost effective methods for making security holograms, which employ both machine and visually verifiable security features in addition to encoded reference beam. In the verification process, specific interferometric /moiré patterns (fringes of random profile) emerge as an additional visually 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 those 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. The advantage of making key holograms lies in the fact that a large number of keys can be made, for distribution to the users, either by directly using the experimental setup or holographic copies of the key hologram can be generated by using hologram copying techniques.

**References:**


1.Van Renesse RL (Ed)., Optical Document Security. Boston/London, p 69-225, UK: Artech House, 1998.

2. Lancaster I (Ed), Holopack Holoprint Guidebook, p 139-54, (Reconnaissance International Publishersand Consultants, Leatherheads, Surrey, UK), 2000.

3. Wang RK, Watson IA, Chatwin C, "Random phase encoding for optical security", Opt. Eng., **35**, 2464 -2469, 1996.

4. Refregier P, Javidi B, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett. **20,** 767-769, 1995.

5. Neto LG, Sheng Y, "Optical implementation of image encryption using random phase encoding", Opt. Eng., **35,** 2459-2463, 1996.

6. Javidi B, Horner JL, "Optical pattern recognition for validation and securityverification" Opt. Eng. **33**, 1752-1756, 1994.

7. Weber D, Trolinger J, "Novel implementation of nonlinear joint transform correlators in optical security and validation", Opt. Eng., **38**, 62-68, 1999.

8. Lai S, "Security holograms using an encoded reference wave" Opt. Eng., **35**, 2470-2472, 1996.

9. Kaura SK, Chhachhia DP, Sharma AK, Aggarwal AK, "Security holograms readable with an encoded key hologram", Indian J. of Pure & Appl. Physics, **41**, 696-699, 2003.

10.Aggarwal AK, Kaura SK, Chhachhia DP, Sharma AK, "Encoded reference wave security holograms with enhanced features" J. of Opt A: Pure and Appl. Opt. **6** 278-281, 2004.

11. Liu S, Zhang X, Lai H, "Artistic effect and application of moiré patterns in security holograms" Appl. Opt., **34**, 4700-4702, 1995.

12. Sharma AK, Chhachhia DP Aggarwal AK, "Moiré pattern encoded extended fractional Fourier transform security hologram" J. Mod. Opt., **55**(3), 351-359, 2008.

13. Aggarwal AK, Kaura SK, Chhachhia DP, Sharma AK, "Concealed moiré pattern encoded security holograms readable by a key hologram" Opt. & Laser Tech., **37**, 117-121, 2006.

14. Aggarwal AK, Kaura SK, Sharma AK, Kumar R, Chhachhia DP, "Interferometry based security hologram readable with an encoded key hologram", Indian J. of Pure & Appl. Physics,**42**, 816-819, 2004.