Optica Applicata, Vol. LII, No. 3, 2022
DOI: 10.37190/oa220305

Concealing information in security hologram using interferometry

Amit Kumar Sharma[1], Prashant Chauhan[2], Anshu D Varshney[2*]

Department of Physics, D.A.V. (PG) College, Dehradun

Department of Physics and Materials Science and Engineering, Jaypee Institute of Information Technology, Noida 201309, Uttar Pradesh, India

[*]Corresponding author: anshu.varshney@jiit.ac.in

A new method utilizing holographic interferometry technique is described to conceal information in security holograms for enhancing their anti-counterfeiting ability. This concealed information can only be imitated if security hologram is illuminated through correct decoding wavefront generated through a key hologram. In decoding process, three spatially separated focus spots emerge at predefined positions which upon divergence further generate interferometric fringes modulated with concealed information in them. When security hologram is perfectly aligned, interferometric fringes disappear and concealed information becomes visible. The advantage of encoding through this technique lies in the fact that relative repositioning of key and security hologram becomes much easier and also additionally brings multifold improvement in the security level of the verification systems.

Keywords: hologram, security hologram, encoded hologram, information encoding, concealed phase.

1. Introduction

Holograms are one of the most popular reliable means for authenticity identification of official papers, plastic cards and any goods [1,2]. They are found to be resistant to counterfeit alteration, duplication or simulation [3,4], impossible to transpose and easily recognizable to traders, the public and customs officials. However rapid technological advances especially in the area of opto-electronics instrumentation are making it increasingly simple for counterfeiter to reproduce a new look-a-like hologram. It is difficult, for a normal eye, to determine whether such a hologram is genuine or counterfeit. The technologies of making holograms are therefore required to be enhanced continuously. Many researchers have investigated various techniques like water mark and steganographic marking, random phase encoding and correlation pattern recognition to increase the difficulty of counterfeiting the security hologram [5–8]. These techniques improve the difficulty level for counterfeit alteration, but many of them required fine control of the optical axis alignment and also need specific and costly equipment to decode the encoded features. A number of cost-effective holograms encoding schemes such as double exposure holographic interferometry in conjunction with random diffuser key hologram [9], using an encoded reference beam [10,11], artistic visualization of moiré pattern produced by key and security holograms pairs [12–14], speckle pattern [15], dot matrix encoding [16,17] or a combination of these have also been reported for authenticity verification and anti-counterfeiting purposes. For encoding of verification features in security holograms, random diffusers based approaches are considered more effective. However, the random diffuser based arrangements are suffered with critical value of mutual placement tolerance of security hologram and random diffuser. Random diffuser displacing about a half of diffuser feature, causes verification feature disappearance. The use of convergent beam in security hologram recording in conjunction with a key hologram containing two convergent beams in a single recording step is also reported [18]. In final reading process, this security hologram generates 10–12 closely packed focus spots which on diversion shows moiré -like fringes in an observation plane. Specific moiré-like fringe pattern of security hologram with the double exposure holographic interferometry is also described [19]. In such holograms, during the final reading process, a specific moiré-like fringe pattern is formed on the security hologram only when it is exposed by the decoding reconstruction beam, generated from the encoded key hologram. The technique though enhances visual appeal of security hologram, has limitations to hide random phase information. To circumvent these problems and to make the security hologram which is easy to align with increased anticounterfeit ability, two reference beam holographic interferometry technique for concealing phase information is proposed in this paper. Two reference beam holographic interferometry [20] is a well-known phenomenon used for nondestructive testing. In this technique, two images have their own reconstruction beams, where one has access to each image separately as well as to their mutual interference pattern. However, to our knowledge, there is no reference in the literature citing the use of two reference beam holographic interferometric techniques for optical security purposes. The two-reference beam holographic interferometry technique offers two new additional benefits over previously reported techniques in terms of improvement of the security level multifold, and relative repositioning of key and security hologram becomes much easier.

2. Principle of the method

The method reported in this paper for the formation of key and security hologram is based on the principle of two reference beam holographic interferometry. In these security holograms, two different states of phase information are recorded with two different reference beams. These two different reference beams are recorded simultaneously as a key hologram (KH) along with security hologram (SH) in two steps. Figure 1 shows the first recording step of the method, where a collimated beam R_1 is recorded with

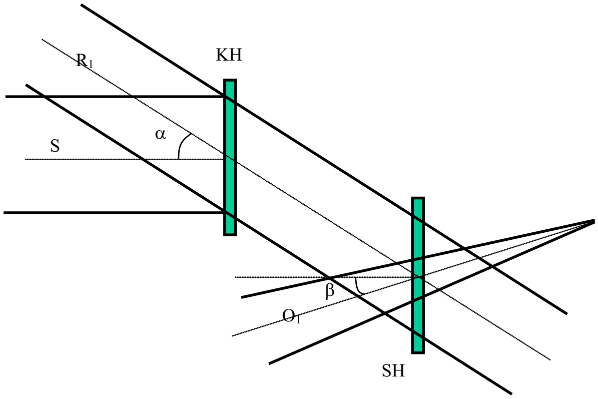

Fig. 1. Schematic of experimental layout for recording scheme of key and security hologram: first step.

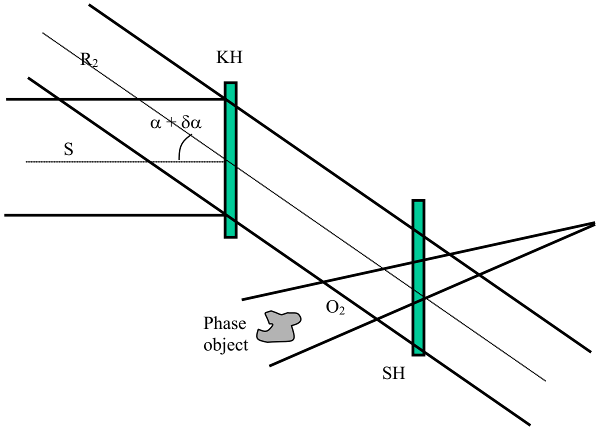

Fig. 2. Schematic of experimental layout for recording scheme of key and security hologram: second step.

a beam S at KH and simultaneously the same R_1 is recorded with another convergent beam O_1 at SH. Before making the second recording on the same plate, the collimated beam R_1 is given a minute angular movement which generates a slightly different beam R_2. In the second recording step, the beam R_2 is used in conjunction with the same reference beam S at KH, whereas for recording SH, the convergent beam O_2 (generated through insertion of a phase object in the beam O_1) is recorded with the beam R_2 (Fig. 2). When these security holograms are read through the genuine key hologram, three spatially separated bright focused spots are generated, which on divergence form interferometric fringe patterns modulated with concealed phase information at an output plane (Fig. 3). A careful spatial filtering of these bright focused spots results in high contrast interferometric fringe patterns in the observation plane. When security hologram is perfectly aligned with KH, the interferometric fringe patterns disappear and it provides direct visual information about the random phase distribution of a con-

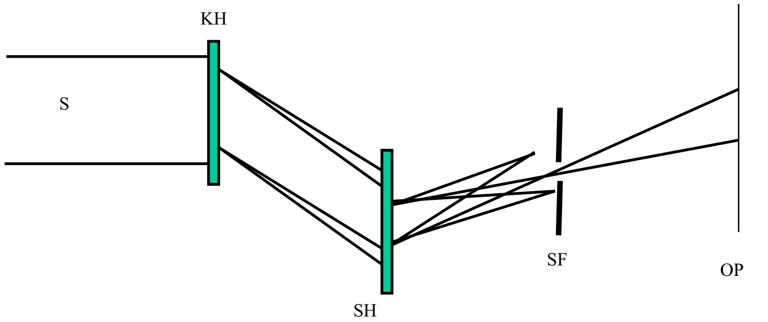

Fig. 3. Schematic of experimental layout for reading the security hologram.

cealed phase, which ensures the hologram authenticity. It is to be noted that the perfect alignment (*i.e.* disappearance of interferometric fringes) is possible with a genuine key and security hologram pair only.

To make the mathematical formulations simple, we have considered O_1 and O_2 as plane wavefronts. In this case, R_1 is taken propagating at an angle α_0 to the axis to form KH, R_2 propagating at an angle $\alpha_0 + \delta\alpha$ to the axis and S propagating along the axis. A different convergent object beam O_1 is propagating at an angle β to the axis and O_2 denotes the beam after insertion a phase object (φ) in beam O_1. The complex amplitude distribution of R_1, R_2, S, O_1 and O_2 can be considered as

$$R_1 = A_\mathrm{r}\exp(-iax);\quad \text{where } a = k\sin\alpha_0 \tag{1}$$

$$R_2 = A_\mathrm{r}\mathrm{eexp}[-i(a+\varepsilon)x];\quad a+\varepsilon = k\sin(\alpha_0+\delta\alpha) \text{ and } \varepsilon = k(\delta\alpha)\cos\alpha_0 \tag{2}$$

$$S = A_\mathrm{s}\exp(ikx) \tag{3}$$

$$O_1 = A_\mathrm{o}\exp(-ibx);\quad \text{where } b = k\sin\beta \tag{4}$$

$$O_2 = A_\mathrm{o}\exp[-i(b+\varphi)x] \tag{5}$$

where A_r, A_s, and A_o are the constant amplitudes of the respective beams. The amplitude transmittance of the processed KH is

$$t_1 \sim [|R_1+S|^2 + |R_2+S|^2] \tag{6}$$

The amplitude transmittance of the processed SH is

$$t_2 \sim [|R_1+O_1|^2 + |R_2+O_2|^2] \tag{7}$$

The complex amplitude of the transmitted field from KH, when illuminated with the beam S, is

$$U_1 \sim St_1 = S|R_1|^2 + S|S|^2 + R_1|S|^2 + R_1^*S^2 + S|R_2|^2 + S|S|^2 + R_2|S|^2 + R_2^*S^2 \tag{8}$$

Here $|S|^2$ can be considered as constant across KH, since the plane reference wave S is used for illumination of KH. Thus only 3rd and 7th terms on the right-hand side of Eq. (8) are of interest to us as they represent two generated beams R_1 and R_2, *i.e.*:

$$|S|^2R_1 + |S|^2R_2 = \text{constant}.R_1 + \text{constant}.R_2 \tag{9}$$

After processing, the SH is repositioned at the same location at which it was recorded. In this configuration, when KH is illuminated with a collimated beam, it provides two illuminating beams R_1 and R_2 for SH. During the final reading process, when there is a slight misalignment in the angle θ with the axis of KH, then it can be considered that SH is illuminated with changed beams R_1' and R_2', where $R_1' = A_\mathrm{r}\exp(-iax')$ and $R_2' = A_\mathrm{r}\exp(-i(a+\varepsilon)x')$; $x' = x\cos\theta$, then amplitude transmittance of the SH is

$$\begin{aligned} U_2 &\sim (R_1' + R_2')[|R_1 + O_1|^2 + |R_2 + O_2|^2] \\ &= R_1'(|R_1|^2 + |O_1|^2) + R_1'R_1^*O_1 + R_1'R_1O_1^* + R_2'(|R_1|^2 + |O_1|^2) + R_2'R_1^*O_1 + R_2'R_1O_1^* \\ &\quad + R_1'(|R_2|^2 + |O_2|^2) + R_1'R_2^*O_2 + R_1'R_2O_2^* + R_2'(|R_2|^2 + |O_2|^2) + R_2'R_2^*O_2 + R_2'R_2O_2^* \end{aligned} \tag{10}$$

On the right hand side of Eq. (10), 1st and 10th terms are self-reconstruction terms, 4th and 7th are cross reconstruction terms, 2nd and 11th are two primary reconstruction terms, 5th and 8th are mixed primary reconstruction terms, all the rest are conjugate terms. Only primary and mixed primary terms in Eq. (10) are of our interest. Thus

$$\begin{aligned} U_3 &= R_1'R_1^*O_1 + R_2'R_2^*O_2 + R_2'R_1^*O_1 + R_1'R_2^*O_2 \\ &= (R_1' + R_2')(R_1^*O_1 + R_2^*O_2) \end{aligned} \tag{11}$$

The resultant intensity distribution $I_1(x)$ in the observation plane could be written as

$$\begin{aligned} I_1(x) &= \left|(R_1' + R_2')(R_1^*O_1 + R_2^*O_2)\right|^2 \\ &= \left|(R_1' + R_2')\right|^2 \left|(R_1^*O_1 + R_2^*O_2)\right|^2 \\ &\sim (1 + \cos\varepsilon x')(1 + \cos(\varepsilon - \varphi)x) \\ &= 1 + \cos\varepsilon x' + \cos(\varepsilon - \varphi)x + \cos\varepsilon x' \cos(\varepsilon - \varphi)x \end{aligned} \tag{12}$$

These terms depict the presence of various interferometric fringes overlapping each other. It is further seen that a careful spatial filtering of primary reconstruction terms results in the generation of high contrast interferometric fringes in the observation plane. *i.e.*

$$U_4 = R_1'R_1^*O_1 + R_2'R_2^*O_2 \tag{13}$$

The resultant intensity distribution $I_1(x)$ in the observation plane could be written as

$$
\begin{aligned}
I_2(x) &= \left|R_1' R_1^* O_1 + R_2' R_2^* O_2\right|^2 \\
&\sim 2 + \exp(-i\varepsilon x')\exp(i(\varepsilon - \varphi)x) + \exp(i\varepsilon x')\exp(-i(\varepsilon - \varphi)x) \\
&= 2 + \exp(-i\varepsilon \cos\theta x)\exp(i(\varepsilon - \varphi)x) + \exp(i\varepsilon \cos\theta x)\exp(-i(\varepsilon - \varphi)x) \\
&= 2 + \exp(i(\varepsilon - \varphi - \varepsilon\cos\theta)x) + \exp(-i(\varepsilon - \varphi - \varepsilon\cos\theta)x) \\
&= 2 + 2\cos(\varepsilon - \varphi - \varepsilon\cos\theta)x \\
&\sim \cos^2[(\varepsilon - \varphi - \varepsilon\cos\theta)/2]x
\end{aligned}
\tag{14}
$$

From Eq. (14), it is clear that intensity distribution, which has concealed phase information φ, varies with interferometric fringes formed due to the misalignment of SH in the angle θ with the axis of KH.

When security hologram is perfectly repositioned (*i.e.* $\theta = 0$), the interferometric fringes get disappeared and concealed phase information (φ) become visible. Under this condition, Eq. (14) becomes

$$I_2(x) \sim \cos^2(\varphi/2)\,x \tag{15}$$

where $\cos^2(\varphi/2)\,x$ shows phase information for verification process. In our method, the use of collimating beams in recording the key hologram is advantageous in terms of alignment and repositioning [21,22] of the security hologram in the reading process.

3. Experimental description and results

In this experimental arrangement, a He-Ne laser (Coherent model 31-2140, 35 mW output power, 632.8 nm wavelength) was used in the recording of encoded key hologram, security hologram and in the final reading process of security holograms. Silver halide holographic recording plates of size 63 mm × 63 mm were used for making KH and SH, where the diameters of the recording beams on KH and SH were 50 mm. The beam R_2 was generated giving 2^0 angular movements to the beam R_1. In this experiment, for incorporation of concealed phase information as a security feature, a soldering gun was inserted in the beam O_1, which was kept switch off during the first exposure and was

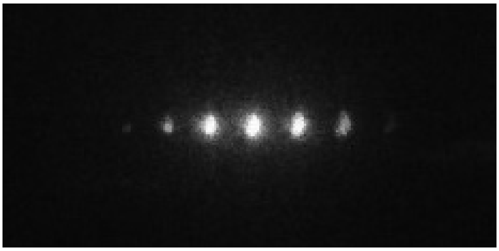

Fig. 4. Photograph of typical results obtained due to the reconstructed spatially separated bright focus spots.

switched-on during the second exposure. The experimental layout for the final reading process of these security holograms is shown in Fig. 3. Here, a collimated beam is used to illuminate the KH, where the KH is placed at a predetermined fixed position. The wavefront derived from the KH serves as a decoding reconstructing beam for reading the SH and three spatially separated bright focused spots are generated from the security hologram (Fig. 4) forming the overlapped interferometric fringe patterns in the observation plane (Fig. 5). A careful spatial filtering (SF) of these focused spots, where only the central spot is allowed to pass through, results in the generation of a high

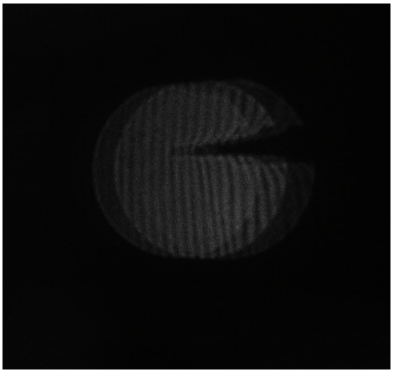

Fig. 5. Photograph of interferometric fringes due to unfiltered focused spots.

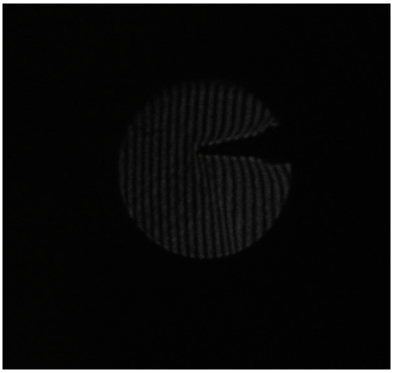

Fig. 6. Photograph of interferometric fringes due to spatially filtered bright focused spots.

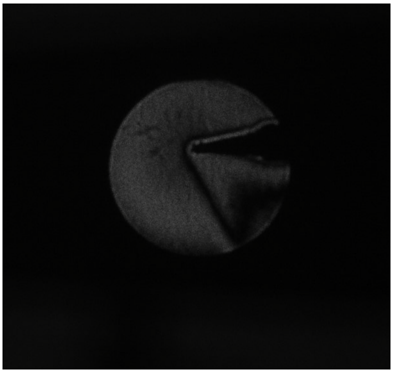

Fig. 7. Photograph of verification fringes due to concealed phase object is retrieved only when SH is perfectly repositioned.

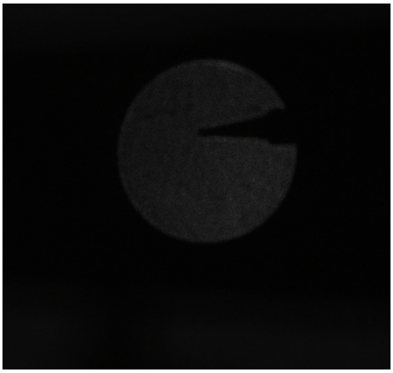

Fig. 8. No verification fringe are obtained when SH is illuminated with simple collimated Beam.

contrast interferometric features in the observation plane OP (Fig. 6). Further, these interferometric fringes disappear as the security hologram is perfectly repositioned in case of the genuine key and security hologram pair and the concealed phase information becomes visible (Fig. 7). Hidden phase information remains concealed if one tries to decode the security hologram with a wrong beam (Fig. 8).

4. Discussion and conclusion

The present schemes employ two beam holographic interferometric techniques for concealing phase information in security hologram. In the decoding process, the key hologram is used to illuminate the security hologram, three spatially separated bright focused spots are generated from the security hologram which additionally contains interferometric fringes. The additional bright spots generated from the security hologram are due to nonlinear recording. It may be noted that these bright spots, formed at a predetermined fixed location (angular and azimuth position), may also be gainfully used for machine inspection. A careful spatial filtering of these bright focused spots results in high contrast interferometric fringe patterns at the observation plane, which additionally contains hidden phase information. Although random diffuser based arrangements are effective, achieving mutual alignment and repositioning between the key hologram and the security hologram is very critical. Encoding through two beam interferometry makes relative repositioning of the key and security hologram much easier and also enhances multifold improvement in the security level of the verification systems.When the security hologram is perfectly repositioned, which is possible only in case of the genuine key and security hologram pair, the interferometric fringepatterns disappear and the concealed phase information becomes visible for visual inspection. These types of security holograms are suitable for both visual and as well as machine inspection. The phase information in security hologram is concealed, random in nature and encoded using two such reference beams by the holographic technique whose nature, angular and azimuth encoding parameters are unknown. The chances of their regeneration by counterfeiter are almost negligible, which enhances the anti-counterfeit ability of security holograms multifold. Also, the sensitivity requirement in positioning of the security hologram in the reading process is not critical as plane wavefronts were used for encoding.

References

[1] Van Renesse R.L. [Ed.], *Optical Document Security*, Artech House, Boston/London, UK, 1998, pp. 169–225.

[2] Lancaster I. [Ed.], *Holopack Holoprint Guidebook*, Reconnaissance International, Leatherheads, Surrey, UK, 2000, pp. 139–154.

[3] Chesak C.E., *Holographic counterfeit protection*, Optics Communications **115**(5–6), 1995, pp. 429–436, DOI: 10.1016/0030-4018(94)00477-C.

[4] Janucki J., Owsik J., *A holographic method for document protection against counterfeit*, Optics Communications **228**(1–3), 2003, pp. 63–69, DOI: 10.1016/j.optcom.2003.09.083.

[5] Wlodarczyk K.L., Ardron M., Weston N.J., Hand D.P., *Holographic watermarks and steganographic markings for combating the counterfeiting practices of high-value metal products*, Journal of Materials Processing Technology **264**, 2019, pp. 328–335, DOI: 10.1016/j.jmatprotec.2018.09.020.

[6] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[7] Wang R.K., Watson I.A., Chatwin C.R., *Random phase encoding for optical security*, Optical Engineering **35**(9), 1996, p. 2464, DOI: 10.1117/1.600849.

[8] Zlokazov E.Yu., Starikov R.S., Odinokov S.B., Tsyganov I.K., Talalaev V.E., Koluchkin V.V., *Specificity of correlation pattern recognition methods application in security holograms identity control apparatus*, Physics Procedia **73**, 2015, pp. 308–312, DOI: 10.1016/j.phpro.2015.09.143.

[9] Aggarwal A.K., Kaura S.K., Sharma A.K., Kumar R., Chhachhia D.P., *Interferometry based security hologram readable with an encoded key hologram*, Indian Journal of Pure & Applied Physics **42**, 2004, pp. 816–819.

[10] Lai S., *Security holograms using an encoded reference wave*, Optical Engineering **35**(9), 1996, p. 2470, DOI: 10.1117/1.600850.

[11] Aggarwal A.K., Kaura S.K., Chhachhia D.P., Sharma A.K., *Encoded reference wave security holograms with enhanced features*, Journal of Optics A: Pure and Applied Optics **6**(2), 2004, p. 278, DOI: 10.1088/1464-4258/6/2/020.

[12] Liu S., Zhang X., Lai H., *Artistic effect and application of moiré patterns in security holograms*, Applied Optics **34**(22), 1995, pp. 4700–4702, DOI: 10.1364/AO.34.004700.

[13] Zhang X., Dalsgaard E., Liu S., Lai H., Chen J., *Concealed holographic coding for security applications by using a moiré technique*, Applied Optics **36**(31), 1997, pp. 8096–8097, DOI: 10.1364/AO.36.008096.

[14] Aggarwal A.K., Kaura S.K., Chhachhia D.P., Sharma A.K., *Concealed moiré pattern encoded security holograms readable by a key hologram*, Optics & Laser Technology **38**(2), 2006, pp. 117–121, DOI: 10.1016/j.optlastec.2004.10.010.

[15] Yeh S.L., *Light-diffusion mark constituted with two-dimensional speckle patterns for enhancing hologram anticounterfeiting characteristics*, Optical Engineering **43**(3), 2004, p. 537, DOI: 10.1117/1.1641786.

[16] Lu Y.T., Chi S., *Compact, reliable asymmetric optical configuration for cost effective fabrication of multiplex dot matrix hologram in anti-counterfeiting applications*, Optik **114**(4), 2003, pp. 161–167, DOI: 10.1078/0030-4026-00241.

[17] Yeh S.L., *Using random features of dot-matrix holograms for anticounterfeiting*, Applied Optics **45**(16), 2006, pp. 3698–3703, DOI: 10.1364/AO.45.003698.

[18] Kaura S.K., Chhachhia D.P., Aggarwal A.K., *Interferometric moiré pattern encoded security holograms*, Journal of Optics A: Pure and Applied Optics **8**(1), 2006, p. 67, DOI: 10.1088/1464-4258/8/1/010.

[19] Kaura S.K., Virdi S.P.S. Aggarwal A.K., *Holographic optical elements encoded security holograms with enhanced features*, Indian Journal of Pure & Applied Physics **44**, 2006, pp. 896–902.

[20] Dandliker R., Marom E., Mottier F.M., *Two-reference-beam holographic interferometry*, Journal of the Optical Society of America **66**(1), 1976, pp. 23–30, DOI: 10.1364/JOSA.66.000023.

[21] Dandliker R., Thalmann R., Willemin J.-F., *Fringe interpolation by two-reference-beam holographic interferometry: Reducing sensitivity to hologram misalignment*, Optics Communications **42**(5), 1982, pp. 301–306, DOI: 10.1016/0030-4018(82)90236-X.

[22] Sharma A.K., Kaura S.K., Chhachhia D.P., Mahajan C.G., Aggarwal A.K., *Holographic optics based two-channel interferometer*, Indian Journal of Pure & Applied Physics **44**, 2006, pp. 501–508.

Received May 26, 2021
in revised form October 19, 2021