Optics Communications 284 (2011) 735–739

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Flexible optical encryption with multiple users and multiple security levels

Naveen K. Nishchal [a,*], Thomas J. Naughton [b,c]

[a] Department of Physics, Indian Institute of Technology Patna, Patna-800 013, India
[b] Department of Computer Science, National University of Ireland Maynooth, Ireland
[c] RF Media Laboratory, Oulu Southern Institute, University of Oulu, Ylivieska, Finland

ARTICLE INFO

Article history:
Received 5 July 2010
Received in revised form 8 September 2010
Accepted 27 September 2010

Keywords:
Optical image encryption
Information security
Fractional Fourier transform
Three-dimensional image processing
Digital holography

ABSTRACT

We present a basic optical encryption architecture that admits several cryptography applications based on multiplexing. Users can decrypt different private images from the same encrypted image, a superuser can have a key that decrypts all encrypted images, and multiplexed images can be encrypted with different levels of security. This system is presented in the context of a general framework of optical encryption application development. We illustrate with a real-world three-dimensional scene, captured with digital holography, and encrypted using the fractional Fourier transform, where different users have access to different three-dimensional objects in the scene.

1. Introduction

Optical encryption has reached a level of maturity recently with the publication of realistic attacks [1–5] that exploit its inherent weakness of linearity. This serious security problem associated with repeated use of the same key can be defended against through the use of modes of encryption [6], which promise to make optical encryption a viable symmetric cryptosystem. The repeated cycle of publication of an attack followed by publication of an appropriate defense is the natural lifecycle of conventional cryptosystems. To encourage widespread use, the field of optical encryption should offer a cohesive and fully-featured suite of practical and unique applications. A single framework for the different applications will allow a single optical hardware arrangement to support this wide range of applications without modification. The aim of this communication is to illustrate one such framework and associated suite of applications.

In the sister field of compression, data compression and image compression have distinct uses. Data compression is synonymous with lossless data compression and in image compression some loss and defects can be tolerated for vastly increased compression ratios and computational efficiency. Similarly, data encryption and image encryption have different motivations, and optical-based techniques are particularly suited for the latter. One unique property of image encryption is that it tolerates lossy multiplexing, which mitigates any disadvantages of optical encryption compared to electronic encryption. The suite of encryption applications presented in this study is based on the concept of secure multiplexing [7] of optical images. In the scenario of a single encrypted image shared between multiple users each with their own private unique decryption key, we consider three user cases, where (i) each user decrypts a different private image, (ii) as before, but where a superuser can view all private images using their master private key, and (iii) different objects in the encrypted image have different security levels.

The most well known optical encryption scheme, double random phase encoding [8], is chosen as the base of our proposed framework. Our demonstration encompasses many generalities. The Fourier transform is replaced by the fractional Fourier transform (FRT) [9–13], and we encrypt three-dimensional (3D) objects captured through digital holography. Multiplexing has been used to encode multiple encrypted two-dimensional images in a single encrypted image, either superposed [14–16] or spatially separated [11,17–19]. For 3D objects, optical encryption has been demonstrated [20], and also a hologram watermarking technique can be regarded as a restricted example of multiplexing two such objects [21]. Although a hierarchical optical security system has been reported [22], in this case the decryption key consists only of a small sequence of scalars. A multi level image encryption method has also been proposed based on cascaded multiple-phase retrieval by an iterative Fresnel transform algorithm [23]. In another communication [24], in order to increase the data security transmission, a multichannel puzzle-like encryption method was proposed. In that method, the input information is decomposed and each decomposed part is encrypted separately. To retrieve the whole information, the properly decrypted channels are composed. Using the full capacity of both amplitude and phase of an object as separate channels, an encryption scheme was proposed [25]. In this scheme, different information can be coded in amplitude and

[*] Corresponding author. Tel.: +91 612 2552027; fax: +91 612 2277383.
E-mail address: nkn@iitp.ac.in (N.K. Nishchal).

0030-4018/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2010.09.065

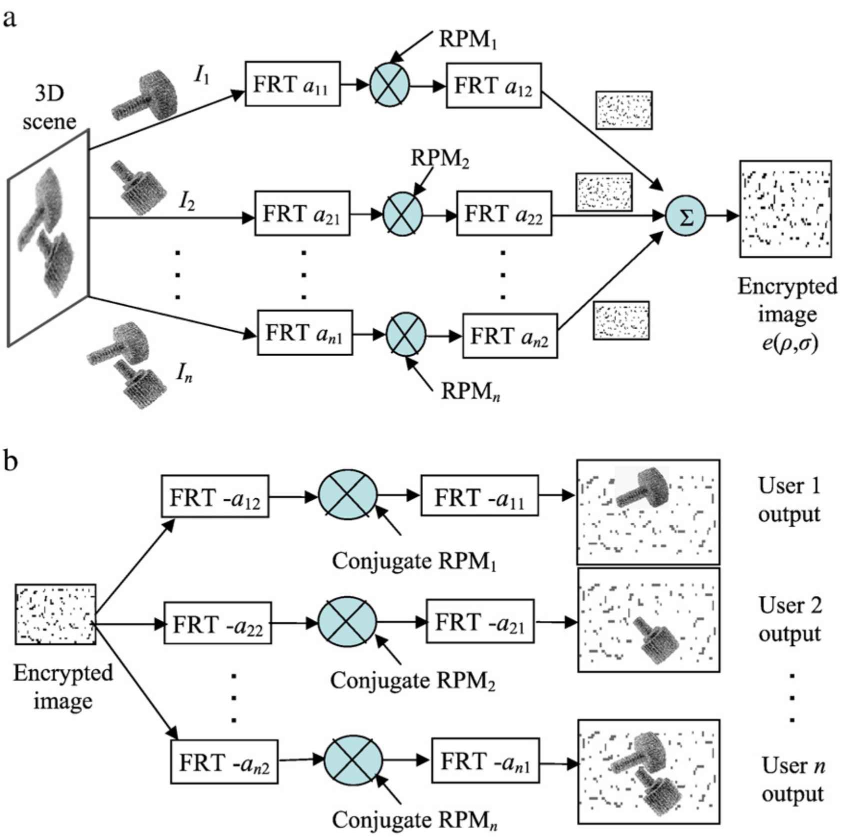

Fig. 1. Schematic of (a) the encryption system; FRT: fractional Fourier transform, RPM: random phase mask, and (b) the decryption system.

phase, in such a way that an amplitude-authorized user can receive the phase encoding but without the appropriate key is unable to read it.

In a recent communication [26], a method of image encryption has been proposed that can encrypt a set of plaintexts into many similar ciphertexts. The phase keys corresponding to different plaintexts are achieved independently from the same designed ciphertext by cascade phase retrieval algorithm. In this paper, we present an optical encryption architecture based on multiplexing, in which users can decrypt different private images from the same encrypted image, a superuser can have a key that decrypts all encrypted images, and multiplexed images can be encrypted with different levels of security. We used a real-world three-dimensional scene, captured with digital holography, and encrypted using the FRT. To the best of our knowledge, this communication represents the first example of a generalized framework of multiplexed-based optical encryption applications, and in addition the first example of using the FRT to encrypt 3D digital holographic objects.

2. Principle

The principle of the multiplexing system is as follows. Several pieces of image data (let us call them image segments, denoted by I) are to be encrypted using different encryption keys. The segments could be different 2D images, different 3D images, or different objects within a 3D scene. They could be overlapping, non-overlapping, completely distinct, or could contain common parts. A schematic for the latter case is shown in Fig. 1(a). Although only three segments are shown, the principle holds for many segments. Each image segment is encrypted with a distinct random phase mask (RPM) placed in a fractional Fourier plane. The RPMs, fractional orders, or both can be distinct for each image segment. In Fig. 1(a), the 3D scene is represented by a complex-valued reconstruction (full Fresnel field) from an optically captured digital hologram. Conveniently, due to the speckle inherent in the digital holograms of macroscopic 3D scenes, the input plane RPM is not needed, but can be included in Fig. 1 in the case of real-valued or non-speckled inputs.

Table 1
Different user cases for the architecture in Fig. 1.

	User 1	User 2	User n
User case	Segment 1	Segment 2	Both segments
(i)	RPM$_1$	RPM$_2$	–
(ii)	RPM$_1$	RPM$_2$	f(RPM$_1$,RPM$_2$,RPM$_u$)
(iii)	RPM$_1$	--	RPM2

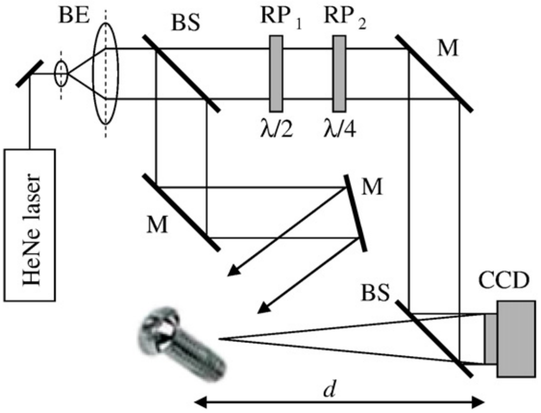

Fig. 2. Optical setup for hologram capture of real-world objects used in these experiments: BE, beam expander; BS, beam splitter; RP, retardation plate; and M, mirror.

The security of an encryption technique depends on the size of the key used. An enlarged key space provides enhanced security. Various techniques [9,11,12] have been proposed to use the additional degrees of freedom offered by an optical system to enlarge the key size. Techniques based on the FRT provide such an example. A two-dimensional FRT, denoted $g_i(\xi_i, \eta_i)$, of the image segment $I_i(x_i, y_i)$, of order ($\alpha_{i1} = a_{i1}\pi/2$) is given by [10]

$$g_i(\xi_i, \eta_i) = K \iint I_i(x_i, y_i) \times \exp\left(j\pi \frac{x_i^2 + y_i^2 + \xi_i^2 + \eta_i^2}{\tan \alpha_{i1}} - 2j\pi \frac{x_i y_i \xi_i \eta_i}{\sin \alpha_{i1}} \right) \mathrm{d}x_i \mathrm{d}y_i. \tag{1}$$

Here (x_i, y_i) and (ξ_i, η_i) represent the space and fractional domain coordinates, respectively, and K is a constant [10]. As shown in Fig. 1(a), the function $g_i(\xi_i, \eta_i)$ is multiplied by a RPM$_i$ defined as RPM$_i = \exp[2\pi j r_i(\xi_i, \eta_i)]$ and undergoes a further FRT of order ($\alpha_{i2} = a_{i2}\pi/2$), giving

$$e_i(\rho_i, \sigma_i) = K \iint \{ g_i(\xi_i, \eta_i) \exp[2\pi j r_i(\xi_i, \eta_i)] \} \times \exp\left(j\pi \frac{\xi_i^2 + \eta_i^2 + \rho_i^2 + \sigma_i^2}{\tan \alpha_{i2}} - 2j\pi \frac{\xi_i \eta_i \rho_i \sigma_i}{\sin \alpha_{i2}} \right) d\xi_i d\eta_i. \tag{2}$$

The function $e_i(\rho_i, \sigma_i)$ is the encrypted function obtained due to I_i. r_i (ξ_i, η_i) is an independent random function uniformly distributed in the interval [0,1). The coordinates (ρ_i, σ_i) refer to the encryption domain

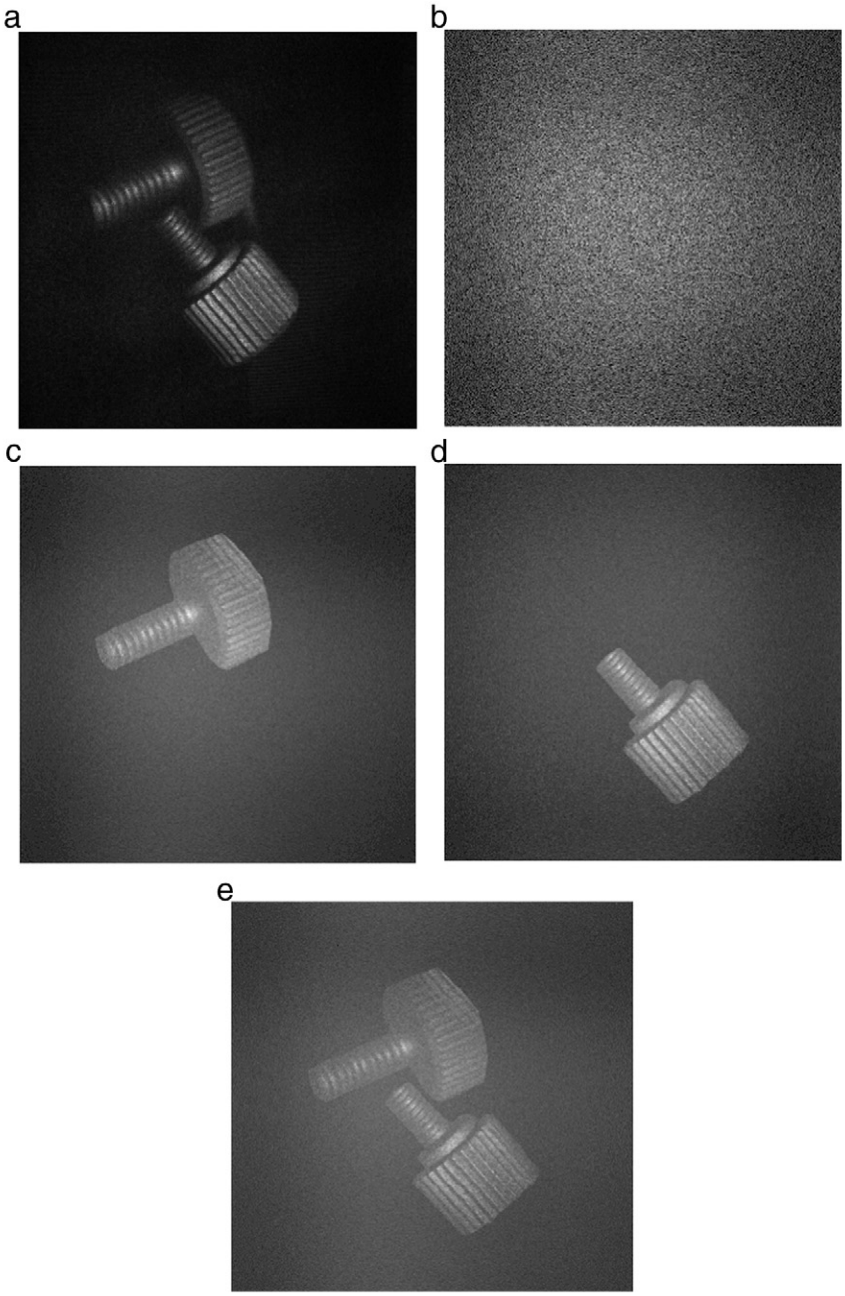

Fig. 3. Simulation results. Intensities of (a) original complex-valued image reconstructed from a digital hologram, (b) multiplexed encrypted image, (c)–(e) decryption using the correct RPM and fractional orders of users 1, 2, and n, respectively.

coordinates. In the encryption plane, all n encrypted functions are multiplexed to generate a single encrypted image

$$e(\rho,\sigma) = \sum_{i=1}^{n} e_i(\rho_i,\sigma_i). \quad (3)$$

The encrypted image $e(\rho,\sigma)$ will be shared among all the users who will access it with different keys. The schematic for decryption is as shown in Fig. 1(b). The decryption is the reverse of the encryption process and is done by using conjugates of the RPMs and inverse FRT. To decrypt the data correctly, one must specify the fractional domains in which the input, the encryption, and the output planes exist. Thus, in addition to the key used for encryption one must specify the orders of the FRTs relating them. A decryption using (RPM$_i$, a_{i1}, and a_{i2}) will decrypt only I_i and all other segments will remain encrypted as a background white noise.

This basic optical architecture can be manipulated to achieve several encryption functionalities, three of which are explained in Table 1. For illustration purposes, we refer to at most three users in each case, but there can be many more. In user case (i), we illustrate the concept of different users decrypting different images from a single encrypted image. To achieve this, as indicated in the first row of Table 1 and referring to Fig. 1, user 1 has RPM$_1$, user 2 has RPM$_2$, and there is no user n in this case. The different RPMs encrypt different image segments that are multiplexed together. It can easily be seen that the two users will decrypt unique images from the encrypted image. In user case (ii), we illustrate the concept of a superuser. User 1 has RPM$_1$, user 2 has RPM$_2$, and user n has RPM$_n$ that can decrypt all encrypted objects. This latter mask could be generated independently or generated as a function of the other phase masks, e.g. RPM$_n = f$ (RPM$_1$,RPM$_2$,RPM$_u$) where RPM$_u$ is known only to the superuser. (RPM$_u$ can be ignored if for one's application the superuser has no more privileges than the basic users combined.) The function f could be an efficient encryption attack algorithm based on simulated annealing [27]. The flexibility inherent in double random phase encoding has been shown previously [28].

In user case (iii), we illustrate the concept of different images being encrypted with different levels of security. User 1 has RPM$_1$ (many users can be given this key), there is no distinct user 2 in this case, and user n has an independent key RPM$_2$ that decrypts what RPM$_1$ decrypts plus some extra image data. The extra image data can be regarded as being encoded with a higher security level because only one decryption key in circulation can decrypt it. The image decrypted with RPM$_1$ can be regarded as being encoded with a lower security level because many users can decrypt it. Although in this example, there are only two users and two levels of security, the number of users and the number of different levels of security can of course be increased. The number of images that can be multiplexed together is bounded due to the noise that each incorrectly decrypted image will contribute to the decryption plane. Various techniques have been proposed to reduce this noise as much as possible [7,29,30] with up to 100 multiplexed digital holograms shown to be possible in some applications with acceptable crosstalk noise [30].

3. Experiment

We verify the proposed framework with a simulation using optically captured data. Our simulation adopts a general scenario of a real-world 3D scene that has been captured by inline phase-shift digital holography [31], rather than a collection of 2D images. Our procedure to capture the 3D scene as shown in Fig. 2 is the same as that described previously [32]. Fractional transforms have been used previously to reconstruct inline holograms [33]. The scene is encrypted so that the different users have access to (can decrypt) different 3D objects in the scene. Fig. 3(a) shows an intensity reconstruction from the 2048×2048 pixel optically captured digital hologram of a real-world 3D scene. The full complex field (not only the intensity) will be input to the encryption scheme. As illustrated in Fig. 1, there will be three users with access to different collections of objects. User 1 will have access to one bolt object, user 2 will have access to a different bolt object, and user n will have access to both objects. The fact that in our example some of the objects are spatially separated, and that there is only two of them, is not important. More objects, and overlapping segments, are possible. Research has commenced on automated segmentation of 3D objects from digital holograms [34].

We randomly generated two random phase masks independent of each other for encrypting the two image segments. We arbitrarily chose two fractional orders to be used with each RPM. An FRT (of order $a_{11} = 0.25$) of I_1 was calculated and multiplied with RPM$_1$, which was again fractional Fourier transformed with order $a_{12} = 0.45$. I_2 was transformed with an FRT of order $a_{21} = 0.65$ and RPM$_2$ was used in the fractional plane. The result was again fractional transformed with order $a_{22} = 0.85$ to get the encrypted image. For the third user, I_3 is the full 3D scene, and was encrypted with FRT orders $a_{n1} = 0.55$ and $a_{n2} = 0.35$ and phase mask RPM$_n$ (= RPM$_1$ + RPM$_2$). Now all the encrypted image segments were multiplexed together to get a single encrypted image, as shown in Fig. 3(b).

The segments I_1, I_2, and I_3 decrypted with correct RPMs and correct fractional orders have been shown in Fig. 3(c)–(e), respectively. User case (i) is verified through Fig. 3(c) and (d), which depicts the different outputs of two users. User case (ii) is verified through Fig. 3 (c)–(e), which depicts outputs of two users and a superuser, respectively. User case (iii) is verified through Fig. 3(c) and (e), which depicts outputs using two different security levels.

4. Conclusion

To summarize, an optical encryption architecture has been presented in which a real-world three-dimensional scene captured with digital holography is encrypted using fractional order Fourier domain random phase encoding, where different users have access to different three-dimensional objects in the scene. Users can decrypt different private images from the same encrypted image, a superuser can have a key that decrypts all encrypted images, and multiplexed images can be encrypted with different levels of security.

Acknowledgement

The authors thank Conor Mc Elhinney for capturing the holograms. Support is acknowledged from the Academy of Finland, Science Foundation Ireland under the National Development Plan, and the European Commission through a Marie Curie Fellowship. The authors' email addresses are nkn@iitp.ac.in and tomn@cs.nuim.ie, respectively.

References

[1] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.
[2] X. Peng, P. Zhang, H. Wei, B. Yu, Opt. Lett. 31 (2006) 1044.
[3] Y. Frauel, A. Castro, T.J. Naughton, B. Javidi, Opt. Express 15 (2007) 10266.
[4] A.M. Youssef, IEEE Signal Process Lett. 15 (2008) 77.
[5] G. Situ, G. Pedrini, W. Osten, Appl. Opt. 49 (2010) 457.
[6] T.J. Naughton, B.M. Hennelly, T. Dowling, J. Opt. Soc. Am. A 25 (2008) 2608.
[7] B.M. Hennelly, T.J. Naughton, J.B. McDonald, J.T. Sheridan, G. Unnikrishnan, D.P. Kelly, B. Javidi, Opt. Lett. 32 (2007) 1060.
[8] P. Réfrégier, B. Javidi, Opt. Lett. 20 (1995) 767.
[9] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. 25 (2000) 887.
[10] H.M. Ozaktas, Z. Zalevsky, M.A. Kutay, The Fractional Fourier Transform with Applications in Optics and Signal Processing, Wiley, Chichester, 2001.
[11] N.K. Nishchal, G. Unnikrishnan, J. Joseph, K. Singh, Opt. Eng. 42 (2003) 3566.
[12] R. Tao, J. Lang, Y. Wang, Opt. Lett. 33 (2008) 581.
[13] M. Joshi, C. Shakher, K. Singh, Opt. Lasers Eng. 46 (2008) 522.
[14] G. Situ, J. Zhang, Opt. Lett. 30 (2005) 1306.
[15] M.Z. He, L.Z. Cai, Q. Liu, X.C. Wang, X.F. Meng, Opt. Commun. 247 (2005) 29.
[16] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 276 (2007) 231.
[17] X. Wang, D. Zhao, F. Jing, X. Wei, Opt. Express 14 (2006) 1476.
[18] W. Jin, C. Yan, Optik 118 (2007) 38.

[19] A. Alfalou, C. Brosseau, Opt. Lett. 35 (2010) 1914.
[20] E. Tajahuerce, B. Javidi, Appl. Opt. 39 (2000) 6594.
[21] S. Kishk, B. Javidi, Opt. Express 11 (2003) 874.
[22] C.H. Yeh, H.T. Chang, H.C. Chien, C.J. Kuo, Appl. Opt. 41 (2002) 6128.
[23] X.F. Meng, L.Z. Cai, Y.R. Wang, X.L. Yang, X.F. Xu, G.Y. Dong, X.X. Shen, H. Zhang, X. C. Cheng, J. Opt. A Pure Appl. Opt. 9 (2007) 1070.
[24] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 281 (2008) 3434.
[25] J.F. Barrera, R. Torroba, Appl. Opt. 48 (2009) 3120.
[26] X. Yong-Liang, Z. Xin, Y. Sheng, C. Yao-Yao, Opt. Commun. 283 (2010) 2789.
[27] U. Gopinathan, D.S. Monaghan, T.J. Naughton, J.T. Sheridan, Opt. Express 14 (2006) 3181.
[28] G. Situ, D.S. Monaghan, T.J. Naughton, J.T. Sheridan, G. Pedrini, W. Osten, Opt. Commun. 281 (2008) 5122.
[29] X.F. Meng, L.Z. Cai, M.Z. He, G.Y. Dong, X.X. Shen, Opt. Commun. 269 (2007) 47.
[30] M. Paturzo, P. Memmolo, L. Miccio, A. Finizio, P. Ferraro, A. Tulino, B. Javidi, Opt. Lett. 33 (2008) 2629.
[31] I. Yamaguchi, T. Zhang, Opt. Lett. 22 (1997) 1268.
[32] T.J. Naughton, Y. Frauel, B. Javidi, E. Tajahuerce, Appl. Opt. 41 (2002) 4124.
[33] Y. Zhang, G. Pedrini, W. Osten, H.J. Tiziani, Opt. Lett. 29 (2004) 1793.
[34] C.P. Mc Elhinney, J.B. Mc Donald, A. Castro, Y. Frauel, B. Javidi, T.J. Naughton, Opt. Lett. 32 (2007) 1229.