A study of the particularities of an authentication system with a method of an asymmetric holographic encryption based on the DRPE to protect the passwords of the technical devices

S S Nalegaev¹ and V V Krasnov²

¹ITMO University, Kronverkskiy pr. 49, 197101 St. Petersburg, Russia
²National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, 115409 Moscow, Russia

E-mail: s.nalegaev@gmail.com

Abstract. The present work is devoted to research the peculiarities of an authentication system of the technical devices with the use of an optical asymmetric holographic encryption on the basis of the Double Random Phase Encoding (DRPE). The series of the numerical experiments was performed to implement the encryption and the decryption of the initial image. The angular spectrum approach was used as a tool for the simulation of the propagation of the light in the free space forward and backward along the whole optical scheme of the DRPE. In the present work the particularities of the authentication system based on an asymmetric approach of the holographic encryption method DRPE were studied.

1. Introduction

The identification and the authentication are a foundation of all the information protection systems, since all the information protection mechanisms are designed to work with the named subjects and objects of the automated system (AS) [1]. The identifiers (IDs) or the usernames is often used as a way of naming of the corresponding subjects and objects of the automated system. In a general sense, the authentication is not intended to establish a correspondence between the entered IDs and subjects of AS which are matched with them, but to authenticate the submitted data [2]. And this is it essential difference from the identification. The authentication systems are often used as an intermediate element that is used to implement an access control to anything between the authorized and the unauthorized subjects. In this case both the users and the processes [1] or the technical devices can act as the subjects of AS. And the information and the other resources of the system [1] including the ability to manage anything can act as the objects of AS.

Such the authentication system can be used, for example, within the concept of the home automation, where it is required to ensure a secure communication of the general system of the monitoring and control with the various technical elements and devices: the temperature and humidity control sensors of the indoor and outdoor air; the detectors of the fire alarm, the water leakage or the short circuit; the sensors used to control the breaking and the entering or the presence of a people in the rooms; for the processing signals from the domestic commercial devices (the electric kettles, the refrigerators, the heating system) or to control such the devices. In all these cases it is necessary to ensure the secure data exchange between this system and all the listed devices, taking into account the
fact that the communication can take place over an insecure communication channel. To accomplish this, it is necessary to bring to the correspondence a set of the unique IDs and the passwords with each of these devices, as well as with the general monitoring and control system to perform the authentication process and to be able to set the interaction privileges among themselves and the general monitoring and control system.

All of these problems can be solved by an authentication system based on the use of some asymmetric optical encryption technique, for example, the asymmetric holographic image encryption based on the method of the Double Random Phase Encoding (DRPE) [3,4]. In the method DRPE, an amplitude object with the spatial distribution of the transmittance usually serves as the source image, and the encryption process is based on the diffraction of the wavefield of the optical radiation transmitted through the object, as it travels along the optical axis [3-5]. In contrast to the methods of the optical encryption in spatially incoherent light (for instance see [6-8]) in the case of DRPE the hologram of the wavefield recorded at the output of the optical system serves as an encrypted image of the object [3-5]. Such the optical encoding system can be performed within an experimental scheme or using a numerical simulation of the light propagation process through the whole optical system, for example, like in these works [9-11].

Theoretically, the information encoded by the method DRPE can be decrypted by the use of the simple brute force attack. In this case the choice of the proper criterion or criteria may play an important role for the estimation of the set of the key parameters of the optical scheme which have been used to obtain the encrypted image [5,12]. On the other hand, because of the multidimensionality of the encryption and decryption process [13], the numerical methods of the breaking DRPE through the direct brute force attack can not be used in the present time due to a high computational complexity of this task [3-5]. But there are several much more efficient approaches of the breaking DRPE based on the iterative techniques [14-21]. Within the frame of this work, we investigated the particularities of an optical authentication system based on the use of an asymmetric method of the optical holographic encryption. Such authentication systems can be used in practice to protect the passwords of the various commercially-rated technical devices within the concept of the home automation.

2. Numerical scheme and results
For the studied asymmetric holographic encryption method the process of the encryption is based on the optical transformations of the initial wavefield at the output plane of the object O with flat spatial distribution of the phase during its propagation along the optical system as it shown in the figure 1. To perform the encryption, the information for which the encryption is required is converted into a two-dimensional image which is used as a two-dimensional spatial distribution of the amplitude of the field in the output plane of the object. This initial amplitude distribution is shown on the figure 2 (a).

![Figure 1](image1.png)  **Figure 1.** The scheme used in the simulation.

![Figure 2](image2.png)  **Figure 2.** The obtained results.
Due to the asymmetry of the encryption method there are two keys one of which (privacy key) includes (without any protection) all the parameters of the optical scheme that are required for the recovery of the encrypted information. For example, these are such parameters as (see the figure 1): propagation distances in free space $l_1$ and $l_2$; spatial phase distribution in the output plane of the second random phase mask RP-2; wavelength $\lambda$. It is interesting to note that there is a possibility to develop many variations of the holographic asymmetric encryption scheme based on the classical scheme DRPE but with some additional key parameters of the optical set-up. For example, it is possible to assume that the properties of the DKDP and the KDP crystals investigated in these works [22, 23] also could be used as the additional parameters. And many of such the variations of this method were developed at the present time already. The private key with all of such the parameters is not intended for the storage or the transmission. The second key (public key) is intended to send it over an insecure communication channel together with the encrypted images. This public key is represented by the digital hologram obtained by the method DRPE from the private key using a set of the key parameters that differs from those used to protect the target images. The pictures (b) and (e) on the figure 2 represents the spatial phase distributions of the wavefield in the object plane: (b) is for initial phase distribution and (e) is for reconstructed one by the decryption of the encrypted hologram (c). The same is for the pictures (a) and (d), which represents the spatial amplitude distributions of the wavefield in the object plane. The hologram (c) (with an enlarged fragment) represents the result of the holographic encryption used to the the initial wavefield with amplitude (a) and phase (b), which is measured in the CCD plane. The figure 1 also includes the following optical elements: LM - laser; BS – beam splitter; M – mirror.

To perform the encryption and the decryption process it is necessary to take into account the diffraction of the light while it propagates through the free space with the distances $l_1$ and $l_2$. And the angular spectrum method [24,25] was used to calculate the results of such the numerical forward (encryption) and backward (decryption) propagation. The reconstruction of the full information about the wavefield in the plane of the CCD (the amplitude and phase distributions) was performed from the hologram (c) according to the method described in [26]. As can be seen from the figure 2, the initial wavefield has a flat spatial phase distribution for the current results of the numerical experiment.

3. Conclusion
The particularities of the authentication system based on an asymmetric approach of the holographic encryption method DRPE were investigated. The encrypting and the decrypting of the images were numerically demonstrated. To take into account the diffraction effects of the light the angular spectrum method was used to calculate the results of the numerical propagation of the wavefield in free space. The use of the some asymmetric variations of the known holographic encryption methods DRPE for the developing new authentication systems is of interest because of the several points of view. For example, a multidimensionality of the process of the encryption and the decryption leads to a high degree of the information security. And the use of the asymmetric algorithms reduce the requirements to the data channel allowing the use of the common unsecured communication channels.

Acknowledgments
S S Nalegaev acknowledge a financial support from the grant of the Russian foundation for basic research (the agreement No 16-52-52049\16 from 29.01.2016).

References
[1] Gladkih A A and Dementiev V E 2009 The basic principles of information security of computing networks (Ulyanovsk: Ulyanovsk state technical university) 156 p
[2] Merkle R C 1979 Secrecy, authentication, and public key systems (Stanford: Stanford university) 182 p
[3] Refregier P and Javidi B 1995 Opt Lett 20 767-769
[4] Chen W, Javidi B and Chen X 2014 Adv Opt Photon 6 120-155
[5] Nalegaev S S and Petrov N V 2015 *Physics Procedia* **73** 281-286
[6] Krasnov V V, Starikov S N, Starikov R S and Cheremkhin P A 2016 *Russian Physics Journal* **58** 1394-1401
[7] Evtikhiev N N, Starikov S N, Cheryomkhin P A, Krasnov V V and Rodin V G 2012 *Proceedings of SPIE* **8429** 84291P
[8] Bondareva A P, Cheremkhin P A, Evtikhiev N N, Krasnov V V and Starikov S N 2015 *Physics Procedia* **73** 320-327
[9] Nalegaev S S and Petrov N V 2015 *Russian Journal of Physical Chemistry B* **9** 555-557
[10] Nalegaev S S, Petrov N V and Bespalov V G 2014 *Journal of Physics: Conference Series* **536** 012025
[11] Nalegaev S S, Petrov N V and Bespalov V G 2014 *Fringe 2013: 7th Int. Workshop on Advanced Optical Imaging and Metrology* ed W Osten (Berlin, Heidelberg: Springer-Verlag) 321-324
[12] Nalegaev S S and Petrov N V *Russian Physics Journal* **58** 128-131
[13] Barrera J F, Mira A and Torroba R 2013 *Opt Express* **21** 5373
[14] Carnicer A, Montes-Usategui M, Arcos S and Juvelles I 2005 *Opt Lett* **30** 1644-1646
[15] Peng X, Wei H Z and Zhang P 2006 *Opt Lett* **31** 1044-1046
[16] Peng X, Tang H Q and Tian J D 2007 *Acta Physica Sinica* **56** 2629-2636
[17] Peng X, Zhang P, Wei H Z and Yu B 2006 *Opt Lett* **31** 3261-3263
[18] Frauel Y, Castro A, Naughton T J and Javidi B 2007 *Opt Express* **15** 10253-10265
[19] Qin W, He W, Meng X and Peng X 2009 *Proc of SPIE* **7512** 751203
[20] Qin W and Peng X 2009 *J Opt A: Pure Appl Opt* **11**
[21] Nalegaev S S, Petrov N V and Bespalov V G 2012 *Scientific and Technical Journal of Information Technologies, Mechanics and Optics* **82** 30-35
[22] Nalegaev S S, Putilin S E and Bespalov V G 2012 *Scientific and Technical Journal of Information Technologies, Mechanics and Optics* **81** 29-35
[23] Nalegaev S S, Putilin S E and Bespalov V G 2013 *Proc SPIE* **8699** 869914
[24] Goodman J W 2005 *Introduction to Fourier Optics* (Englewood: Roberts & Company) 491 p
[25] Poon T C and Banerjee P P 2001 *Contemporary Optical Image Processing with MATLAB* (Elsevier Science & Technology) 262 p
[26] Liebling M, Blu T and Unser M 2004 *J Opt Soc Am* **A21** 367–77