Conference Paper

Method of Asymmetric Optical Encryption of Images Using Spatially Incoherent Illumination

N.N. EVTIKHIEV, V.V. KRASNOV, and A.V. SHIFRINA

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

The method of asymmetric encryption of images based on the double optical encryption with spatially incoherent illumination is presented. Numerical simulations of the presented method in various modifications are carried out and their efficiency is estimated. The modification providing the best balance between maintaining the advantages peculiar to the optical encryption and quality of the decoded images is chosen. In this case the value of the normalized standard deviation (NSTD) of the decoded image from original one for asymmetric encryption differs no more than by 8% from NSTD of standard optical encryption with spatially incoherent illumination.

Corresponding Author:
V.V. Krasnov
VVKrasnov@mephi.ru

Received: 28 January 2018
Accepted: 15 March 2018
Published: 25 April 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the PhIO Conference Committee.

1. Introduction

Information security methods are actively investigated at present time. One of such methods is optical encryption [1]–[9]. In comparison with more widespread digital encryption, it has a number of advantages: high speed, parallelism, an ability to encrypt data directly in the course of its registration, and also the lack of the accompanying emission in radio frequency range. Optical encryption can be used for encrypting monochrome and color images [8] or digital information [3], including QR codes [9].

The most widespread method of optical encryption is optical encryption with coherent monochromatic illumination with use of two random phase masks [1], [2], [7]. This method allows to receive encrypted image with "white" spectrum which provides high degree of concealment. "White" spectrum has no special features which makes a task of decoding for illegitimate user more complicate.

Optical encryption can be mathematically described as operation of convolution of the image to-be-encrypted with the encryption key. For decoding of the received encrypted image it is necessary to use inverse filter based on the encryption key.

How to cite this article: N.N. EVTIKHIEV, V.V. KRASNOV, and A.V. SHIFRINA, (2018), "Method of Asymmetric Optical Encryption of Images Using Spatially Incoherent Illumination" in *VII International Conference on Photonics and Information Optics*, KnE Energy & Physics, pages 498–508. DOI 10.18502/ken.v3i3.2064

Thus, according to cryptography this method of encryption is a symmetric one [10], i.e. the same key is applied to encryption and decryption.

The modification of the double random phase encoding technique allowing to create asymmetric system of encryption has been developed [11]. The idea of division of the encrypted image into amplitude and phase components lies in its basis. Phase component is used as an open encryption key. Unlike the symmetric encryption, in the asymmetric encryption it is not necessary to exchange the encryption key between sender and recipient.

However the double random phase encoding technique possesses the considerable drawback in the form of a necessity to register both amplitude and phase of the encrypted image — i.e. it is necessary to use the holographic setup for registration. It considerably complicates the hardware implementation of this system. It is also necessary to use completely coherent illumination. It leads to appearance of the speckle noise in encrypted image, which leads to bad decryption quality [12].

Application of spatially incoherent illumination instead of completely coherent one allows to eliminate these drawbacks [4]. In this case the phase component of the encrypted image does not contain useful information and it is not necessary to register it. It allows to use photosensors as the registering devices. In this case only light intensity distribution represents the encrypted image. The basic scheme of optical encryption using monochromatic spatially incoherent illumination illustrated in fig. 1. In this scheme the diffractive optical element (DOE) such as kinoform forms an encryption key.

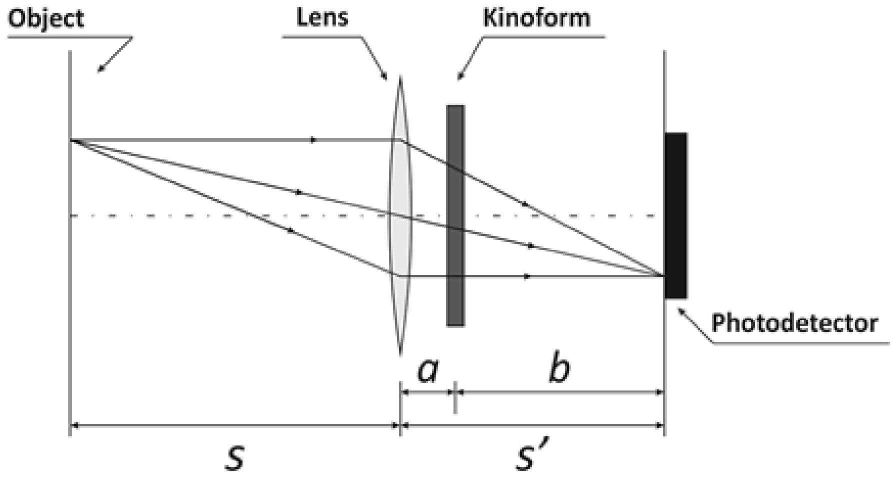

Figure 1: The basic scheme of optical image encryption using monochromatic spatially incoherent illumination.

Unlike optical encryption with completely coherent illumination, this scheme does not suffer from speckle noise and it is much simpler for hardware implementation.

However the absence of the useful phase component of encrypted image leads to the impossibility to create the system of asymmetric encryption using the same principles as for the double random phase encoding technique.

Thus it is proposed to use the scheme with double consecutive encryption of the image with consecutive decoding both by the sender and the recipient to create the system of asymmetric optical encryption with spatially incoherent illumination.

2. Description of optical encryption with spatially incoherent illumination and encrypted images numerical decryption

The mathematical description of basic optical encryption with spatially incoherent illumination can be described as follows:

Using model of the additive noise dominating over other types of noise [13], process of optical encryption can be approximately described by the equation:

$$g(i,j) = f(i,j) \otimes h(i,j) + n(i,j), \tag{1}$$

where g — encrypted image, f — image to-be-encrypted, h — point spread function (PSF) of DOE, n — additive noise, i, j — indexes corresponding to image pixels coordinates.

Fourier spectrum of an encrypted image G might be written as:

$$G(u,v) = F(u,v) \cdot H(u,v) + N(u,v), \tag{2}$$

where G, F, H and N are Fourier spectra of g, f, h and n accordingly; u, v – indexes corresponding to coordinates in Fourier domain. If there is no noise (N(u,v)=0) and no zeros in H(u,v), Fourier spectrum F′ of an decoded image f′ might be found as:

$$F^{'}(u,v) = \frac{G(u,v)}{H(u,v)} = G(u,v) \cdot Y(u,v), \tag{3}$$

where Y(u,v)=1/H(u,v) – inverse decryption filter. However if there is noise present (and it always present in real systems), then inverse filter 1/H(u,v) will not work properly. To make it work additional stabilization is required.

Inverse filter with Tikhonov regularization [14] was utilized in this paper. The maximum value of PSF power spectrum was used in capacity of smoothing function:

$$Y(u,v,\alpha) = \frac{H(u,v)}{H(u,v)^2 + \alpha \cdot \max(H(u,v)^2)}, \tag{4}$$

where α is a regularization parameter.

3. Asymmetrical optical encryption with spatially incoherent illumination

As shown in the equation 1, the mathematical operation of convolution is the base of optical encryption. In this paper it is important that convolution has the property of commutativity:

$$h(i,j) \otimes f(i,j) = f(i,j) \otimes h(i,j) \quad (5)$$

Thanks to it the scheme of asymmetric encryption based on the double optical encryption, showed in fig. 2 can be created.

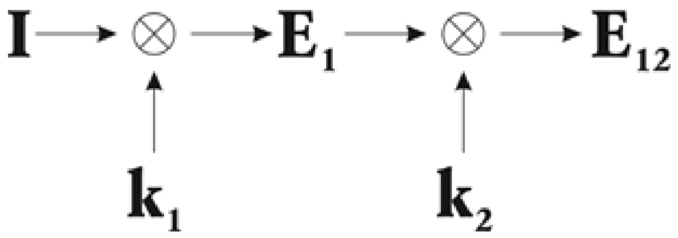

Figure 2: Data encryption in the scheme of asymmetric encryption based on the double optical encryption.

In this case encryption of the image is carried out as follows:

1. The sender encrypts the base image **I** with their encryption key $\mathbf{k}_1$ and sends the encrypted image $\mathbf{E}_1$ to the recipient.
2. The recipient encrypts the received encrypted image $\mathbf{E}_1$ with their encryption key $\mathbf{k}_2$ and returns twice encrypted image $\mathbf{E}_{12}$ to the sender.

The commutativity of convolution operation provides a possibility to decode the encrypted image $\mathbf{E}_{12}$ backwards in comparison with encryption.

The scheme of decoding is shown in fig. 3.

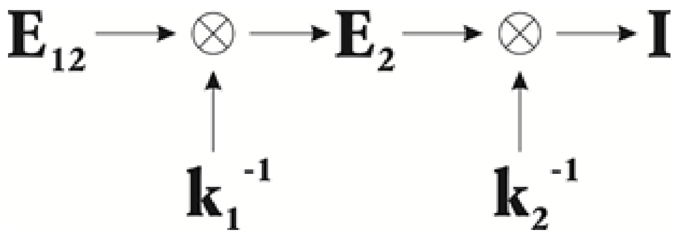

Figure 3: Data decoding in the scheme of asymmetric encryption based on the double optical encryption.

Decoding of image is carried out as follows:

1. The sender decodes twice encrypted image $\mathbf{E}_{12}$ using the inverse filter $\mathbf{k}_1^{-1}$ based on the encryption key $\mathbf{k}_1$ and sends the encrypted image $\mathbf{E}_2$ to the recipient.

2. The recipient decodes the encrypted image $\mathbf{E}_2$ using the inverse filter $\mathbf{k}_2{}^{-1}$ based on the encryption key $\mathbf{k}_2$ and receives the base image **I**.

Thus, only the encrypted images $\mathbf{E}_1$, $\mathbf{E}_{12}$ and $\mathbf{E}_2$, but not keys $\mathbf{k}_1$ and $\mathbf{k}_2$ are transferred via unprotected communication channels.

It is worth noting that both operations of encryption (sections 1 and 2) can be implemented by hardware (optically) or numerically. Therefore, four modifications of this scheme are possible:

I. Both operations are implemented numerically. This option is not of a particular interest as in case of numerical implementation (i.e. emulation on a computer) all advantages of optical implementation are lost: high-speed performance, parallelism, a possibility to encrypt data directly in the course of its registration.

II. Both operations are implemented optically. In this case advantages remain, however because of accumulation of noise, the quality of the decoded image considerably decreases [15]. Also this modification requires presence of equipment for the optical encryption both at the sender, and at the recipient.

III. The first operation is implemented optically, the second — numerically. This modification has optimum balance between maintaining advantages of optical encryption and quality of the decoded image. Only properties of the first encryption key $\mathbf{k}_1$ will impact the value of the normalized standard deviation of the decoded image from encrypted (NSTD) [15] while the second key $\mathbf{k}_2$can be chosen almost arbitrarily.

VI. The first operation is implemented numerically, the second — optically. Being similar to modification 3, this modification has no possibility to encrypt data directly in the course of its registration and also requires presence of equipment for the optical encryption at the recipient.

Modifications 2 (higher speed and NSTD) and 3 (lower speed and NSTD) are of the practical interest. In section 4 of this article numerical simulation of them is carried out and their efficiency is estimated.

4. Results of numerical simulation

The image with 512x512 elements and a set of 5 encryption keys of different robustness with 128x128 elements were used for carrying out numerical simulation for estimation of efficiency of asymmetric optical encryption with spatially incoherent illumination.

The robustness of keys was evaluated by the normalized on the number of elements ratio of amplitude at zero frequency to average spectrum amplitude (NRZA).

Zero frequency peaks emerge due to registration of only intensity of light distributions and considerably impact quality of the decoded images. The multiplication of spectrum of image to-be-encrypted and encryption key occurs in the process of the optical encryption. As a result the spectrum components of the encrypted image which contain information about the base image are lower than those in a spectrum of the base image. Besides, existence of a maximum in zero spatial frequency noticeably reduces encrypted image concealment.

The NRZA is directly connected to normalized average energy (NAE) of an encryption key (fig. 4) — the ratio of matrix mean value to its maximum value, i.e. key's density.

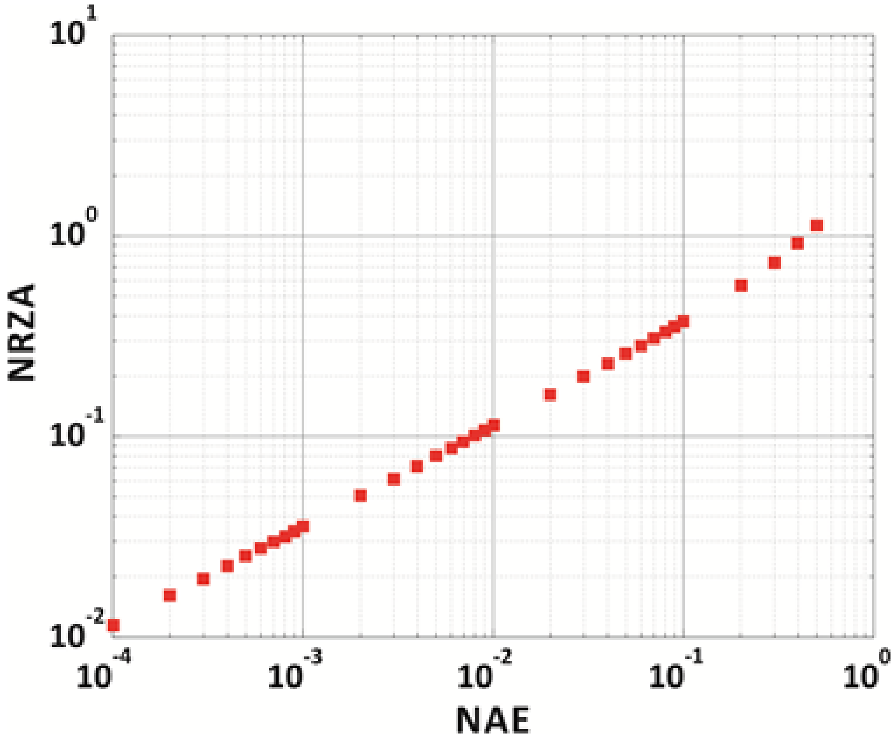

Figure 4: The dependency of encryption key NRZA on its NAE value.

NRZA values of the used keys lay in the range from 0.04 to 0.29 which close to the optimum balance between robustness and NSTD of the decoded image from the original one for basic optical encryption with spatially incoherent illumination [16]. The noise characteristics of the scientific digital camera MegaPlus II ES11000 measured in [17], [18] were used in simulation.

Dependences of NSTD on the second encryption key $\mathbf{k}_2$ NRZA values for various NRZA values of the first encryption key $\mathbf{k}_1$ are presented In fig. 5 in case when both operations of encryption are implemented optically (modification 2 from section 3).

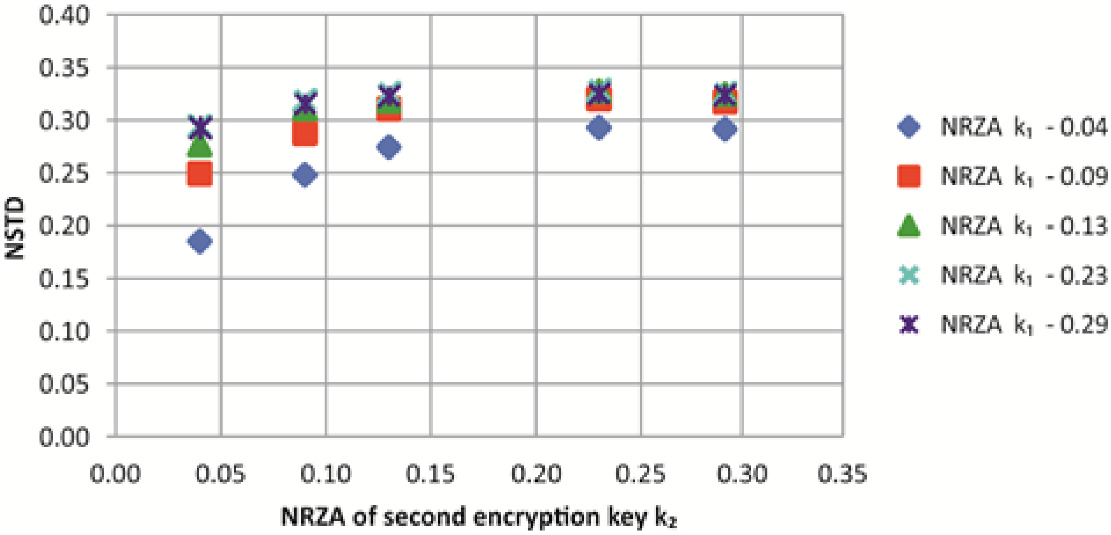

Figure 5: Dependences of NSTD on the second encryption key $\mathbf{k}_2$ NRZA values for various NRZA values of the first encryption key $\mathbf{k}_1$ in case when both operations of encryption are implemented optically.

Results of numerical simulation have confirmed high NSTD for this modification. Almost for all combinations of encryption keys NRZA NSTD does not fall below 0.25 which corresponds to the high noise pollution of the decoded image.

Dependences of NSTD on the second encryption key $\mathbf{k}_2$ NRZA values for various NRZA values of the first encryption key $\mathbf{k}_1$ are presented In fig. 6 in case when first operation of encryption is implemented optically and second – numerically (modification 3 from section 3).

In this case the second encryption key $\mathbf{k}_2$ has almost no impact on NSTD, and NSTD has approximately the same values as for basic optical encryption with spatially incoherent illumination.

Examples of image to-be-encrypted, encrypted, and decoded images and encryption keys for modification when the first operation of encryption implemented optically, and the second – numerically are presented in fig. 7.

The first encryption key NRZA value equals 0.09, the second encryption key NRZA value – 0.13, the decoded image NSTD – 0.12.

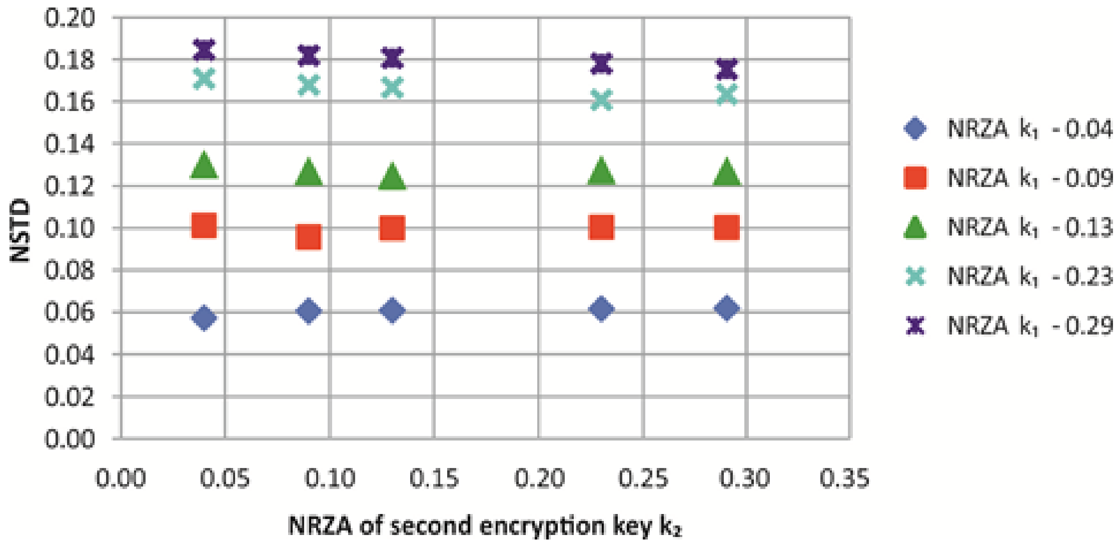

Figure 6: Dependences of NSTD on the second encryption key $\mathbf{k}_2$ NRZA values for various NRZA values of the first encryption key $\mathbf{k}_1$ in case when first operation of encryption is implemented optically and second — numerically.

5. Conclusion

Results of numerical simulation have confirmed efficiency of the proposed method of asymmetric optical encryption of images with spatially incoherent illumination.

The modification of the method in which the first operation of encryption is implemented optically and the second — numerically is most perspective for further researches. In this case the normalized standard deviation of the decoded image from original one (NSTD) differs no more than by 8% from NSTD obtained using standard optical encryption with spatially incoherent illumination. For the same modification when encryption keys with optimal parameters are used NSTD lie in the range from 0.05 to 0.13.

It is worth noting that the presented scheme of asymmetrical encryption is vulnerable to the cryptography attacks of the 'Man in the middle'-type. For elimination of this vulnerability authentication of users (the sender and the recipient) can be added to the scheme, however such research is beyond the scope of this paper.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, no. 7, p. 767, 1995.

[2] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain.," Opt. Lett., vol. 25, no. 12, pp.

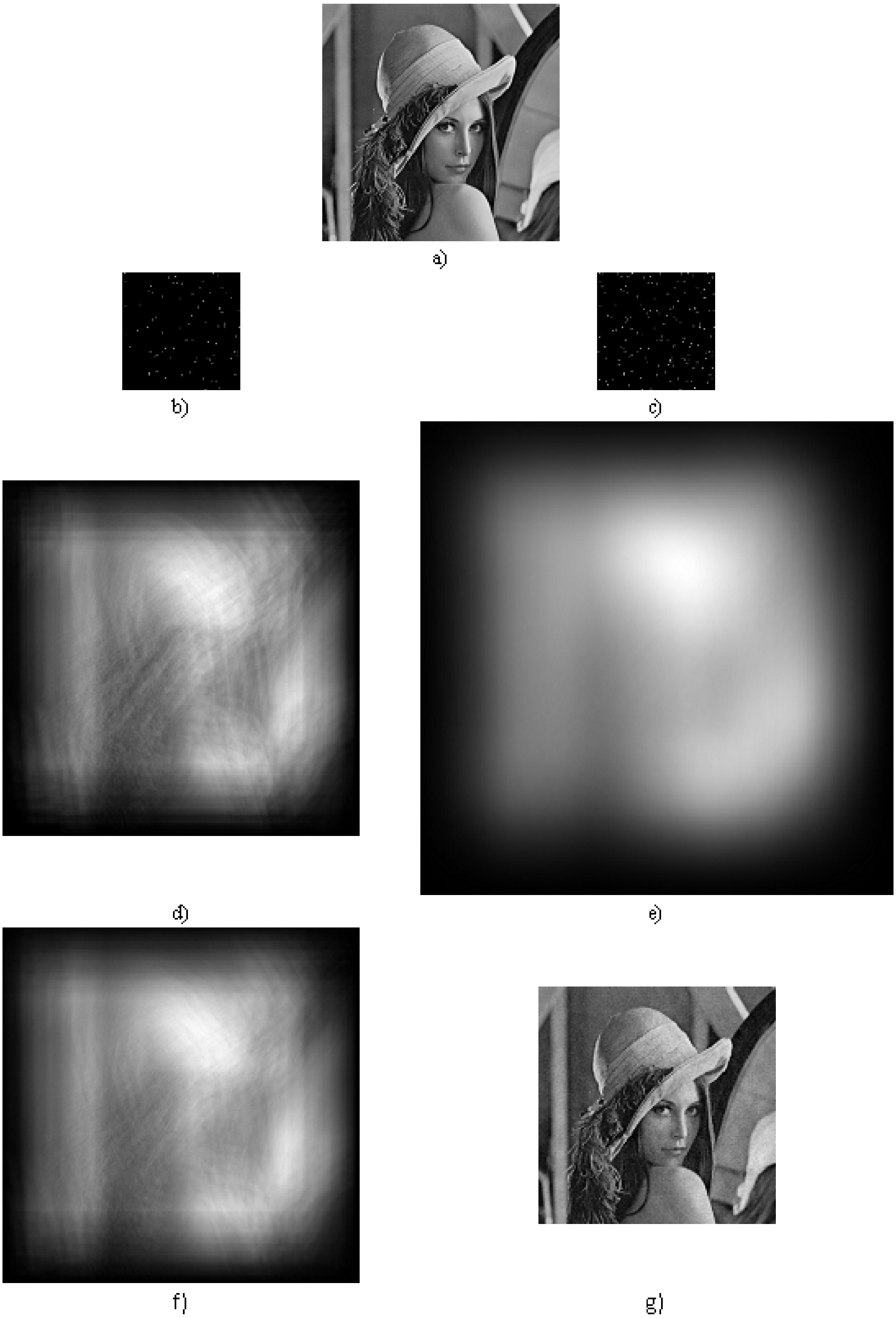

Figure 7: Image to be encrypted (a), encryption keys (b, c), once (d) and twice (e) encrypted and once (f) and twice decoded (g) images for modification when the first operation of encryption implemented optically, and the second — numerically.

887–889, 2000.

[3] V. V. Krasnov, S. N. Starikov, R. S. Starikov, and P. A. Cheremkhin, “Optical Encryption of Arrays of Binary Digits in Spatially Incoherent Light,” Russ. Phys. J., vol. 58, no. 10, pp. 1394–1401, 2016.

[4] N. N. Evtikhiev, S. N. Starikov, P. A. Cheryomkhin, V. V. Krasnov, and V. G. Rodin, “<title>Method of optical image coding by time integration</title>,” Proc. SPIE - Int. Soc. Opt. Eng., vol. 8429, p. 84291P–84291P–9, 2012.

[5] W. T. Cathey and E. R. Dowski, “New paradigm for imaging systems,” Appl. Opt., vol. 41, no. 29, p. 6080, 2002.

[6] P. A. Cheremkhin, N. N. Evtikhiev, V. V. Krasnov, V. G. Rodin, and S. N. Starikov, “Generation of keys for image optical encryption in spatially incoherent light aimed at reduction of image decryption error,” in Proceedings of SPIE - The International Society for Optical Engineering, 2014, vol. 9131, p. 913125.

[7] J. Li, J. Li, L. Shen, Y. Pan, and R. Li, “Optical image encryption and hiding based on a modified Mach-Zehnder interferometer,” Opt. Express, vol. 22, no. 4, p. 4849, 2014.

[8] Z. Liu, J. Dai, X. Sun, and S. Liu, “Color image encryption by using the rotation of color vector in Hartley transform domains,” Opt. Lasers Eng., vol. 48, no. 7–8, pp. 800–805, 2010.

[9] J. F. Barrera, A. Mira, and R. Torroba, “Optical encryption and QR codes: secure and noise-free information retrieval.,” Opt. Express, vol. 21, no. 5, pp. 5373–8, 2013.

[10] H. Delfs and H. Knebl, Introduction to cryptography : principles and applications. Springer, 2007.

[11] W. Qin and X. Peng, “Asymmetric cryptosystem based on phase-truncated Fourier transforms.,” Opt. Lett., vol. 35, no. 2, pp. 118–20, Jan. 2010.

[12] P. A. Cheremkhin, V. V. Krasnov, V. G. Rodin, and R. S. Starikov, “QR code optical encryption using spatially incoherent illumination,” Laser Phys. Lett., vol. 14, no. 2, 2017.

[13] J. R. Janesick, Scientific charge-coupled devices. SPIE Press, 2001.

[14] V. Arsenin and A. Tikhonov, Methods for solving of incorrect problems [In Russian]. Moscow: “Nauka” Publisher, 1979.

[15] A. V. Shifrina, N. N. Evtikhiev, and V. V. Krasnov, “Application of input amplitude masks in scheme of optical image encryption with spatially-incoherent illumination,” J. Phys. Conf. Ser., vol. 737, no. 1, 2016.

[16] N. Evtikhiev, V. Krasnov, P. Cheremkhin, and A. Shifrina, “Application of additional input amplitude masks in schemes of optical image encryption with spatially incoherent illumination,” Comput. Opt., vol. 41, pp. 391–398, 2017.

[17] P. Cheremkhin, N. Evtikhiev, V. Krasnov, V. Rodin, and S. Starikov, “Modified temporal noise measurement method with automatic segmentation of nonuniform target, its accuracy estimation, and application to cameras of different types,” Opt. Eng., vol. 53, p. 102107, 2014.

[18] N. N. Evtikhiev, S. N. Starikov, P. A. Cheryomkhin, and V. V. Krasnov, “Measurement of noises and modulation transfer function of cameras used in optical-digital correlators,” in Intelligent Robots and Computer Vision XXIX: Algorithms and Techniques, 2012, vol. 8301, p. 830113.