# Application of input amplitude masks in scheme of optical image encryption with spatially-incoherent illumination

**A V Shifrina, N N Evtikhiev, V V Krasnov**

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

E-mail: vitaly.krasnov@mail.ru

**Abstract.** Optical encryption with spatially incoherent illumination does not have drawbacks of coherent encryption techniques. In this case however, one of the factors affecting decrypted image quality is original image spectrum. In most cases, majority of image energy is concentrated in area of low spatial frequencies. Therefore, only this area in spectrum of encrypted image contains information about original image, while other areas contain only noise. Additional amplitude encoding of input scene can be used for increase of the size of the area of spatial frequencies containing useful information. Numerical simulation demonstrates reduction of decryption error up to 2.7 times.

## 1. Introduction

Majority of optical encryption techniques operate not only with light intensity, but also with its phase, thus requiring coherent illumination. Original method from whom many varieties were created is double random phase encoding technique [1–6]. Its best feature is transformation of spectrum of image to be encrypted into white spectrum with random phase mask, also, encryption key, which is point spread function (PSF) of second random phase mask, has also white spectrum, consequently encrypted image also has white spectrum. This ensures best security with given number of elements and phase levels a random phase mask. Unfortunately, there are also serious disadvantages in form of holographic setup to register not only light intensity distribution, but also its phase and speckle noise coming with coherent illumination. These factors results in bad decryption quality in optical implementations.

Elimination of these disadvantages is possible via usage of incoherent illumination instead of coherent one. In this case, phase registration is not required and speckle noise is gone. Basic principle of this approach is illustrated in Figure 1. Object is illuminated with spatially-incoherent monochromatic light. In the absence of diffractive optical element (DOE), lens forms object image on photosensor. DOE acts as an encryption element, its PSF is an encryption key. Light passing through DOE forms convolution of object image and DOE PSF in photosensor plane. This convolution is encrypted image.

This technique is simpler in experimental implementation and does not suffer from speckle, but it has its own weaknesses. Major one is it operates only with positive real numbers and not complex ones, which is the case with coherent techniques. This leads to two drawbacks. First, mean value of image to be encrypted is always above zero which leads to intensive zero spatial frequency peak in image spectrum. Second, in DRPE based techniques first random mask transforms spectrum of any

Published under licence by IOP Publishing Ltd

image into white one, here we have no control over image spectrum. Because encryption is based on convolution Fourier spectrum amplitude distribution of encryption key should overlap Fourier spectrum amplitude distribution of image to be encrypted, in other case some spatial frequencies will be lost among with information they carried. Moreover, correct decryption of every spatial frequency is possible only if key spectrum do not have values below noise level. Additionally, heights of zero frequency peaks is defined by average energies of image and key. Because encrypted image contains noise, ratio of its average spectrum energy to noise average energy defines signal to noise ratio of decrypted image. In other words if image contains more white than others, then after encryption-decryption it will contain more noise compared to others. Also, ratio of amplitude at zero frequency to average spectrum amplitude of encryption key impacts decrypted images quality [7].

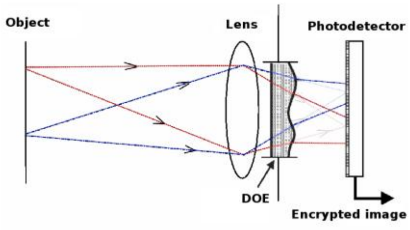


**Figure 1.** Example of basic scheme of optical image encryption using monochromatic spatially incoherent illumination

Phase masks cannot be used in case of spatially incoherent illumination, but amplitude ones can. Additional amplitude encoding of input scene can be used for increase of the size of the area of spatial frequencies containing useful information. This allows to increase signal-to-noise ratio in encrypted image and, therefore, leads to better quality of decrypted images.

Therefore, purpose of this paper is application of additional encoding of input scene and analysis of its effects on decryption quality and encryption strength of encrypted image for optical encryption with spatially-incoherent illumination technique.

Rest of the paper organized as follows. In Section 2 description of applied methods of input scene encoding is given. In Section 3 results of numerical simulation of optical encryption with spatially incoherent illumination and input scene additional encoding are presented. Main results are given in Conclusion.

## 2. Methods of Additional encoding of input scene

Input scene encoding is accomplished by overlaying image to be encrypted with amplitude mask.

Two different types of amplitude masks were used. First one is rectangular grating mask (RGM). This mask increases area of spatial frequencies containing useful information by duplicating original image spectrum in high spatial frequencies corresponding to RGM frequency. Test image before and after application of RGM is shown in figure 2.

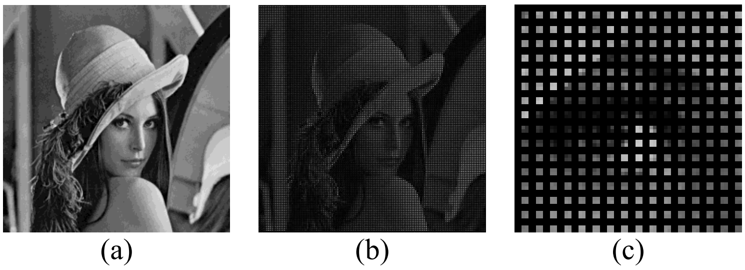


**Figure 2.** Test image before (a) and after (b) application of RGM, magnified fragment of encoded test image (c)

Second one is random mask (RM). Unlike RGM, RM has white spectrum (excluding zero spatial frequency). Two encryption-decryption procedures were applied with two inverse RM, and then resulting encrypted images were subtracted. This is equivalent to application of random binary phase mask. Resulting encrypted image has basically white spectrum. RM mask can be used for increased security. Example of random mask fragment is shown in figure 3a. Fragment of test image before and after application of RM is shown in figure 3b and figure 3c. Encoded images for both AM are shown in figure 4.

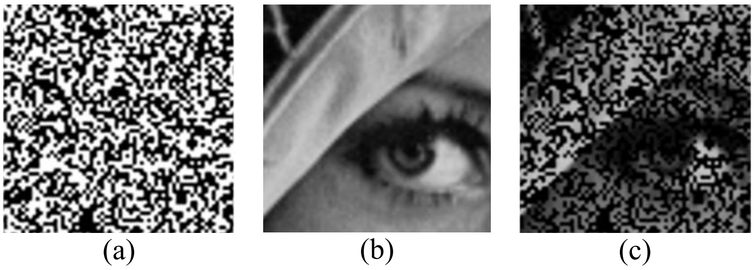


**Figure 3.** Random mask (a), fragments of test image before (b) and after (c) application of random mask

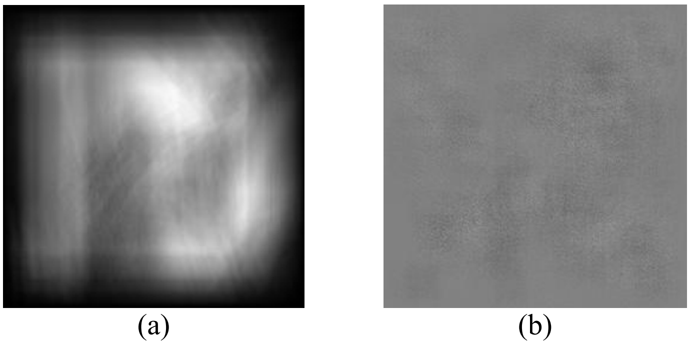


**Figure 4.** Images encoded using RGM (a) and RM (b)

Encryption strength for RGM (figure 4a) is much lower then for RM (figure 4b). Some fragments of original image can be recognized in first case. It should be noted that improvement provided by AM requires registration of 4 frames in case of RGM and 2 frames in cases of RM (instead of 1 frame originally).

## 3. Results of numerical simulation of optical encryption with input scene additional amplitude encoding

The set of 160 random encryption keys with RZA values varying in range 1.6÷191.5 were used in experiments. They had 128×128 elements each with normalized average energy (NAE) ranging from 0.0001 to 0.5. Ten test images (for example see figure 2a) had 512×512 elements. Noises of scientific camera Megaplus ES II 11000 with high maximum linear signal-to-noise ratio (SNR) equal to 141 were simulated.

Numerical simulation is described as follows. First, input scene is encoded with AM, then convolution with encryption key is calculated. Then, simulated camera noises are added. Measured cameras noise characteristics were taken from [8,9]. Then, decryption process takes place. Inverse filter with Tikhonov regularization [10] was used for decryption. After decryption, AM effects are compensated and normalized standard deviations (NSTD) [11] between decrypted and original image is calculated.

Results of encryption-decryption procedure without additional input AM are shown in figure 5. It is clear that encryption keys with low RZA values provide high SNR in the decrypted image.

Results of application of additional input AM are shown in figure 6. Figure 6a corresponds to RGM, figure 6b corresponds to RM and figure 6c corresponds to joint application of RGM and RM in order to increase SNR and encryption strength at the same time.

Application of RGM provides greatest NSTD decrease up to 2.3 times at cost of 4 frames instead of one. Application of RM provides lower NSTD decrease up to 1.6 times at cost of 2 frames instead. Joined application of RGM and RM reduce decrease to 1.9 times at cost of 8 frames.

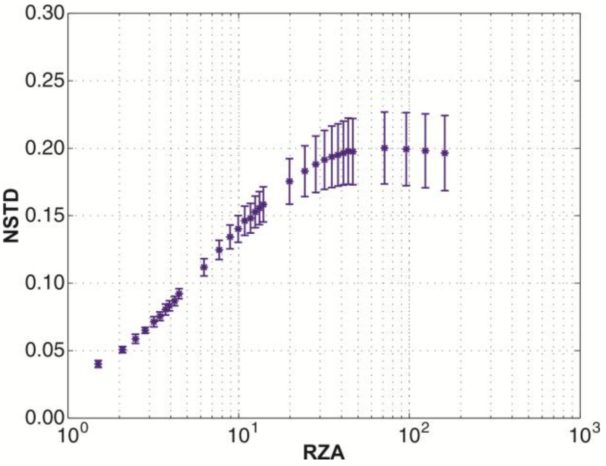
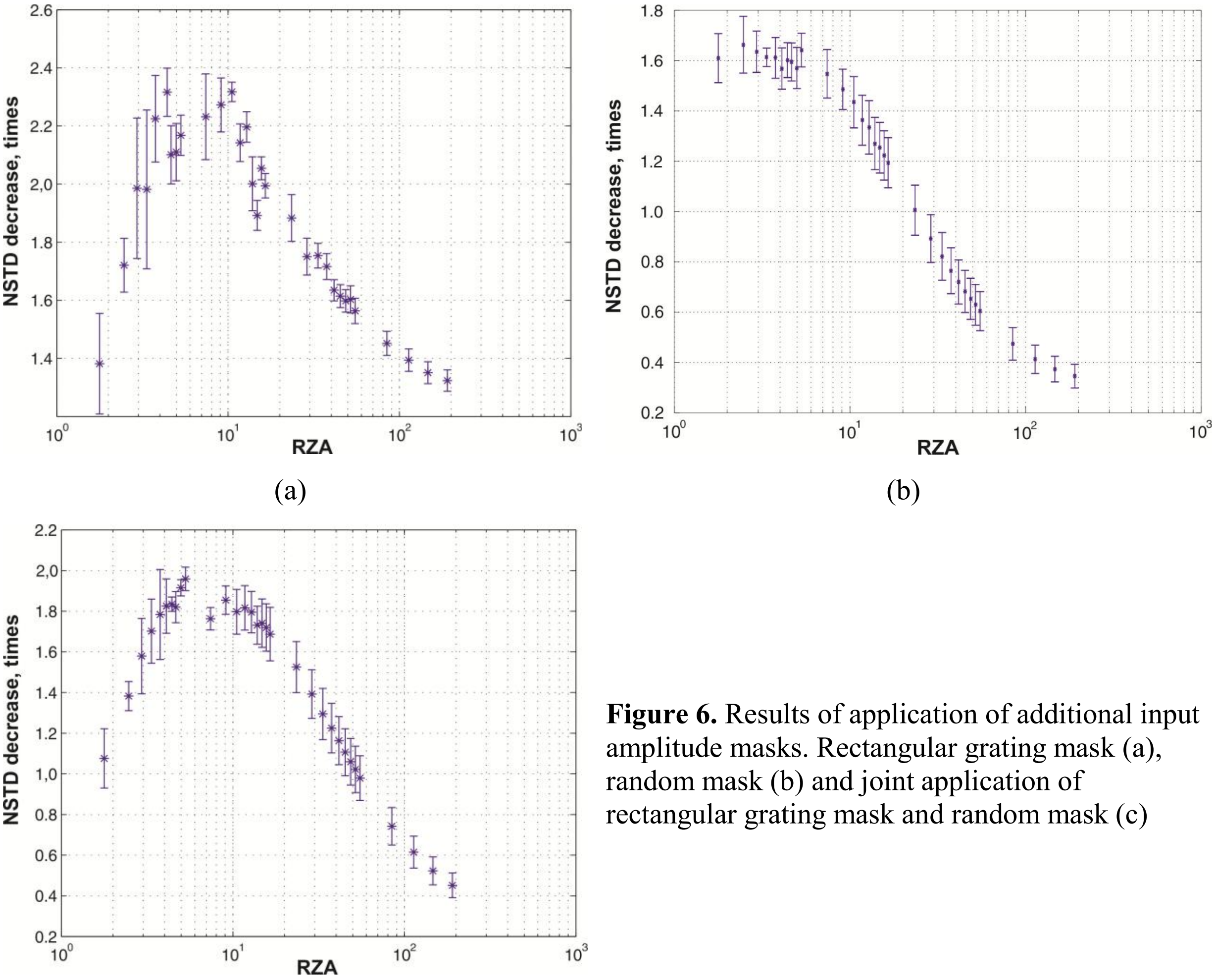


**Figure 5.** Results of encryption-decryption procedure without additional input amplitude masks



(a)

(b)

(c)

**Figure 6.** Results of application of additional input amplitude masks. Rectangular grating mask (a), random mask (b) and joint application of rectangular grating mask and random mask (c)

While keys with low RZA values provide highest NSTD decrease for each AM, encryption strength of such keys is too weak. But joint application of RGM and RM allows encryption with low-RZA (in range 3.0÷20.0) keys: decrease in encryption strength compensates by usage of RM and at the same time it keeps high NSTD decrease.

## 4. Conclusion

Input scene additional amplitude encoding provides significant reduction of decryption error. Rectangular grating mask provides greatest decryption error decrease up to 2.3 times at cost of 4 frames instead of one. With additional application of random mask decryption error decreases up to 1.9 times at cost of 8 frames, but encoded image has higher encryption strength than image encrypted with only rectangular grating mask or no additional mask at all.

**Acknowledgments**

This work was partially supported by grant 14-19-01751 from the Russian Science Foundation (RSF).

## 5. References

[1] Refregier P, and B Javidi 1995 *Opt. Lett.* **20** p 767.
[2] Javidi B, Sergent Arnaud, Z Guanshen, and L Guibert 1997 *Opt. Eng.* **36** p 992.
[3] Unnikrishnan G, J Joseph, and K Singh 2000 *Opt. Lett.* **25** p 887.
[4] Javidi B, N Towghi, N Maghzi, and S C Verrall 2000 *Appl. Opt.* **39** p 4117.
[5] Hennelly B M, and J T Sheridan 2004 *Opt. Eng.* **43** p 2239.
[6] Rajput S K, and N K Nishchal 2014 *Appl. Opt.* **53** p 418.
[7] Cheremkhin P A, N N Evtikhiev, V V. Krasnov, V G Rodin, and S N Starikov 2014 *Proc. SPIE.* **9131** p 913125.
[8] Evtikhiev N N, S N Starikov, P A Cheryomkhin, and V V. Krasnov 2012 *Proc. SPIE.* **8301** p 830113.
[9] Cheremkhin P A, N N Evtikhiev, V V. Krasnov, V G Rodin, and S N Starikov 2014 *Opt. Eng.* **53** p 102107.
[10] Tykhonoff A N, and V Y Arsenin 1977 Solution of Ill-posed Problems, Washington: Winston & Sons, Washington, .
[11] Fienup J R 1997 *Appl. Opt.* **36** p 8352.