*Optica Applicata, Vol. XLV, No. 4, 2015*
DOI: 10.5277/oa150407

# A simple and practical color image encryption with the help of QR code

XIAOPENG DENG[1*], XIANG ZHU[2]

[1]Department of Physics and Information Engineering, Huaihua University,
Huaihua 418008, China

[2]College of Information and Communication Engineering, Harbin Engineering University,
Harbin 150001,China

[*]Corresponding author: dxpzqh@163.com

A simple and practical color image encryption is proposed with the help of quick response (QR) code. The original color image to be encoded is firstly transformed into the corresponding QR code, and then a joint transform correlator encrypting architecture is used to encode the corresponding QR code into a positive ciphertext. In the decryption, the corresponding QR code can be restored with the correct decryption key, and hence the original color image can be retrieved without any quality loss by scanning the restored QR code with a smartphone. Compared with the reported color image encryption techniques, the proposed technique does not need to convert color image (RGB) into indexed image formats or segregate into three color components prior to encryption and hence the corresponding reverse processes also are not required after decryption. Moreover, with the help of the QR code, the proposed method has strong tolerance to speckle noise and other noises resulting from optical system. In addition, the proposed method is practical because its ciphertext is a positive image and can be printed directly or manufactured as a card. The feasibility and effectiveness of the proposed method are demonstrated by numerical results.

Keywords: color image encryption, quick response (QR) code, joint transform correlator (JTC).

## 1. Introduction

In the past two decades, due to high-speed processing of two-dimensional complex data in parallel, optical image encryption techniques have been receiving more and more attention since REFREGIER and JAVIDI first proposed the double random phase encoding (DRPE) technique [1]. Various techniques, such as diffractive imaging [2, 3], phase retrieval algorithm [4–7], interference-based technique [8–10], phase-shifting interferometry [11] and so on, have been proposed for optical encryption. In addition, Arnold transform and gyrator transform are also used to encode optical images [12, 13]. However, most of them are not suited for color image encoding although they are quite robust and secure. In these encryption techniques, color information of a decrypted image will be lost when we use a monochromatic light to illuminate a color image. Since color information of an image sometimes plays an important role in many fields, color image encoding has become an important issue. To solve this issue, a variety of methods have been proposed for color image encryption [4, 6, 9, 14–16]. One kind of them is multichannel encryption system [9, 14, 15], in which the color image to be encoded is decomposed into three color components (typically red, green, and blue) prior to encoding and then each of these components is encrypted or decrypted independently by an optical encrypting system. Obviously, the multichannel color image encryption method makes the encryption and decryption processes become very complicated.

Other color image encryption approaches are based on single-channel encryption system [4, 6, 16]. These so-called single-channel systems are usually based on encoding the three color components into a single gray image by different methods prior to encryption and then the encoded gray image is used as the input image to be encrypted. During the decryption process, the three original color components can be extracted from a single gray ciphertext with the corresponding decryption keys, respectively. A distinct advantage about the single-channel encryption system is that only one channel is used instead of three because of encoding in advance. However, the single-channel encryption system as well as the multichannel encryption system requires the user to segregate color image into three color components prior to encryption and combine three decrypted color components into a color image after decryption, which still makes the whole processing become very complicated.

In addition to the above two kinds of methods, ZHANG and KARIM proposed a simple color image encryption based on index image [17]. In this method, the color image (RGB) to be encoded is converted into the corresponding index image prior to encryption. During the process of decryption, the color image can be recovered by converting the decrypted indexed images back into its RGB formats. Compared with the single-channel encryption system, this color encryption system is more compact and simple. However, this color encryption algorithm as well as the multichannel and single-channel algorithms is facing the same issue, which is that if these algorithms are implemented optically, the quality of experiment results is very poor because of speckle noise and other noises resulting from optical system. As we know, noise will influence not only image shapes but also image colors. So these color encryption techniques are not suited for implementing in optics. From this perspective, these color encryption techniques are not real optical color image encryptions and at most can be regarded as digital color image encryptions based on optical principles.

In this paper, with the help of the quick response (QR) code [18–20], a simple and practical optical method for color image encryption is proposed based on joint transform correlator (JTC) encrypting architecture. In encryption process, the original color image is firstly transformed into the corresponding QR code, and then the QR code is encoded into a positive ciphertext by using JTC encrypting architecture [21]. In decryption process, the QR code can be approximately recovered with the decryption key. Although the quality of the recovered QR code is somewhat degraded, the original color image still can be retrieved without any quality loss by scanning the restored QR code with a smartphone because QR codes are tolerant to speckle noise and other noises resulting from optical system. Compared with the single-channel and multi-channel encryption systems, the proposed method does not require the user to segregate the original color image into three color components prior to encryption and combine the three decrypted color components into a color image after decryption, which simplifies the whole processing. Moreover, with the help of the QR code, the proposed method can be absolutely implemented by the optical method [19]. In addition, the ciphertext of the proposed method is a positive function and can be printed directly or manufactured as a card, which makes it very convenient for users to store and transfer it in the real-world.

This paper is organized as follows. In Section 2, the encryption and decryption procedures are introduced in detail. Some simulation results and discussions are given in Section 3. A brief conclusion is presented in Section 4.

## 2. Encryption and decryption process

Suppose that the original color image to be encoded is denoted by $f(x, y)$. The encryption process of the proposed method includes two steps. First of all, the original color image is converted into the corresponding QR code denoted by $q(x, y)$. Secondly, the QR code is encrypted into a ciphertext by using an optical encryption system. Here we choose the JTC encrypting architecture [21], as shown in Fig. 1, as the optical encryption system because it is more compact, stable and practical than the $4f$ scheme. Thus the second step can be described as follows.

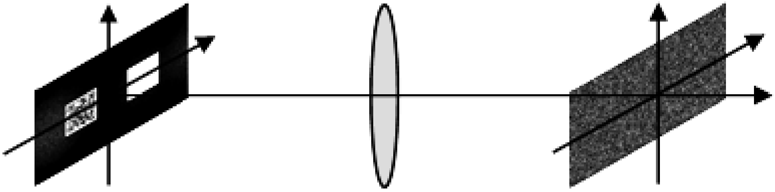

Fig. 1. Optical setup for color image encryption.

The QR code multiplied with a random phase mask $r(x, y)$, which locates at $(b, 0)$, and the encryption key $k(x, y)$, which locates at $(-b, 0)$, combine into the joint input image

$$i(x, y) = q(x - b, y)r(x - b, y) + k(x + b, y) \tag{1}$$

It should be pointed out that in order to avoid overlapping between the decrypted image and the zero-order term, we must choose an appropriate constant $b$ based on the actual situation. After performing the Fourier transform of the joint input image, the joint power spectrum (JPS) of the joint input image can be expressed as

$$\begin{aligned} J(u,v) = {} & |Q(u,v)\otimes R(u,v)|^2 + |K(u,v)|^2 + \\ & + [Q(u,v)\otimes R(u,v)]^* K(u,v)\exp(4\pi ibu) + \\ & + [Q(u,v)\otimes R(u,v)] K(u,v)^* \exp(-4\pi ibu) \end{aligned} \tag{2}$$

where ⊗ denotes the convolution, * means complex conjugate, $Q(u, v)$, $R(u, v)$ and $K(u, v)$ are the Fourier transforms of $q(x, y)$, $r(x, y)$ and $k(x, y)$, respectively. Although the first two terms of the JPS do not contribute to decrypting the QR code, we still choose the whole JPS rather than the last two terms as the ciphertext because it is a positive function and can be printed directly or manufactured as a card.

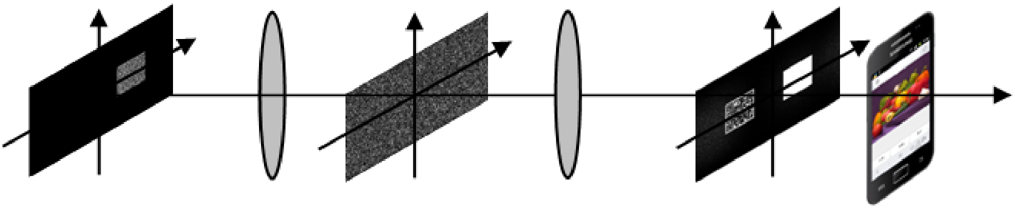

Fig. 2. Optical setup for color image decryption.

Based on the JTC decryption architecture [21], as shown in Fig. 2, the decrypting process can be described as follows.

First, the decryption key $k(x, y)$, which is displayed on the SLM, is Fourier transformed to the Fourier spectrum plane to obtain $K(u, v)$, and then the $K(u, v)$ is multiplied by $J(u, v)$ (*i.e.* the ciphertext), which leads to

$$\begin{aligned} m(u,v) = {} & \left[|Q(u,v)\otimes R(u,v)|^2 + |K(u,v)|^2\right] K(u,v) + \\ & + [Q(u,v)\otimes R(u,v)]^* K^2(u,v)\exp(4\pi ibu) + \\ & + [Q(u,v)\otimes R(u,v)]|K(u,v)|^2 \exp(-4\pi ibu) \end{aligned} \tag{3}$$

Finally, an inverse Fourier transform (ITF) of $m(u, v)$ is performed to obtain the input image

$$\begin{aligned} o(x,y) = {} & \mathrm{IFT}\left\{\left[|Q(u,v)\otimes R(u,v)|^2 + |K(u,v)|^2\right] K(u,v)\right\} + \\ & + \mathrm{IFT}\left\{\left[Q(u,v)\otimes R(u,v)\right]^* K^2(u,v)\right\}\otimes \delta(x-2b,y) + \\ & + \mathrm{IFT}\left\{\left[Q(u,v)\otimes R(u,v)\right]|K(u,v)|^2\right\}\otimes \delta(x+2b,y) \end{aligned} \tag{4}$$

where IFT stands for the inverse Fourier transform. It can be seen from Eq. (4) that when $|K(u, v)|^2 = 1$ the modulus of the third term of Eq. (4) is just the decrypted QR code, which is located at $(-2b, 0)$, while the first and second terms are uniformly distributed white noises and spread uniformly with some area, centered around (0, 0) and $(2b, 0)$, respectively. Hence, the corrupting noises can be spatially separable, depending on the value of $b$. With a smartphone positioned at $(-2b, 0)$ on the output plane, the original color image can be recovered by scanning the restored QR code.

It can be seen from the above encryption and decryption process that the proposed method does not require the user to segregate color image into three color components prior to encryption and combine three decrypted color components into a color image after decryption, which makes the whole processing become very simply and compactly. Although the proposed method also requires a mutual transformation between the original color image and the corresponding QR code, the transformation will not bring inconvenience to the user because the QR code could be generated by means of worldwide free available software and decoded by massively used smartphones. On the contrary, with the help of QR code the original color image can be retrieved without any quality loss because QR codes are tolerant to speckle noise and other noises resulting from optical system, which makes the proposed method be absolutely implemented by optical method [19].

However, owing to the current resource limitation in our laboratory, we just made some numerical simulations to verify the feasibility and effectiveness of the proposed method.

## 3. Simulation results and discussion

Computer simulations are performed to verify the efficiency of the proposed approach. A color image comprising 200×300 pixels, as shown in Fig. 3**a**, is used as the original image to be encoded. The corresponding QR code is shown in Fig. 3**b**, which is with the size of 200×200 pixels. Figures 3**c** and 3**d** show the real parts of the two decryption keys. The joint input image for JTC is shown in Fig. 3**e**, where the constant $b$ is 320 pixels. Figure 3**f** shows the encrypted result (*i.e.* JPS). It should be pointed out that the encryption key $k(x, y)$ is generated by iterative algorithm rather then random number generator, of which the reason is as follows.

As it is known, the Fourier transform of a random phase-only function is not always a phase-only function. However, it can be seen from Eq. (4) that only when $|K(u, v)|^2 = 1$, the QR code can be recovered accurately from the modulus of the third term of Eq. (4). So here we use iterative algorithm rather than random generator to generate the encryption key $k(x, y)$ so as to ensure that $|K(u, v)|^2$ is close to 1 [22].

The decrypted QR code is shown in Fig. 4**a**. To objectively estimate the decryption results, we calculate the correlation coefficient (CC) between the recovered image $f'(x, y)$ and the primary image $f(x, y)$, which is defined as

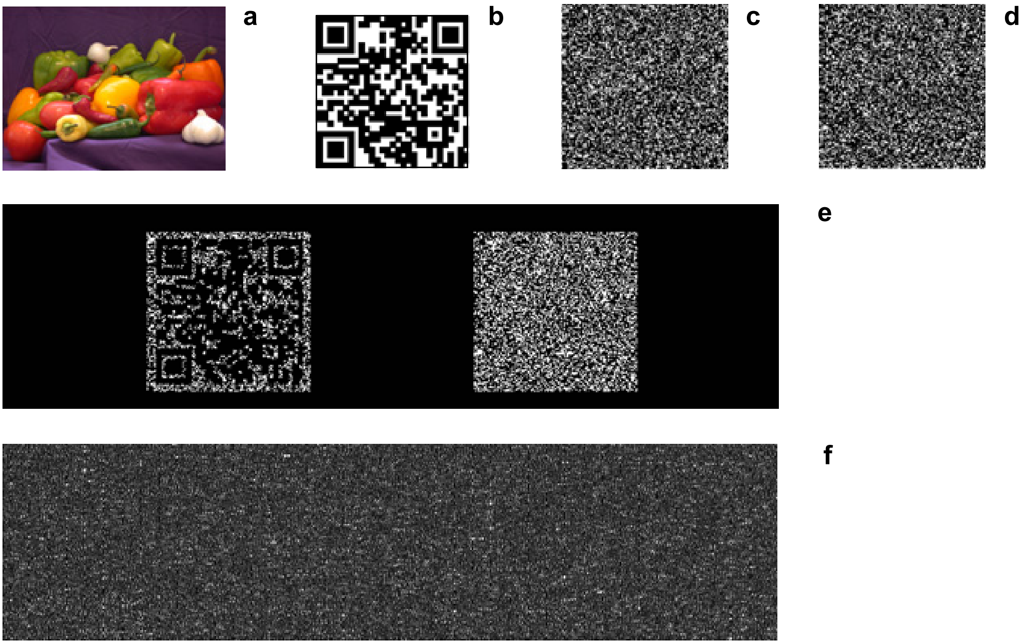

Fig. 3. The original color image (**a**); the corresponding QR code (**b**); the real part of encryption key $r(x, y)$ (**c**); the real part of encryption key $k(x, y)$ (**d**); the joint input image for JTC (**e**); the encrypted result (**f**).

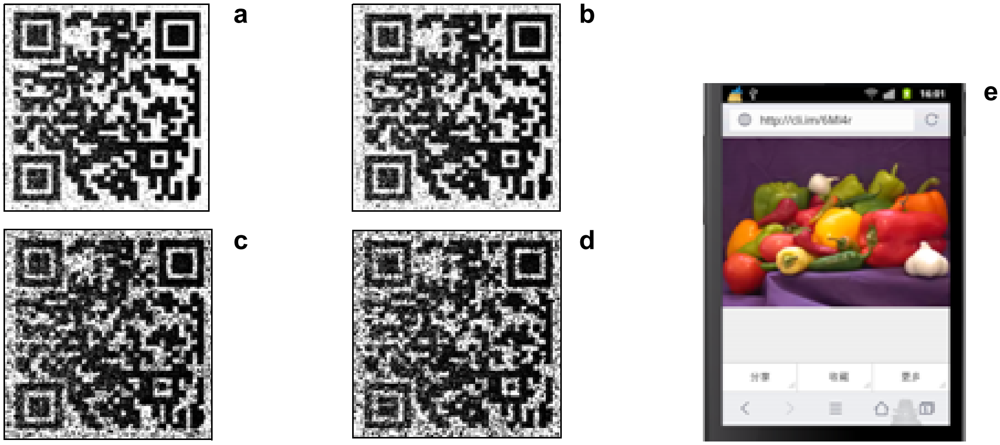

Fig. 4. The decryption QR code (**a**); the decrypted QR code corrupted by zero-mean speckle noise with a variance of 0.1 (**b**); the decrypted QR code corrupted by zero-mean additive speckle noise with a variance of 0.5 (**c**); the decrypted QR code corrupted by zero-mean additive speckle noise with a variance of 0.6 (**d**); the outcome obtained by scanning **a**–**d** with a smartphone (**e**).

$$\mathrm{CC} = \frac{E([f - E(f)][f' - E(f')])}{\sqrt{E([f - E(f)]^2)\,E([f' - E(f')]^2)}} \tag{5}$$

where $E$ is the expectation value and the coordinates are omitted for brevity. The CC value between the original and the restored QR code is 0.8421, which shows a satisfactory retrieval. The result obtained by scanning Fig. 4**a** with a smartphone is shown in Fig. 4**e**. It can be seen that the information hidden in the QR code was retrieved without any quality loss.

As we know, in the optical decryption system, the decrypted results are always affected by speckle noise. To test the robustness against speckle noise, we study the sensitivity of the recovered QR code to noise. Figures 4**b**–4**d** show the restored QR codes which are corrupted by zero-mean speckle noise with different variances. By a series of simulation experiments, we find that when the number of variances is less then or equal to 0.6, the original image still can be successfully displayed by scanning the corrupted QR codes, as shown in Fig. 4**e**. It can be seen from the above simulation results that although the noise makes a degradation of the decryption QR code in quality, the information hidden in the QR code still can be retrieved without any quality loss because the QR code has strong tolerance to speckle noise.

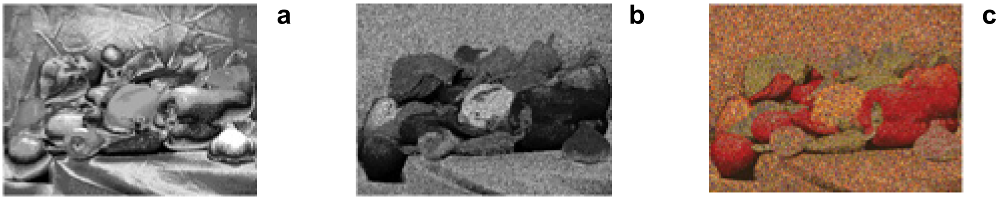

Fig. 5. The data matrix (**a**); the data matrix corrupted by zero-mean speckle noise with a variance of 0.1 (**b**); the index image of which the data matrix is corresponding to **b** (**c**).

For comparing the proposed method with that based on index image [17], we also study the sensitivity of the recovered index image to noise. In order to facilitate observation, the data matrix of the index image, which corresponds to Fig. 3**a**, is shown in Fig. 5**a**. Figure 5**b** shows the data matrix corrupted by zero-mean speckle noise with a variance of 0.1. Although the color mapping table of index image can remain the same, the data matrix corrupted by noise will affect the color of index image because in index image pixel values of data matrix denote color pointers, which can be seen from Fig. 5**c**. It can be seen from these results that although the encryption method based on index image is as compact and simple as our encryption method, it has poor tolerance to speckle noise.

Since the encryption system of this paper is essentially an encryption system based on JTC, its security and robustness entirely depend on the encryption system based on JTC. For the encryption system based on JTC, the security and robustness have been checked detailed in some published papers [23–25]. So the security and robustness of the proposed method are no longer studied in this paper.

## 4. Conclusions

In summary, a simple and practical optical method for color image encryption is proposed with the help of the QR code. First, the original color image to be encoded is transformed into a QR code by using a QR code generator, and then the QR code is encoded into a positive ciphertext by using JTC encrypting architecture. In decryption process, the QR code corresponding to the original color image can be approximately recovered with the correct decryption key, and hence the original color image can be retrieved without any quality loss by scanning the recovered QR code with a smartphone. Compared with the single-channel and multichannel encryption systems, the proposed method does not require the user to segregate the original color image into three color components prior to encryption and combine the three decrypted color components into a color image after decryption. Also compared with the method in [17], the proposed method has strong tolerance to speckle noise because of incorporating the QR code into encryption architecture. Simulation results show that the method is feasible and has strong tolerance to noise.

*Acknowledgements* – This work was supported by the Hunan Provincial Natural Science Foundation of China under Grant No.14JJ2129.

## References

[1] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.

[2] WEN CHEN, XUDONG CHEN, SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010, pp. 3817–3819.

[3] WEN CHEN, XUDONG CHEN, *Optical cryptography topology based on a three-dimensional particle -like distribution and diffractive imaging*, Optics Express **19**(10), 2011, pp. 9008–9019.

[4] XIAOPENG DENG, DAOMU ZHAO, *Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain*, Optics and Laser Technology **44**(2), 2012, pp. 374–377.

[5] HENNELLY B., SHERIDAN J.T., *Fractional Fourier transform-based image encryption: phase retrieval algorithm*, Optics Communications **226**(1–6), 2003, pp. 61–80.

[6] XIAOPENG DENG, DAOMU ZHAO, *Single-channel color image encryption using a modified Gerchberg –Saxton algorithm and mutual encoding in the Fresnel domain*, Applied Optics **50**(31), 2011, pp. 6019–6025.

[7] WEN CHEN, XUDONG CHEN, *Interference-based optical image encryption using three-dimensional phase retrieval*, Applied Optics **51**(25), 2012, pp. 6076–6083.

[8] YAN ZHANG, BO WANG, *Optical image encryption based on interference*, Optics Letters **33**(21), 2008, pp. 2443–2445.

[9] CHEN W., QUAN C., TAY C.J., *Optical color image encryption based on Arnold transform and interference method*, Optics Communications **282**(18), 2009, pp. 3680–3685.

[10] XIAOGANG WANG, DAOMU ZHAO, *Image encoding based on coherent superposition and basic vector operations*, Optics Communications **284**(4), 2011, pp. 945–951.

[11] Xiaogang Wang, Daomu Zhao, *Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry*, Optics Communications **268**(2), 2006, pp. 240–244.

[12] Zhengjun Liu, Min Gong, Yongkang Dou, Feng Liu, Shen Lin, Ahmad M.A., Jingmin Dai, Shutian Liu, *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255.

[13] Zhengjun Liu, Lie Xu, Qing Guo, Chuang Lin, Shutian Liu, *Image watermarking by using phase retrieval algorithm in gyrator transform domain*, Optics Communications **283**(24), 2010, pp. 4923–4927.

[14] Linfei Chen, Daomu Zhao, *Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms*, Optics Express **14**(19), 2006, pp. 8552–8560.

[15] Joshi M., Shakher C., Singh K., *Logarithms-based RGB image encryption in the fractional Fourier domain: a non-linear approach*, Optics and Lasers in Engineering **47**(6), 2009, pp. 721–727.

[16] Nanrun Zhou, Yixian Wang, Lihua Gong, Hong He, Jianhua Wu, *Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform*, Optics Communications **284**(12), 2011, pp. 2789–2796.

[17] Shuqun Zhang, Karim M.A., *Color image encryption using double random phase encoding*, Microwave and Optical Technology Letters **21**(5), 1999, pp. 318–323.

[18] Barrera J.F., Mira A., Torroba R., *Optical encryption and QR codes: secure and noise-free information retrieval*, Optics Express **21**(5), 2013, pp. 5373–5378.

[19] Barrera J.F., Mira-Agudelo A., Torroba R., *Experimental QR code optical encryption: noise-free data recovering*, Optics Letters **39**(10), 2014, pp. 3074–3077.

[20] Yi Qin, Qiong Gong, *Optical information encryption based on incoherent superposition with the help of the QR code*, Optics Communications **310**, 2014, pp. 69–74.

[21] Nomura T., Javidi B., *Optical encryption using a joint transform correlator architecture*, Optical Engineering **39**(8), 2000, pp. 2031–2035.

[22] Li-Chien Lin, Chau-Jern Cheng, *Optimal key mask design for optical encryption based on joint transform correlator architecture*, Optics Communications **258**(2), 2006, pp. 144–154.

[23] Chenggong Zhang, Meihua Liao, Wenqi He, Xiang Peng, *Ciphertext-only attack on a joint transform correlator encryption system*, Optics Express **21**(23), 2013, pp. 28523–28530.

[24] Wan Qin, Xiang Peng, Xiangfeng Meng, *Cryptanalysis of optical encryption schemes based on joint transform correlator architecture*, Optical Engineering **50**(2), 2011, article 028201.

[25] Barrera J.F., Vargas C., Tebaldi M., Torroba R., *Chosen-plaintext attack on a joint transform correlator encrypting system*, Optics Communications **283**(20), 2010, pp. 3917–3921.

*Received May 12, 2015*
*in revised form July 3, 2015*