

Improved decryption quality and security of joint transform correlator-based encryption system

Juan M. Vilardy, María S. Millán, Elisabet Pérez-Cabré

Applied Optics and Image Processing Group, Department of Optics and Optometry, Universitat Politècnica de Catalunya, 08222 Terrassa (Barcelona), Spain.

E-mail: juan.manuel.vilardy@estudiant.upc.edu

Abstract. Some image encryption systems based on modified double random phase encoding and joint transform correlator architecture produce low quality decrypted images and are vulnerable to a variety of attacks. In this work, we analyse the algorithm of some reported methods that optically implement the double random phase encryption in a joint transform correlator. We show that it is possible to significantly improve the quality of the decrypted image by introducing a simple nonlinear operation in the encrypted function that contains the joint power spectrum. This nonlinearity also makes the system more resistant to chosen-plaintext attacks. We additionally explore the system resistance against this type of attacks when a variety of probability density functions are used to generate the two random phase masks of the encryption-decryption process. Numerical results are presented and discussed.

Keywords: Image encryption, decryption, Joint transform correlator, Fourier transform, Random phase mask, Chosen-plaintext attack.

1. Introduction

Optical encryption technology is useful for security applications as it is proved by the intense research developed in the field in the last two decades. Significant progress in optoelectronic devices has made optical technologies attractive for security [1].

A pioneer optical encryption system, named double random phase encoding (DRPE), was proposed by Réfrégier and Javidi [2]. The optical hardware initially proposed to perform DRPE was the classical $4f$ -processor [3]. This processor typically requires strict optical alignment, which in practice is difficult to attain. To alleviate this constraint, Nomura and Javidi proposed a technique for optical DRPE using joint transform correlator (JTC) architecture that also showed other advantages [4]. With JTC, a common power-law sensor (such as CCD) captures the intensity distribution of the joint power spectrum (JPS) as the encrypted data, while the classical DRPE method requires

the recording of complex-valued information. An additional advantage of JTC is that the decryption process utilizes the same security key previously used in the encryption process, which eliminates the need to produce an exact complex conjugate of the key. Two non-overlapping data distributions are placed side-by-side at the input plane of the JTC that can be mathematically expressed by the addition of two terms, i. e. $A(x)*\delta(x-a)+B(x)*\delta(x+a)$, written in one-dimensional notation for the sake of simplicity. The first random phase mask (RPM-I) $r(x)$ is bonded to the image to be encrypted $f(x)$ and both are placed together at coordinate $x=a$, so that $A(x)=r(x)f(x)$. The inverse Fourier transform of the second random phase mask (RPM-II) $h(x)$ is placed at coordinate $x=-a$, so that $B(x)=\text{FT}^{-1}\{h(u)\}$, where FT^{-1} denotes inverse Fourier transform and variable u the spatial frequency coordinate. The random phase distributions $r(x)$ and $h(x)$ are statistically independent, purely phase data of the form $k(x)=\exp\{i2\pi\varphi_k(x)\}$, where $\varphi_k(x)$ is a normalized positive function randomly generated and uniformly distributed in the interval $[0, 1]$. Nomura and Javidi introduced the term “key code” for the inverse Fourier transform of the RPM-II in [4], which is generally fully complex-valued, with both amplitude and phase being variant magnitudes. Such an arrangement of the information in the JTC was mathematically equivalent to the DRPE proposed in [2]. Due to the difficulties encountered to display complex-valued functions on the spatial light modulators (SLMs) available at the time Ref. [4] was published, Nomura and Javidi used the optical Fourier transform of a RPM, i. e. $\text{FT}\{h(u)\}$, as the key code. In their optical implementation [4], they split in two beams the optical entrance of the setup, all what became more complex and required finer alignment than a conventional JTC. This difficulty was alleviated in [5] with the adoption of real-valued data for the key code $\text{FT}^{-1}\{h(u)\}$. This key code was designed using an algorithm so that its Fourier transform has a uniform amplitude distribution and a uniformly random phase distribution. An amplitude only SLM can be used to display the real-valued key code $\text{FT}^{-1}\{h(u)\}$ and the image to encrypt $f(x)$ side-by-side in the input plane of a conventional JTC setup to implement DRPE. In such a case, RPM-I is bonded to the part of the SLM where $f(x)$ is displayed [5].

Other modifications in DRPE implemented by JTC have been proposed by several authors [6-11]. Reference [6] gathers other optical encryption systems based on the JTC architecture. Among them, Islam and Alam [7] proposed a two-channel shifted-phase encoded JTC that eliminates the central orders in the JTC output plane, which results in a quality improvement of the decrypted image. However, the encrypted function resulting from the proposed method is a complex-valued distribution and cannot be captured by a conventional camera, therefore making the optical implementation more complicated in practice. Other contributions closer to the original JTC architecture and to our work are found in [8-10]. They substitute the complex-valued key code $\text{FT}^{-1}\{h(u)\}$ by the very RPM-II, that is, they take $B(x)=h(x)$ in the input plane of the JTC. Although this does not reproduce exactly the DRPE algorithm as proposed in [2], this modified JTC-based encryption system becomes easier to implement with the help of a simple full size diffuser glass (random phase element) placed in the input plane. On the one part of the JTC input plane, a zone of the diffuser (RPM-I) is against the image to be encrypted and, laterally shifted from it, another zone of the diffuser (RPM-II) is used on the other part. The latter RPM-II constitutes the security key used in both the

encryption and the decryption stages. Thus, whereas the RPM-II used as key in the original DRPE algorithm acts in the Fourier domain [2], it acts in the spatial domain in the modified DRPE algorithm [8-10]. This main difference between both proposals has a significant influence on the quality of the decrypted image, as we will show in this paper.

In [11] another modification of the setup is proposed. The diffuser acting as RPM is moved to a different plane, so that its Fourier transform is obtained in the input plane of the JTC. In this case $A(x) = f(x)\text{FT}\{r(u)\}$ and $B(x) = \text{FT}\{h(u)\}$. Note that, neither the modification described in [8-10] nor the second modification introduced in [11], exactly reproduce the mathematics of the original DRPE algorithm [2] implemented in a JTC [4].

The optical encryption methods proposed in [8-10] are vulnerable to plaintext attacks [12, 13]. In cryptanalysis, it is always assumed that attackers already know the encryption process and other resources, such as a pair consisting of an original image and its encrypted image, and that the attackers are trying to determine the security key. In chosen-plaintext attack (CPA), for instance, the attacker introduces an adequate input image (skillfully designed chosen plaintext) in the encryption [14] or decryption [15] process, and they get the corresponding output image in order to deduce the security key.

In this work, we analyse the algorithm of the method reported in [8-10] that optically implements the modified DRPE in a JTC. We show that it is possible to significantly improve the quality of the decrypted image by introducing a simple nonlinear operation in the encrypted function that contains the JPS. This nonlinearity consists of dividing the JPS by the square magnitude of the Fourier transform of the RPM-II. With this nonlinearity the encryption JTC system approaches better the implementation of the DRPE as it was originally proposed in [2]. There is no need to make the optical setup more complicated because a conventional JTC is sufficient for the implementation of the whole process. This nonlinearity also makes the system more resistant to CPAs. We additionally explore the system resistance against this type of attacks when a variety of probability density functions are used to generate the two RPMs of the encryption-decryption process. The proposed nonlinear-modified encryption method still benefits from the easier optical implementation of contributions [8-10] and, in addition to this, it keeps the same amount of information to be transmitted since the resulting encrypted function has the same size as its original counterpart and only requires one key for decryption.

The rest of the paper is organized as follows: Section 2 provides the mathematical background of the modified DRPE implemented in JTC architecture [8-10]. In Section 3, the proposed nonlinearity is introduced in the encrypted function and its effects on the decrypted image quality and on the system resistance against CPAs are analysed. Numerical experiments are designed to illustrate the proposal. The results presented and discussed lead to outline the conclusions in Section 4.

2. Image encryption system based on the JTC

Let $f(x)$ be the real image to be encrypted with values in the interval $[0, 1]$, $r(x)$ and $h(x)$ be two RPMs given by

$$r(x) = \exp\{i2\pi m(x)\}, \quad h(x) = \exp\{i2\pi n(x)\}, \quad (1)$$

where $m(x)$ and $n(x)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval $[0, 1]$. Figure 1 shows the optical encrypting scheme based on a JTC architecture (*via 1*), and the optical decrypting scheme based on a $4f$ -processor. In the encryption process, the RPM-I $r(x)$ is placed on the real image $f(x)$ and then, the product $r(x)f(x)$ and the RPM-II $h(x)$ are placed side by side in the input plane of JTC at coordinates $x = a$ and $x = -a$, respectively [8]. The JPS, also named the encrypted power spectrum $e(u)$, is given by

$$e(u) = \text{JPS}(u) = \left| \text{FT} \left[\{r(x)f(x)\} * \delta(x-a) + h(x) * \delta(x+a) \right] \right|^2 = |F(u) * R(u)|^2 + |H(u)|^2 + [F(u) * R(u)]^* H(u) e^{i2\pi(2a)u} + [F(u) * R(u)] H^*(u) e^{-i2\pi(2a)u}, \quad (2)$$

where the functions represented by capital letters correspond to the FTs from functions represented in lowercase letters, the symbol $(*)$ indicates the convolution operation and the superscript $*$ denotes the complex conjugation operation. Equation (2) demonstrates that the encrypted image is real, and thus, it can be registered and stored by a conventional intensity capture device, such as a CCD camera. The security key is represented by the RPM-II $h(x)$ and the RPM-I $r(x)$ is used to spread the information content of the original image $f(x)$ onto the encrypted image $e(u)$.

In the decryption process (Figure 1), the RPM-II $h(x)$ is placed at coordinate $x = -a$ in the input plane of a $4f$ -processor [8], and, consequently, in the Fourier plane, the encrypted power spectrum $e(u)$ is illuminated by $H(u)\exp[i2\pi au]$. The resulting product is given by

$$g(u) = e(u)H(u)e^{i2\pi au} = |F(u) * R(u)|^2 H(u)e^{i2\pi au} + |H(u)|^2 H(u)e^{i2\pi au} + [F(u) * R(u)]^* H^2(u)e^{i2\pi(3a)u} + [F(u) * R(u)] H^*(u)H(u)e^{-i2\pi au}. \quad (3)$$

The fourth term of equation (3) is the most interesting term since it retains the information to be decrypted [8]. Therefore, when the inverse FT is applied to the fourth term of equation (3) we obtain

$$d(x) = \text{FT}^{-1} \left\{ [F(u) * R(u)] H^*(u) H(u) e^{-i2\pi au} \right\} = r(x)f(x) * \{h(x) \otimes h(x)\} * \delta(x-a), \quad (4)$$

where the symbol (\otimes) indicates the correlation operation. Although RPM-I $r(x)$ is a phase-only function, the intensity distribution of $d(x)$ centered at coordinate $x = a$ would not longer be the intensity of the original image function $f(x)$ as it was obtained for the decrypted image in [2, 4]. Note that in equation (4) the product $r(x)f(x)$ appears convolved by the complex-valued autocorrelation of the RPM-II $h(x)$. The more this autocorrelation approaches a Dirac delta function (i.e, $h(x) \otimes h(x) \equiv \delta(x)$) [8], the more the intensity distribution captured at $x = a$ resembles the original image intensity $|f(x)|^2$.

The simulation results of the encryption and decryption processes following the steps described above, are shown in Figure 2. The image to be encrypted (original image) is

presented in Figure 2(a). The random distribution code $n(x)$ of RPM-II $h(x)$ is shown in Figure 2(b). The encrypted image is depicted in Figure 2(c). The decrypted image is shown in Figure 2(e), which depicts the magnified region of interest of the output plane (Fig. 2d). Note the difference between the decrypted image of Fig. 2(e), which has been obtained through the whole process represented by equations (1) to (4), and the image of Fig. 2(f) that has been obtained by calculating just the right term of equation (4) and taking the absolute value (i.e. $|r(x)f(x)*\{h(x)\otimes h(x)\}|$). The autocorrelation of RPM-II $h(x)$ is shown in Figure 2(g) to 2(i): Figure 2(g) represents the absolute value $|h(x)\otimes h(x)|$ in logarithmic scale, Figure 2(h) the phase $\{h(x)\otimes h(x)\}/|h(x)\otimes h(x)|$ coded in gray levels, and Figure 2(i) is a truncated linear representation of the absolute value $|h(x)\otimes h(x)|$. To evaluate the quality of the decrypted image, we use the root mean square error (RMSE) defined by [16]

$$\text{RMSE} = \left(\frac{\sum_{x=1}^M [f(x) - d(x)]^2}{\sum_{x=1}^M [f(x)]^2} \right)^{\frac{1}{2}}, \quad (5)$$

where $f(x)$ and $d(x)$ denote the original image and the decrypted image, respectively. The RMSE between the original image of Figure 2(a) and the decrypted image of Figure 2(e) is 0.687, and 0.505 if it is compared with the decrypted image of Figure 2(f). This value confirms the poor quality of the decrypted image as a consequence of the fact that the autocorrelation of RPM-II $h(x)$ is not purely a Dirac delta function. The autocorrelation of RPM-II $h(x)$ usually has a noisy background (Figure 2(g) to 2(i)) that may significantly affect the quality of the decrypted image.

2.1. Chosen-plaintext attack applied to the encryption system based on a JTC

According to [12], a CPA can reconstruct the FT of the security key, RPM-II $h(x)$. To obtain the FT of the RPM-II $h(x)$, this attack introduces a couple of chosen plaintexts in the encryption system. The first chosen plaintext and its corresponding encrypted image are

$$f_1(x) = 0, \quad e_1(u) = |H(u)|^2. \quad (6)$$

Therefore, when a null image is introduced in the encryption system, the square modulus of the FT of the security key is obtained. The second chosen plaintext is a shifted Dirac delta function, and its corresponding encrypted image is

$$f_2(x) = \delta(x - x_p), \quad e_2(u) = 1 + |H(u)|^2 + 2|H(u)| \cos \left\{ 2\pi \left[\phi(u) - m(x_p) + (2a + x_p)u \right] \right\}, \quad (7)$$

where $\phi(u)$ is the phase of $H(u)$ and $m(x_p)$ represents a constant value. The argument of the cosine function in equation (7) is mainly related to $\phi(u)$ with some additional phase terms. Provided $|H(u)|$ is obtained from equation (6), the phase of $H(u)$ can be retrieved from equation (7) by following a phase-shifting procedure similar to the one indicated in [12].

Therefore, after the two chosen plaintexts represented by the equations (6)-(7) are introduced into the encryption system, the attacker can have access to the complete complex information of the FT of the security key. Thus the encryption system based on JTC presented in the section 2 is vulnerable to the CPA [12].

3. Nonlinear modification of the JTC architecture

The analysis of the JTC-based encryption system carried out in the previous section, in terms of both the low quality of the decrypted image and the vulnerability to CPA, leads us to propose a nonlinear modification of the encryption step to overcome these drawbacks. We propose to introduce a nonlinearity that consists of dividing the JPS by $|H(u)|^2$. Thus, the nonlinearly modified encrypted information becomes

$$e_N(u) = \frac{\text{JPS}(u)}{|H(u)|^2} = \frac{|F(u) * R(u)|^2}{|H(u)|^2} + 1 + [F(u) * R(u)]^* \frac{H(u)}{|H(u)|^2} e^{i2\pi(2a)u} + [F(u) * R(u)] \frac{H^*(u)}{|H(u)|^2} e^{-i2\pi(2a)u}. \quad (8)$$

If $|H(u)|^2$ is equal to zero for a particular value of u , this intensity value is substituted by a small constant to avoid singularities when computing $e_N(u)$. Equation (8) represents the new encrypted image when the JPS is nonlinearly modified. Figure 1, which corresponds to the encrypting and decrypting schemes based on a JTC architecture, also shows the nonlinear modification of this new proposal (*via* 2).

In the decryption process (Figure 1), the product between the encrypted image (now represented by equation (8)) and the FT of the RPM-II $h(x+a)$ is given by

$$g_N(u) = e_N(u)H(u)e^{i2\pi au} = |F(u) * R(u)|^2 \frac{H(u)}{|H(u)|^2} e^{i2\pi au} + H(u)e^{i2\pi au} + [F(u) * R(u)]^* \frac{H^2(u)}{|H(u)|^2} e^{i2\pi(3a)u} + [F(u) * R(u)] \frac{H^*(u)H(u)}{|H(u)|^2} e^{-i2\pi au}. \quad (9)$$

When the inverse FT is applied to the simplified fourth term of equation (9), the obtained decrypted distribution is

$$d_N(x) = \text{FT}^{-1} \left\{ [F(u) * R(u)] e^{-i2\pi au} \right\} = r(x)f(x) * \delta(x-a). \quad (10)$$

The intensity of equation (10) produces the original image intensity $|f(x)|^2$ at coordinate $x = a$. Unlike equation (4), we remark that equation (10) does not have the autocorrelation term of the RPM-II $h(x)$, therefore a higher quality decrypted image is expected. It is worth mentioning that the proposed nonlinearity allows the whole system to closer approach the output result of DRPE as it was originally formulated by Réfrégier and Javidi in reference [2].

The simulation results of the nonlinearly modified encryption scheme are shown in Figure 3. The original image to be encrypted is depicted in Figure 3(a). The encrypted and decrypted images are shown in Figure 3(b) and 3(c), respectively. The RMSE between the original image from Figure 3(a) and the decrypted image from Figure 3(c) is 0.061. According to this parameter, the quality of the decrypted image shown in Figure 3(c) has greatly improved in comparison to the decrypted image displayed in Figure 2(e) or 2(f). This fact is mainly due to the removal of the autocorrelation term from the decrypted signal (see equations (4) and (10)).

The nonlinear modification of the JPS can be implemented using the optoelectronic setup of Figure 1 (JTC part) by following the procedure proposed in references [17-19].

The encrypted image given by equation (8) can be optically implemented by a two-step JTC [17-18]. In the first step, the power spectrum of the security key ($|H(u)|^2$) is captured. Then, the JPS of equation (2) is captured in the second step [19]. Finally, the JPS is digitally divided by $|H(u)|^2$, and thus, the encrypted image is computed. This encrypted distribution, along with the key, is the only information to be transmitted; therefore, this method does not increment the amount of data to be sent prior to the decryption stage.

3.1. Chosen-plaintext attack applied to the nonlinear JTC-based encryption system

In this section we test the resistance of the proposed nonlinear encryption system against CPA. According to equation (8), if a null image $f_1(x) = 0$ is introduced in the encryption system, the encrypted distribution will be

$$e_{N1}(u) = 1. \quad (11)$$

Unlike the classical JTC (via 1 of Figure 1), it will not be possible to obtain any information about the RPM-II $h(x)$ from the encrypted image given by equation (11). The second chosen plaintext uses a shifted Dirac delta function $f_2(x) = \delta(x - x_p)$ at the input plane of the nonlinear JTC. The corresponding encrypted image using equation (8) is

$$e_{N2}(u) = \frac{1}{|H(u)|^2} + 1 + \frac{2}{|H(u)|} \cos\left\{2\pi\left[\phi(u) - m(x_p) + (2a + x_p)u\right]\right\}, \quad (12)$$

where both the modulus and phase functions of $H(u)$ will be unknown. Therefore, these chosen-plaintext attacks will not allow the attacker to easily obtain any information about neither $h(x)$ nor $H(u)$.

However, some methods to extract the phase information [20-22] could be used to retrieve partial information of the security key $h(x)$. For this reason we analyse in the following subsection the relevance of the magnitude and phase information of the FT of $h(x)$ in the decryption step.

3.2. Security tests depending on RPMs features

The security of the proposed nonlinear JTC-based encryption system is further analysed in this section. The effects of knowing partial information of the security key in the decryption step are evaluated. To this end, different types of random distributions are considered to generate the RPMs. For the different cases studied in this section, the original image to be encrypted is represented by Figure 3(a), its corresponding encrypted image is calculated by using equation (8), and the modulus and phase of the FT of the security key $H(u)$ are denoted by $|H(u)|$ and $\phi(u)$, respectively.

The first case of study considers uniform random distributions so that all gray levels have the same probability [16]. For example, images shown in Figure 4(a) and 4(b) depict $m(x)$ and $n(x)$ with the named *Uniform* and *Beta* random distributions, respectively. These random codes were used to obtain the encrypted image of Figure 3(b). Figure 4(c) and 4(d) show the histograms of $m(x)$ and $n(x)$, respectively, which reveal the relative uniformity of the probability density function of these codes.

In a first experiment, we perform the decryption process using only the information $|H(u)|$ from $H(u)$ and we assume that $\phi(u) = 0$. The decrypted image $|d_{N3}(x)|$ for this case is shown in Figure 4(e), where the original image cannot be made out from the noisy background. In a second experiment, we perform again the decryption process but using only the phase of $H(u)$ and we consider that $|H(u)| = 1$. The corresponding decrypted image $|d_{N4}(x)|$ for this case is presented in Figure 4(f). In this case, the original image can be distinguished from the noisy background even though its quality is much lower (RMSE = 0.704). The results of the decrypted images of Figures 4(e) and 4(f) indicate that the information of $\phi(u)$ is more relevant in the decryption process than the information of $|H(u)|$, whenever $m(x)$ and $n(x)$ use uniform random distributions.

In the second case of study, non-uniform random distributions are used to generate the RPMs [16]. In particular, *Weibull* and *Chi-Square* random distributions are considered to generate $m(x)$ and $n(x)$, respectively. These images of random distributions codes are shown in Figure 5(a) and 5(b) and their histograms are depicted in Figures 5(c) and 5(d), respectively. Using the original image $f(x)$, $m(x)$ in RPM-I, $n(x)$ in RPM-II and the equation (8), the encrypted image $e_{N5}(u)$ is obtained and shown in Figure 5(e). For the decryption process, let us consider the full information of $\phi(u)$ (with $|H(u)| = 1$), which has been shown to be the most relevant piece of information if only partial data of the FT of the security key is available. The corresponding decrypted image $|d_{N5}(x)|$ is shown in Figure 5(f). This result demonstrates that the retrieval of the original image is much harder when $m(x)$ and $n(x)$ are generated by non-uniform random distributions. We repeat the latter experiment for different combinations of random distributions (*Uniform*, *Weibull* and *Chi-Square*) to generate $m(x)$ and $n(x)$ in the encryption-decryption process. Figure 6(a) shows the decrypted image when we swap the random distributions of Figure 5, that is, when $m(x)$ and $n(x)$ are given by *Chi-Square* and *Weibull* random distributions, respectively. In Figure 6(a), the original image can be identified although with some difficulty. The result is clearly different from Figure 5(f), hence the encryption-decryption scheme proposed in this work is asymmetric with respect to the role played by random distributions used for the RPMs. Images in Figure 6(b)-6(e) correspond to the decryption images when $m(x)$ is generated by a *Uniform* random distribution and $n(x)$ by a non-uniform random distribution (either *Chi-Square* or *Weibull*), and *vice versa*. If we use a *Uniform* random distribution for $n(x)$, the decrypted images showed in Figure 6(c) and 6(d) can be visualized more easily than the decrypted images of Figure 6(b) and 6(e) that use a non-uniform random distribution for $n(x)$. Therefore, in order to better protect the secret of the encrypted image we recommend to use non-uniform random distributions for $n(x)$, which is the random code associated to the security key RPM-II $h(x)$.

Finally, in the third case of study, we consider a more realistic case, for which $\phi(u)$ is not available, but it has to be estimated from equation (12) by taking $|H(u)| = 1$ and assuming a chosen-plaintext attack represented by a Dirac delta function $f_6(x) = \delta(x - x_p)$. In such a case the encrypted image is

$$e_{N6}(u) = 2 \left[1 + \cos \left\{ 2\pi \left[\phi(u) - m(x_p) + (2a + x_p)u \right] \right\} \right]. \quad (13)$$

In order to eliminate the ambiguities of the cosine function when its argument is evaluated from equation (13), a new chosen plaintext represented by a shifted Dirac

delta function $f_7(x) = \delta(x - x_p)e^{i\varphi}$ with a phase value ($\varphi < \pi/2$) is introduced in the encryption system. The result for the encrypted image with $|H(u)| = 1$ is

$$e_{N7}(u) = 2 \left[1 + \cos \left\{ 2\pi \left[\phi(u) - m(x_p) + (2a + x_p)u \right] - \varphi \right\} \right]. \quad (14)$$

Giving different values to the phase difference φ introduced in equation (14), for instance, using phase-shifting interferometry [23, 24], it is possible to suppress the ambiguity given by the sign of the cosine function in equation (13). This interferometry method is described in detail in reference [12]. Once determined, the argument of the cosine function of equation (13) without ambiguities, it permits to obtain $\phi(u)$, the phase of $H(u)$.

Then, the phase of $H(u)$ estimated by the equations (13)-(14) can be used in the decryption process (we assume that $|H(u)| = 1$) with different random distributions for $m(x)$ and $n(x)$. When either the uniform random distributions (Figure 4(a) and 4(b)) or non-uniform random distributions (Figure 5(a) and 5(b)) are used to generate $m(x)$ and $n(x)$, the respective decrypted images $|d_{N8}(x)|$ (Figure 7(a)) or $|d_{N9}(x)|$ (Figure 7(b)) are obtained, respectively. Images in Figure 7 are noisy and the original image cannot be identified. The results shown in Figure 7 prove that the retrieval of the original image is not possible when the security key $h(x)$ is estimated through the equations (13-14), regardless what random distribution has been used for $m(x)$ and $n(x)$ within *Uniform*, *Beta*, *Weibull* and *Chi-Square*.

For the sake of comparison of the cases of study provided in this work, table 1 contains a summary of all the results obtained so far.

4. Conclusions

In this paper we have presented an image encryption system based on a nonlinear joint transform correlator architecture. The nonlinear modification, introduced in the Fourier domain, has improved the quality of the decrypted image with respect to other previous works based on a modified DRPE algorithm implemented by JTC. Since the proposed modification is applied to the JPS, just before the generation of the encrypted image, there is no additional burden in the transmitted data. In addition, using the nonlinear term introduced into the JPS, it permits an improvement in the security of the encrypted image. Due to this, the encrypted image is robust against chosen-plaintext attacks. Concerning the RPMs features, the most relevant piece of information in the decryption process is the phase of the Fourier transform of the RPM-II provided the RPMs have been generated by uniform random distributions; the encryption-decryption scheme is asymmetric with respect to the random distributions used for the two RPMs, and the secret of the encrypted image is better protected when a non-uniform random distribution is used in the generation of RPM-II. Finally, the nonlinear encryption and the decryption processes are suitable for optoelectronic implementation in a two-step JTC and a 4f-processor, respectively.

Acknowledgement

This research has been partly funded by the Spanish Ministerio de Ciencia e Innovación and Fondos FEDER (Project DPI2009-08879). The first author also wishes to thank the

Departamento Administrativo de Ciencia, Tecnología e Innovación from Colombia, COLCIENCIAS, for a doctoral scholarship.

References

- [1] E. Pérez-Cabré, M. S. Millán, Optical data encryption, in *Optical and Digital Image Processing: Fundamentals and Applications* (Eds. G. Cristóbal, P. Schelkens and H. Thienpont), Wiley-VCH Verlag GmbH & Co. (2011).
- [2] P. Réfrégier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, *Opt. Lett.* 20, 767-769, (1995).
- [3] J. W. Goodman, *Introduction to Fourier Optics*, Second edition, McGraw-Hill, New York, (1996).
- [4] T. Nomura, B. Javidi, Optical encryption using a joint transform correlator architecture, *Opt. Eng.* 39, 2031-2035, (2000).
- [5] T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator, *Appl. Opt.* 42, 1508-1514 (2003).
- [6] A. Alfalou, and C. Brosseau, Optical image compression and encryption methods, *Adv. Opt. Photon.* 1, 589-636 (2009).
- [7] M. N. Islam, and M. S. Alam, Optical security system employing shifted phase-encoded joint transform correlation, *Opt. Commun.* 281, 248-254, (2008).
- [8] E. Rueda, J. F. Barrera, R. Henao, R. Torroba, Optical encryption with a reference wave in a joint transform correlator architecture, *Opt. Commun.* 282, 3243-3249 (2009).
- [9] J. F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, and R. Torroba, Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality, *Opt. Commun.* 284, 4350-4355 (2011).
- [10] J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, and R. Torroba, Experimental multiplexing of encrypted movies using a JTC architecture, *Opt. Express* 20, 3388-3393 (2012).
- [11] E. Rueda, J. F. Barrera, R. Henao, and R. Torroba, Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture, *Opt. Eng.* 48, 027006-027006 (2009).
- [12] J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, Chosen-plaintext attack on a joint transform correlator encrypting system, *Opt. Commun.* 283, 3917-3921, (2010).
- [13] J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, and N. Bolognini, Known-plaintext attack on a joint transform correlator encrypting system, *Opt. Lett.* 35, 3553-3555 (2010).
- [14] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, *Opt. Express* 15, 10253-10265, (2007).
- [15] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys, *Opt. Lett.* 30, 1644-1646 (2005).
- [16] R. C. Gonzalez, R. E. Woods, S. L Eddins, *Digital Image Processing Using Matlab*, Second edition, Gatesmark Publishing, USA, (2009).
- [17] E. Pérez, K. Chałasińska-Macukow, K. Styczyński, R. Kotyński, M. S. Millán, Dual nonlinear correlator based on computer controlled joint transform processor: Digital analysis and optical results, *Journal of Modern Optics* 44, 1535-1552 (1997).
- [18] E. Pérez, M. S. Millán, and K. Chałasińska-Macukow, Optical pattern recognition with adjustable sensitivity to shape and texture, *Opt. Commun.* 202, 239-255 (2002).
- [19] M. Tebaldi, S. Horrillo, E. Pérez-Cabré, M. S. Millán, D. Amaya, R. Torroba, N. Bolognini, Experimental color encryption in a joint transform correlator architecture, *Journal of Physics: Conference Series* 274 (2011) 012054.
- [20] R. W. Gerchberg and W. O. Saxton, A practical algorithm for the determination of the phase from image and diffraction plane pictures, *Optik* 35, 237-246 (1972).
- [21] J. R. Fienup, Phase retrieval algorithms: a comparison, *Appl. Opt.* 21, 2758-2769 (1982).
- [22] G. Situ, U. Gopinathan, D. S. Monaghan and J. T. Sheridan, Cryptanalysis of optical security systems with significant output images, *Appl. Opt.* 46, 5257-5262 (2007).
- [23] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, Optoelectronic information encryption with phase-shifting interferometry, *Appl. Opt.* 39, 2313-2320 (2000).
- [24] X. F. Meng, L. Z. Cai, X. F. Xu, X. L. Yang, X. X. Shen, G. Y. Dong, and Y. R. Wang, Two-step phase-shifting interferometry and its application in image encryption, *Opt. Lett.* 31, 1414-1416 (2006).

List of figure captions

Fig. 1. Scheme of the optical setup composed by an encryption system based on a JTC architecture (*via 1* or *via 2*) and a decryption system based on a $4f$ -processor.

Fig. 2. (a) Original image $f(x)$ to be encrypted, (b) Random function $n(x)$ of RPM-II $h(x)$, (c) Encrypted image $e(u)$, (d) Absolute value of the output plane obtained by computing the whole encryption/decryption process, (e) Magnified region of interest of (d) corresponding to the decrypted image $|d(x)|$, (f) Decrypted image obtained by calculating just the right term of equation (4) and taking the absolute value $|r(x)f(x)*\{h(x)\otimes h(x)\}|$, and (g)-(i) Autocorrelation of $h(x)$: (g) Absolute value $|h(x)\otimes h(x)|$ in logarithmic scale, (h) Phase $\{h(x)\otimes h(x)\}/|h(x)\otimes h(x)|$ coded in gray levels, and (i) Truncated linear representation of the absolute value $|h(x)\otimes h(x)|$.

Fig. 3. (a) Original image $f(x)$ to be encrypted; results obtained when the JPS is nonlinearly modified: (b) Encrypted image $e_N(u)$, and (c) Decrypted image $|d_N(x)|$.

Fig. 4. (a)-(b) Random distributions: (a) *Uniform* for $m(x)$, and (b) *Beta* for $n(x)$. (c)-(d) Histograms of: (c) $m(x)$, and (d) $n(x)$. (e)-(f) Decrypted images: (e) $|d_{N3}(x)|$ using only the information of $|H(u)|$ and taking $\phi(u) = 0$, and (f) $|d_{N4}(x)|$ using only the phase of $H(u)$ and taking $|H(u)| = 1$.

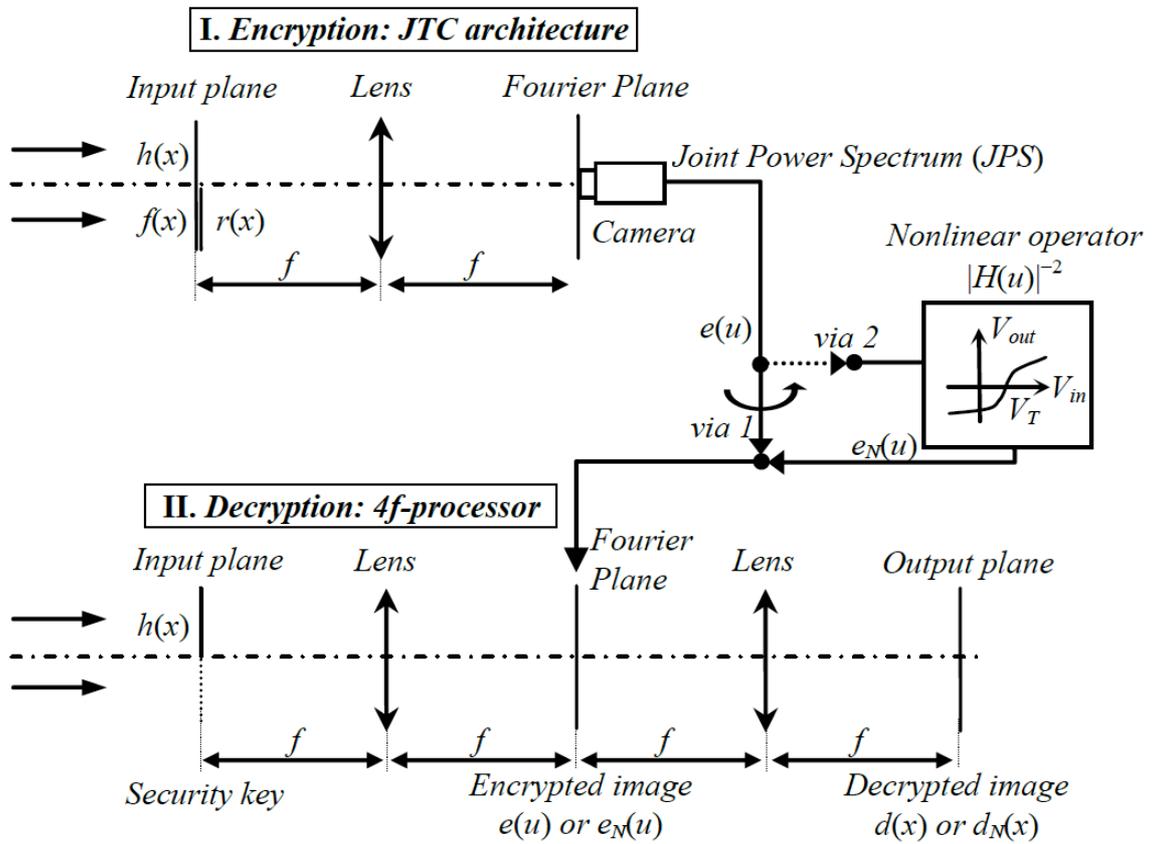
Fig. 5. (a)-(b) Random distributions: (a) *Weibull* for $m(x)$, and (b) *Chi-Square* for $n(x)$. (c)-(d) Histograms of: (c) $m(x)$, and (d) $n(x)$. (e) Encrypted image $e_{N5}(u)$, and (f) Decrypted image $|d_{N5}(x)|$ using only the phase of $H(u)$ and taking $|H(u)| = 1$.

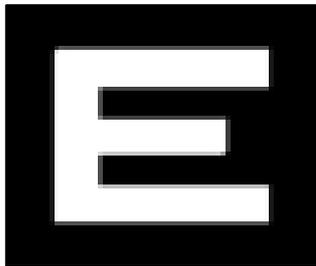
Fig. 6. Decrypted images with their respective RMSE generated when we use only the phase of $H(u)$ and take $|H(u)| = 1$ and the following random distributions for $m(x)$ and $n(x)$, respectively: (a) *Chi-Square* and *Weibull* (for which the random distributions have been swapped with respect to Figure 5), (b) *Uniform* and *Chi-Square*, (c) *Chi-Square* and *Uniform*, (d) *Weibull* and *Uniform*, and (e) *Uniform* and *Weibull*.

Fig. 7. Decrypted images $|d_{N8}(x)|$ and $|d_{N9}(x)|$ obtained in the third case of study when $m(x)$ and $n(x)$ are respectively represented by the following random distributions: (a) *Uniform* and *Beta*, and (b) *Weibull* and *Chi-Square*.

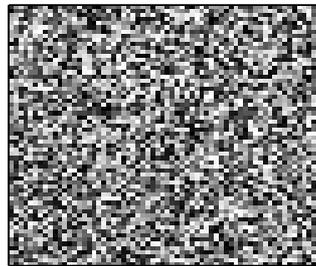
List of table captions

Table 1. Summary of the results obtained for the decrypted images in the experiments simulated in this work.

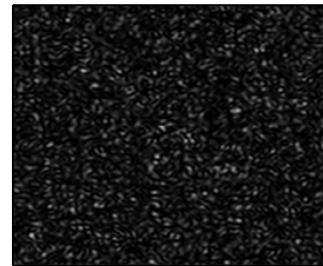




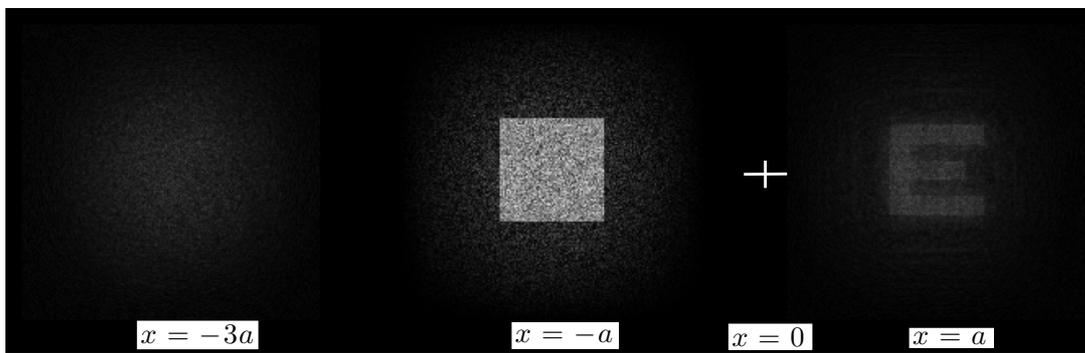
(a)



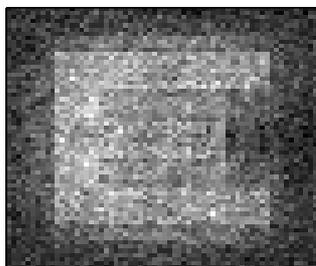
(b)



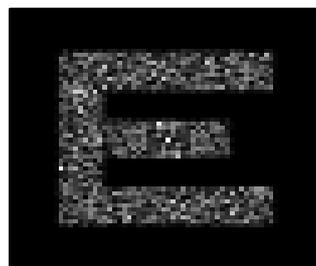
(c)



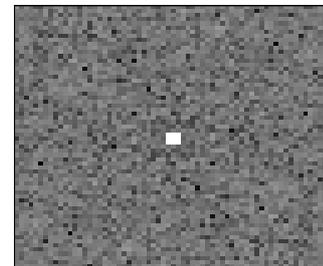
(d)



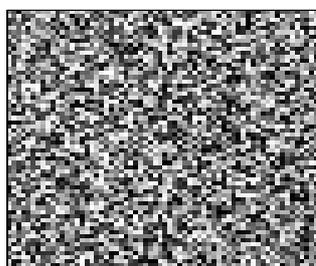
(e)



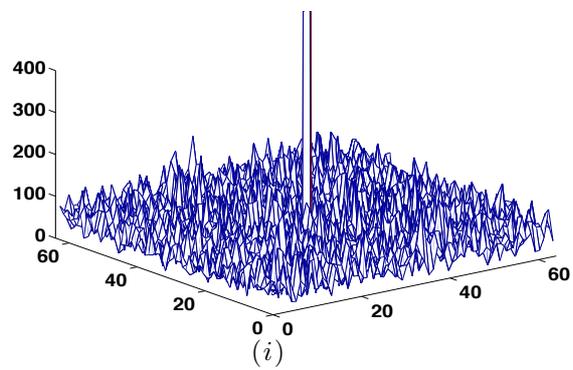
(f)



(g)



(h)



(i)

Fig. 2.

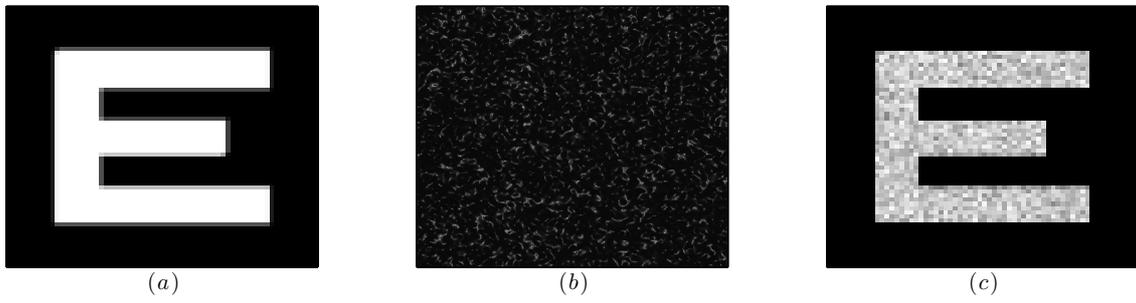


Fig. 3.

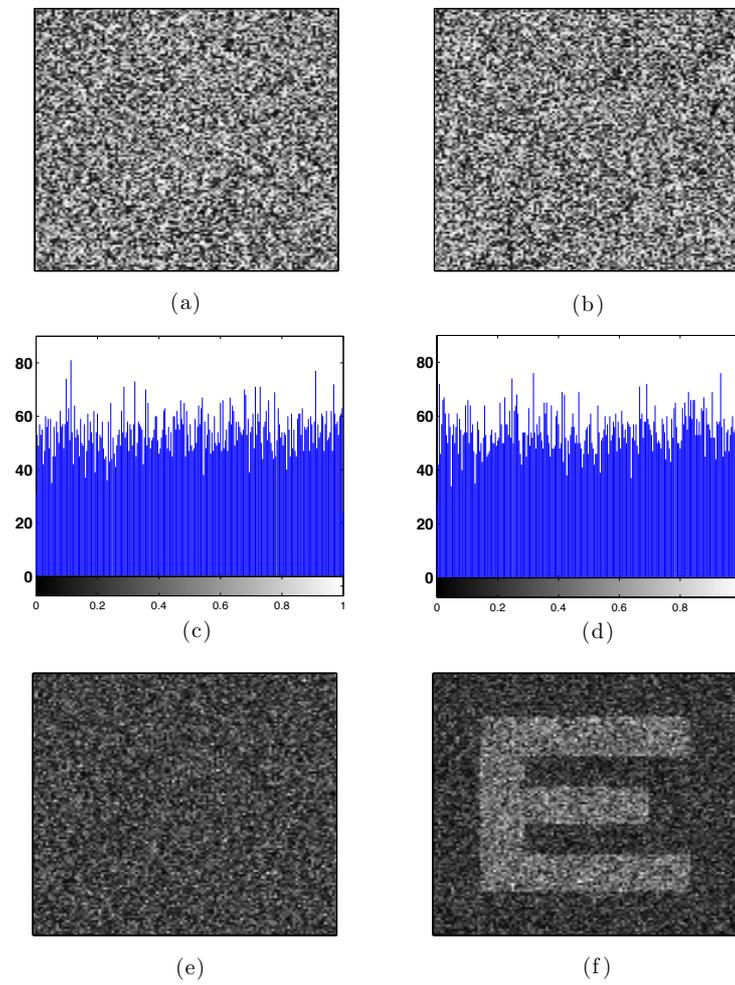


Fig. 4.

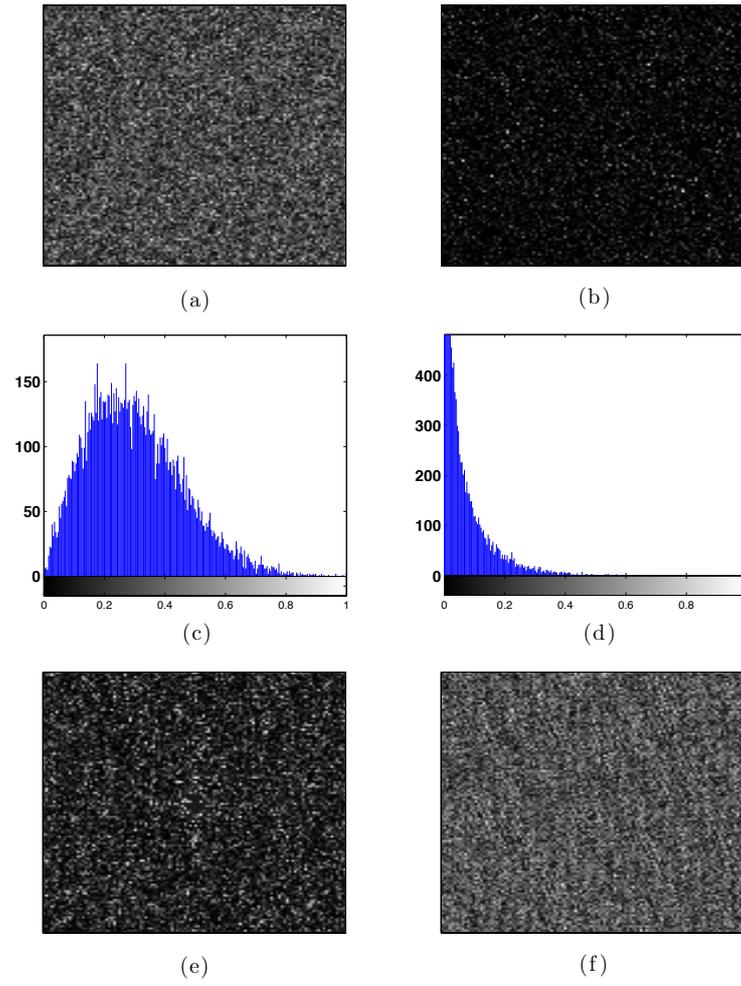


Fig. 5.

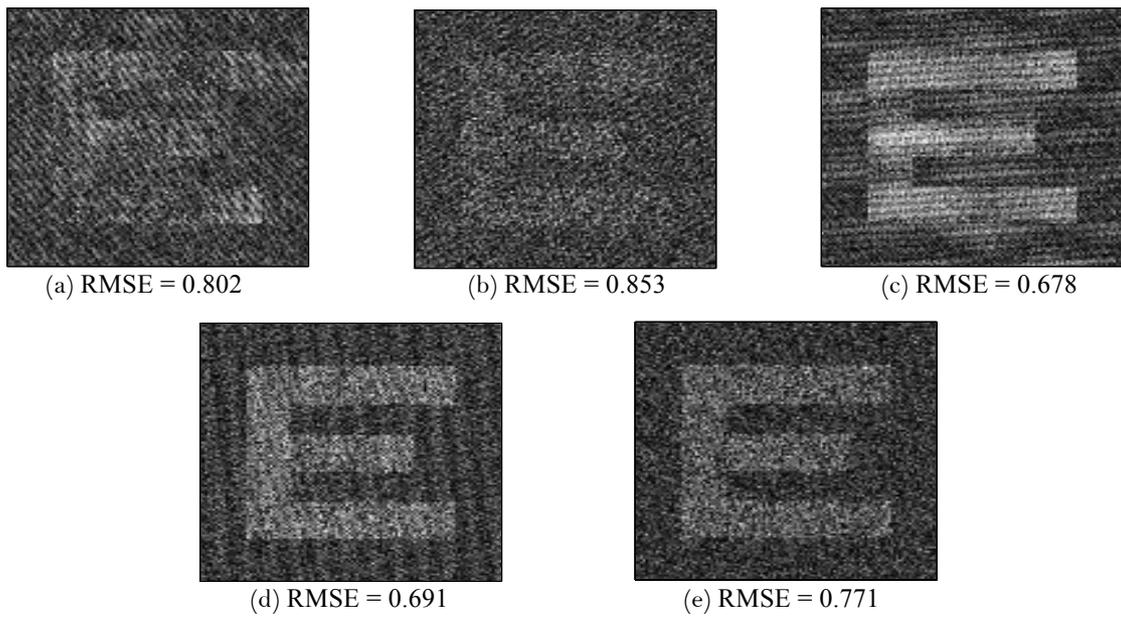
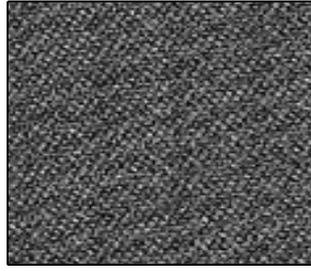
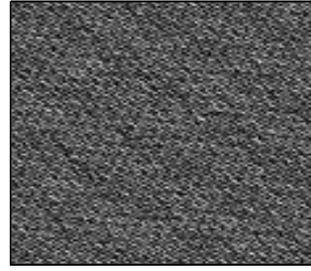


Fig. 6.



(a)



(b)

Fig. 7.

Table 1.

	RPM-I $m(x)$	RPM-II $n(x)$	Available information of the key	RMSE	Figure
Procedure according reference [8]	<i>Uniform</i>	<i>Beta</i>	Full $H(u)$	0.687	2(e)
Our proposal	<i>Uniform</i>	<i>Beta</i>	Full $H(u)$	0.505	2(f)
1 st Case of study	<i>Uniform</i>	<i>Beta</i>	$ H(u) $	0.917	4(e)
	<i>Uniform</i>	<i>Beta</i>	$\phi(u)$	0.704	4(f)
2 nd Case of study	<i>Weibull</i>	<i>Chi-Square</i>	$\phi(u)$	0.903	5(f)
	<i>Chi-Square</i>	<i>Weibull</i>	$\phi(u)$	0.802	6(a)
	<i>Uniform</i>	<i>Chi-Square</i>	$\phi(u)$	0.853	6(b)
	<i>Chi-Square</i>	<i>Uniform</i>	$\phi(u)$	0.678	6(c)
	<i>Weibull</i>	<i>Uniform</i>	$\phi(u)$	0.691	6(d)
3 rd Case of study (CPA)	<i>Uniform</i>	<i>Beta</i>	Estimated $\phi(u)$	0.771	6(e)
	<i>Weibull</i>	<i>Chi-Square</i>	Estimated $\phi(u)$	0.957	7(a)
				0.935	7(b)