IOP Publishing Journal of Optics
J. Opt. 19 (2017) 105703 (7pp) https://doi.org/10.1088/2040-8986/aa8738

Cryptographic salting for security enhancement of double random phase encryption schemes

Alejandro Velez Zea[1,4], **John Fredy Barrera**[2] and **Roberto Torroba**[1,3]

[1] Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) C.P 1897, La Plata, Argentina
[2] Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia
[3] UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

E-mail: alejandrov@ciop.unlp.edu.ar

Received 22 June 2017, revised 16 August 2017
Accepted for publication 21 August 2017
Published 19 September 2017

Abstract

Security in optical encryption techniques is a subject of great importance, especially in light of recent reports of successful attacks. We propose a new procedure to reinforce the ciphertexts generated in double random phase encrypting experimental setups. This ciphertext is protected by multiplexing with a 'salt' ciphertext coded with the same setup. We present an experimental implementation of the 'salting' technique. Thereafter, we analyze the resistance of the 'salted' ciphertext under some of the commonly known attacks reported in the literature, demonstrating the validity of our proposal.

Keywords: optical encryption, joint transform correlator, multiplexing

(Some figures may appear in colour only in the online journal)

1. Introduction

Optical cryptosystems are an interesting field of research, due to their many degrees of freedom and their potential to provide fast and reliable data security. The first optical encryption scheme was proposed by Refreiger and Javidi [1], called double random phase mask encryption (DRPE) scheme. Since then, many alternative optical encryption systems have been proposed, highlighting the flexibility of these setups [2].

Further research deals with the main limitations of the DRPE systems [3], namely, the challenges regarding their experimental realization, or the degradation of the decrypted data compared with the input objects [4], while at the same time attempting to assess and to improve their security [5].

As part of the ongoing efforts in determining the security of these systems, researchers have proposed a variety of attacks against them. These attacks are classified depending on the amount of information and access to the cryptosystem that is assumed available to the attacker.

The first of these categories of attacks is the chosen plaintext attack (CPA), where the attacker has full access to the cryptosystem, and can introduce specially tailored plaintexts to be encrypted in order to deduce the encryption key. This was the first kind of attack demonstrated against the DRPE scheme [6]; however, several methods have been proposed to thwart them [7, 8]. In practice, most actual encryption systems, digital or optical, are known to be vulnerable if the attacker has full access to the encryption machine.

The next attack is the known plaintext attack (KPA), where one or more plaintext–ciphertext pairs are in possession of the attacker [9, 10]. The unauthorized user has no access to the machine, cannot choose the plaintexts at his disposal, and his target is to deduce the encryption key from the available information. Depending on the number of plaintext–ciphertext pairs available to the intruder, there are several different implementations of KPA against optical cryptosystems. Like in CPA, several modifications have been proposed to harden the DRPE systems against these attacks [11].

Finally, the last kind of attack to be successfully demonstrated against DRPE systems is the ciphertext only attack

[4] Author to whom any correspondence should be addressed.

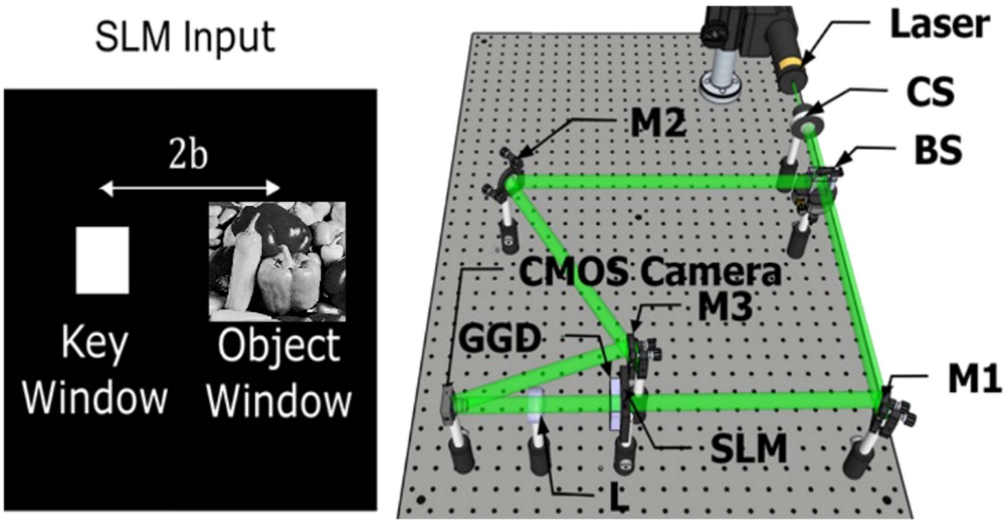

Figure 1. Experimental JTC cryptosystem (SLM: spatial light modulator, CS: collimation system, M: mirror, L: lens, BS: beam splitter, GGD: ground glass diffuser).

(COA) [12–16], where the intruder can retrieve the plaintext directly from the ciphertext, without the need for the encryption key. This is the most critical attack any cryptosystem must resist to be considered secure. In optical cryptosystems, COA makes use of phase retrieval algorithms. As a measure to guarantee their convergence to a solution, additional information about the encryption scheme is often necessary, for example the object and key sizes.

According to the above descriptions, it becomes evident that the developing of new methods to increase the security of DRPE systems is of great relevance in the field.

In this work, we propose a new procedure to strengthen the ciphertext produced by DRPE schemes against attacks. We achieve this by multiplexing the ciphertext of the data to be safeguarded with another ciphertext encrypted with the same system. This technique is analog to the 'cryptographic salting' of the ciphertexts found in some computer encryption algorithms, to guarantee that the same plaintext produces different ciphertexts [17]. In these algorithms, random data is added to the plaintext prior or after encryption, altering the resulting ciphertext. This is especially relevant in large databases containing encrypted passwords. In these cases, an entropy attack aided by a dictionary of common passwords can be used to guess a portion of the plaintexts, and from there the encryption key may be cracked by the use of known-plaintext attacks.

In optical encryption, a similar level of protection can be achieved with our proposal, where each ciphertext is multiplexed with another ciphertext corresponding to a 'salt'. Each time the system encrypts a new data, the salt is changed, to ensure that two ciphertexts always have different salts, even when encrypted using the same key.

2. Encryption and cryptographic salting scheme

To show the effectiveness of our proposal, we will use as case study the joint transform correlator (JTC) cryptosystem [18] with amplitude encoding, as shown in figure 1.

In the experimental setup, one arm contains the JTC system and the other provides a reference plane wave that will be used to register the encryption key. In the JTC system, the input plane has two windows, separated a distance $2b$ that are projected on a SLM placed in the focal plane of a convergent lens. The SLM is in contact with a random phase mask, provided by a ground glass diffuser. One of the windows is an empty square and will be used as key window. Light propagates through the diffuser, acquiring a random phase and then through the key window. This produces the encryption key. The image to be encrypted is projected in the other window, which will be the object window. In the conjugate plane of the lens, there is a CMOS camera as an intensity recording medium. To achieve encryption, we block the reference wave, and then the CMOS camera registers the intensity of the interference between the Fourier transforms (FTs) of both windows, called the joint power spectrum (JPS).

$$\begin{aligned} J(v, w) = &|F(v, w)|^2 + |K(v, w)|^2 \\ &+ F^*(v, w)K(v, w)\exp(4\pi ibv) \\ &+ F(v, w)K^*(v, w)\exp(-4\pi ibv), \end{aligned} \tag{1}$$

where * means complex conjugate, and $K(v, w)$, $F(v, w)$ are the FTs of the key window $k(x, y)$, and the object window given by $f(x, y) = o(x, y)r(x, y)$, respectively, with $o(x, y)$ the object and $r(x, y)$ the object window phase mask.

The JPS is sometimes considered the ciphertext of the JTC encryption scheme, since the original data can be retrieved from it by using the correct encryption key. The JPS as ciphertext, however, is vulnerable to COA since it contains information about the input plane beyond the encrypted object, as seen in equation (1). Peng *et al* [12] demonstrated that the recovery of the encrypted data from the JPS can be achieved by solving a phase retrieval problem with a single measurement. The inverse Fourier transform (IFT) of the JPS contains information about the distance $2b$ and the key and object sizes. This information allows for the convergence of the phase retrieval problem. To avoid these vulnerabilities, we can extract from the JPS the data related to the ciphertext (in our case the fourth term of

equation (1)), discarding remaining data. This is done by performing the IFT of the JPS, which results in a central order and two side orders containing the ciphertext and its complex conjugate. We can filter the unwanted terms while retaining the ciphertext [19], which is given by

$$e(x, y) = [o(x, y)r(x, y)] \otimes k^*(x, y), \tag{2}$$

where $o(x, y)$ is the plaintext the attacker wants to retrieve, $r(x, y)$ and $k(x, y)$ are random phase masks.

Decryption is achieved by performing the IFT of the ciphertext, multiplying it by the FT of the encryption key $k(x, y)$ and then performing the FT of the result. To experimentally register the encryption key, we use the scheme of figure 1 with the reference arm unblocked, and we project only the key window in the SLM. The lens performs the FT of the encryption key in the camera plane, which will interfere with the reference plane wave. The resulting intensity pattern is an off-axis Fourier hologram of the encryption key which is registered by the CMOS camera. After eliminating the DC term and the twin image from this hologram [20], we recover the encryption key $k(x, y)$.

We now introduce our salting proposal, where using the same system, we encrypt a 'salt' $s(x, y)$. The salt may be any object with larger support than the plaintext of the data to be salted, for example, a random amplitude mask. The ciphertext of this salt is then multiplexed with the ciphertext of the data we are interested in protecting. The salted ciphertext is then given by

$$\begin{aligned} e_s(x, y) = &[o(x, y)r(x, y)] \otimes k^*(x, y) \\ &+ [s(x, y)r(x, y)] \otimes k^*(x, y). \end{aligned} \tag{3}$$

After decryption with the correct key $k(x, y)$, the recovered data is given by

$$d_s(x, y) = [o(x, y)r(x, y)] + [s(x, y)r(x, y)], \tag{4}$$

which is an overlap of the salt and the object. If an authorized user knows the salt plaintext and the two-phase masks, he/she can subtract it from equation (4) to recover the object $o(x, y)$.

It is worth noting that depending on the salt and the encrypted object, the decrypted object may remain recognizable even if the salt is not subtracted from the result (see figure 2(d)). Therefore, salt is not an additional encryption key, but rather a way to hinder attacks. The salt ciphertext should not be available to anyone, to prevent an attacker from simply subtracting it from the salted ciphertext to undo the salting.

3. Cryptographic salting results

We test the reconstruction of the salted ciphertext by using data encrypted with the experimental implementation of the scheme of figure 1. The object and key windows had a size of 4.096 mm by 4.096 mm. The lens focal length was 200 mm and a DPSS laser with a wavelength of 532 nm and 300 mW of power was used. The registering medium was a EO-10012C CMOS camera with a resolution of 3840 × 2748 and a pixel size of 1.67 μm.

Figure 2(a) is the input object, with figure 2(b) the result after encryption–decryption without salting the ciphertext. We choose as salt a random amplitude mask, shown in figure 2(c). In figure 2(d), we see the result of decrypting the salted ciphertext with the correct key. As previously discussed, the decrypted plaintext is recognizable with a slight degradation in quality. In figure 2(e), we show the decrypted result from the salted ciphertext after subtracting the salt plaintext. As expected, the quality becomes very similar to the unsalted result shown in figure 2(b).

4. Resistance to data loss and noise of the ciphertext

One of the advantages of DRPE encryption schemes is that its ciphertexts are highly resistant to data loss and noise. We now show that salting does not affect this resistance. To do this, we used the ciphertext corresponding to the results of section 3.

We tested the resistance to data loss, by removing randomly distributed pixels in both the salted and unsalted ciphertext. The resulting ciphertexts were decrypted with the correct key. Then we obtained the correlation coefficient cc between the decrypted object from the unsalted ciphertext without data loss R compared with the one obtained from the salted and unsalted ciphertexts after data loss I. The correlation coefficient is given by

$$cc = \frac{\sum_m \sum_n (R_{mn} - \overline{R})(I_{mn} - \overline{I})}{\sqrt{\left(\sum_m \sum_n (R_{nm} - \overline{R})^2\right)\left(\sum_m \sum_n (I_{nm} - \overline{I})^2\right)}}, \tag{5}$$

where n, m are pixel coordinates, and $\overline{R}$, $\overline{I}$ are the mean values of R and I.

As we can see in figure 3, salting introduces a small reduction of the correlation coefficient. However, the behavior after data loss is very similar to the one of the unsalted ciphertext.

We also tested the effect of additive noise on the salted and unsalted ciphertexts. We added random noise with increasing amplitude and we calculated the correlation coefficient between the decrypted object from the unsalted ciphertext without additive noise compared with the decrypted data obtained from the salted and unsalted ciphertext with additive noise.

In figure 4, we show that the resistance to additive noise remains roughly the same for salted and unsalted ciphertexts. The results of figures 3 and 4 demonstrate that salting can be implemented without altering the robustness of DRPE ciphertexts.

5. Resistance to attacks

We will now discuss the effects salting has on some of the most widely reported attacks against the DRPE systems. The

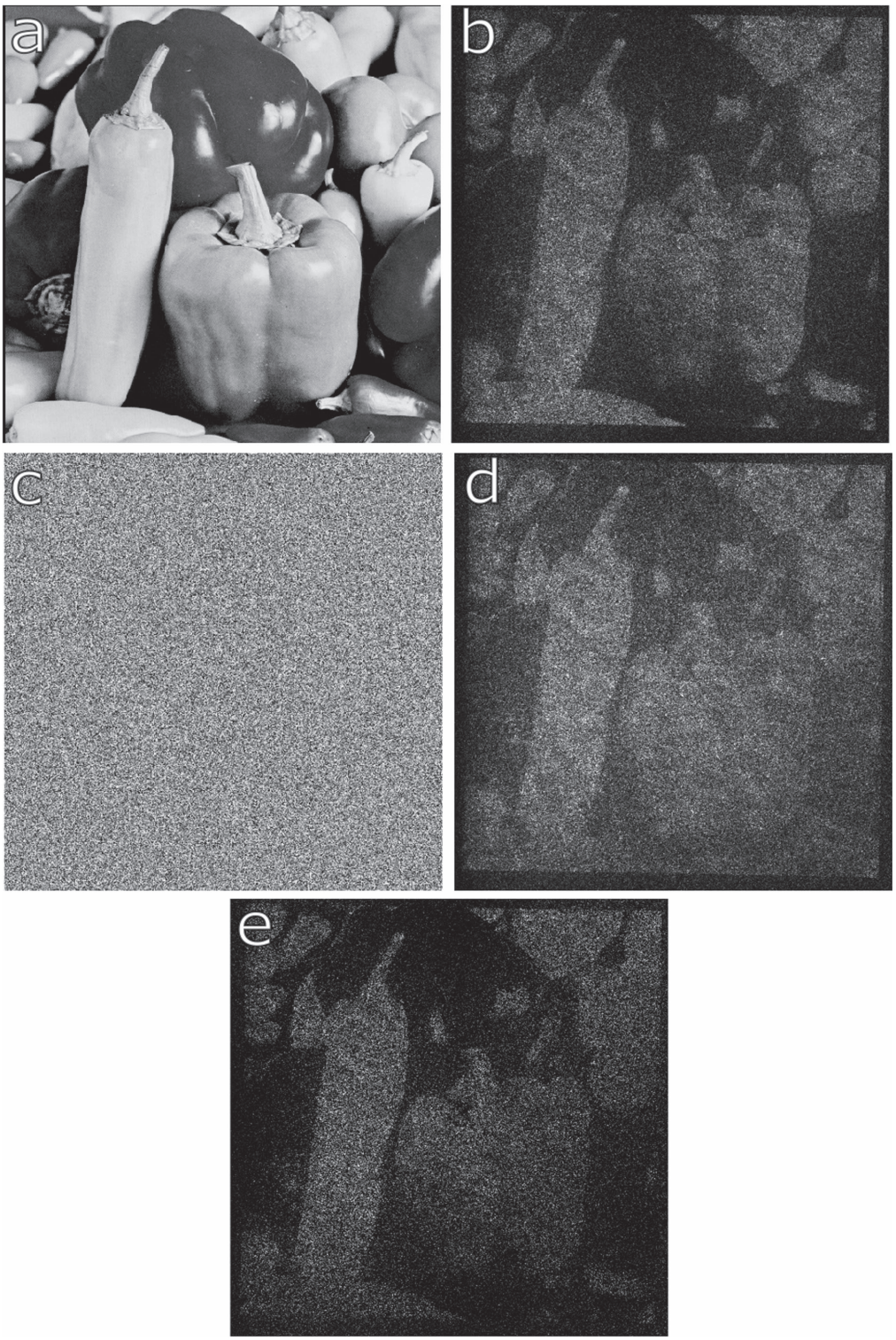

Figure 2. Decrypted data from salted ciphertext: (a) input plaintext, (b) decrypted object without salt, (c) salt plaintext, (d) decryption result from salted ciphertext and (e) decryption result from salted ciphertext after subtraction of the salt plaintext.

most basic attack against the JTC cryptosystem is the Dirac delta attack or impulse attack. This is a CPA where the attacker uses the cryptosystem to encrypt a Dirac delta. The resulting ciphertext is then

$$e_{\mathrm{cpa}}(x, y) = [\delta(x, y)r(x, y)] \otimes k^{*}(x, y) \tag{6}$$

which is the conjugate of the encryption key with a constant phase. If we continue to consider an ideal simulated setup, when our ciphertext is now salted, we obtain

$$e_{\mathrm{scpa}}(x, y) = [\delta(x, y)r(x, y)] \otimes k^{*}(x, y) + [s(x, y)r(x, y)] \otimes k^{*}(x, y). \tag{7}$$

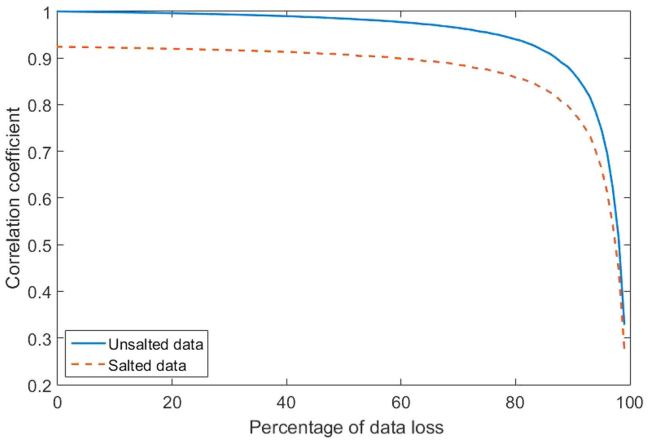

Figure 3. Correlation coefficient of the decrypted data from salted and unsalted ciphertext after data loss.

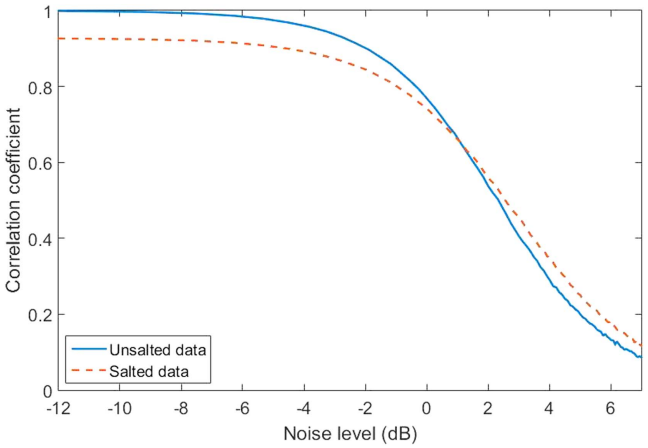

Figure 4. Correlation coefficient of the decrypted data from salted and unsalted ciphertext after adding random noise.

If we can guarantee that the salted function overlaps the key (the support of $s(x, y)$ is larger than the support of $k(x, y)$), it is not possible to separate the salted ciphertext from the key information.

This attack is difficult to accomplish in an experimental setup, where an attacker would only be able to encrypt an aperture with a finite size, not an ideal Dirac delta. Furthermore, the key is contained in the JPS, which is an interference pattern. This means that the amount of light coming from the finite aperture must be similar than the amount of light coming from the key window to ensure adequate fringe visibility.

Due to these difficulties, we tested the resistance of the salted ciphertext to this attack by using a virtual optical system. The object and key windows had a size of 4.096 by 4.096 mm. The simulated lens focal length was 200 mm and coherent illumination with a wavelength of 532 nm was considered.

In figure 5, we can see the result of attempting to use the Dirac delta attack on a JTC system without salting (figure 5(a)) and with salting (figure 5(b)). As expected from equation (7), the presence of the salt ciphertext obfuscates the key information, enhancing the security of the system.

Another possible attack is the KPA. The working assumption is that the attacker has access to one or more plaintexts and their respective ciphertexts.

If we take the FT of the unsalted ciphertext in equation (2) we obtain

$$E(v, w) = [O(v, w) \otimes R(v, w)]K^*(v, w), \tag{8}$$

where $O(v, w)$ and $R(v, w)$ are the FTs of the object $o(x, y)$ and phase mask $r(x, y)$, respectively. Taking the intensity of equation (2), and assuming $K(v, w)$ as a phase only function, we obtain

$$|E(v, w)|^2 = |FT\{o(x, y)r(x, y)\}|^2. \tag{9}$$

From equation (8), we can conclude that if the attacker knows $o(x, y)$, and since the plaintext is taken to be an amplitude only distribution, he/she can apply the Gerchberg–Saxton algorithm to recover the missing phase, which will correspond to $r(x, y)$. Once the intruder is in possession of this phase, the encryption key can be estimated by solving

$$K(v, w) = \frac{E(v, w)}{FT\{o(x, y)r(x, y)\}}. \tag{10}$$

If we attempt this attack on the salted ciphertext of equation (3), we obtain, after the IFT

$$\begin{aligned} E_s(v, w) = {} & [O(v, w) \otimes R(v, w)]K^*(v, w) \\ & + [S(v, w) \otimes R(v, w)]K^*(v, w). \end{aligned} \tag{11}$$

Taking the intensity of equation (11)

$$\begin{aligned} |E_s(v, w)|^2 = {} & |[O(v, w) \otimes R(v, w)]|^2 \\ & + |[S(v, w) \otimes R(v, w)]|^2 \\ & + [S(v, w) \otimes R(v, w)]^* \\ & \times [O(v, w) \otimes R(v, w)] \\ & + [S(v, w) \otimes R(v, w)] \\ & \times [O(v, w) \otimes R(v, w)]^*. \end{aligned} \tag{12}$$

The first term of equation (12) is the intensity of the FT of the object window, which is the relevant data necessary to successfully retrieve the key using this KPA. This information, however, suffers cross talk from the remaining terms of equation (12), which appears due to the addition of the salt ciphertext. This cross talk ensures that a phase retrieval algorithm fails unless the attacker has access to additional data, like the salt ciphertext, which should not be available to any user. The salt should be changed in each run of the encrypting system to maintain security. Additional protection is achieved if the salt is encrypted with different masks.

The last attacks reported are the COA. These work by taking the amplitude retrieved in equation (9) and performing a phase retrieval algorithm without knowledge of the plaintext, like the hybrid input–output algorithm. To achieve convergence of the solution, the attacker makes use of assumptions about the encrypted object, for example, that

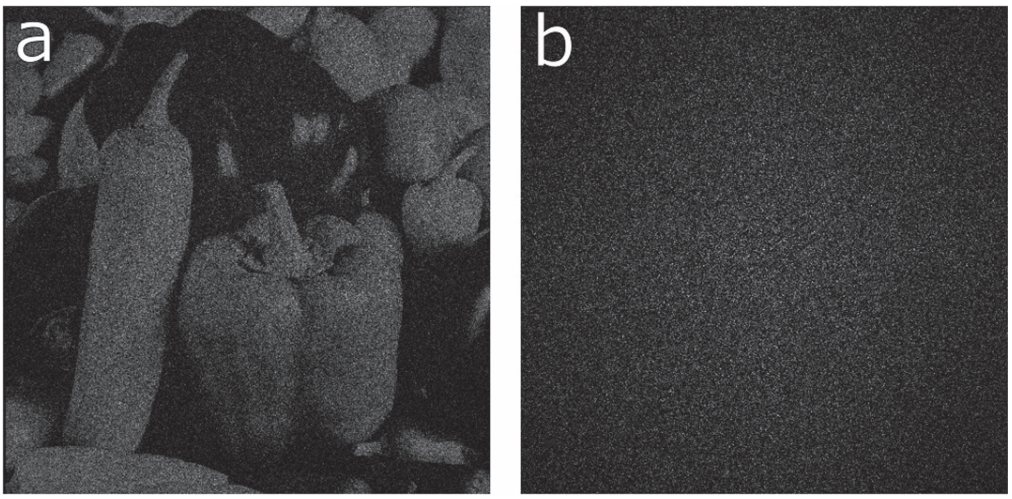

Figure 5. (a) Decrypted data using a key retrieved by a Dirac delta attack, (b) the same data decrypted using the result of a Dirac delta attack on a cryptosystem with salting.

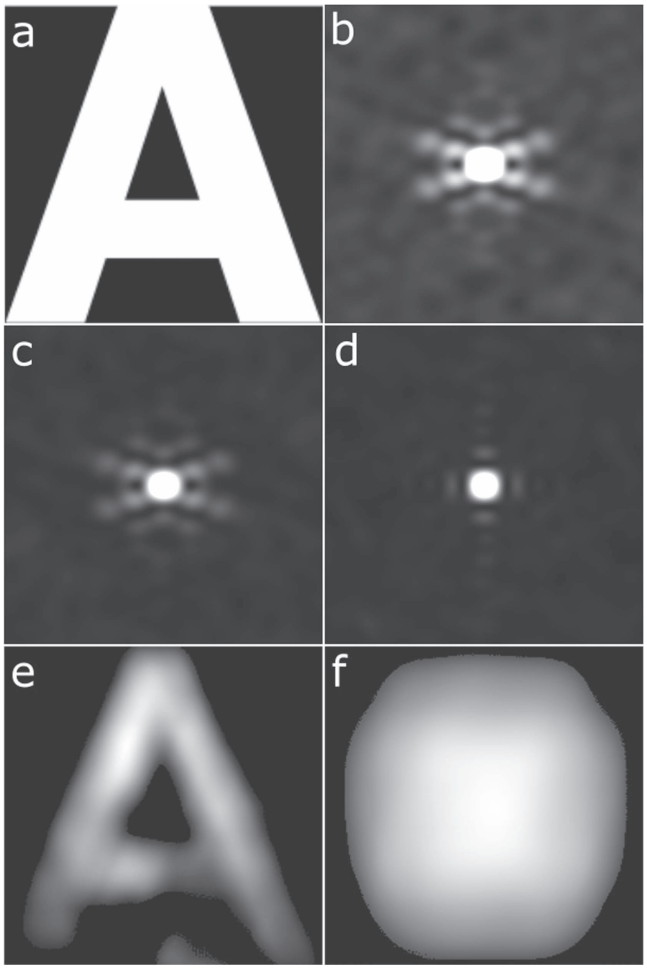

Figure 6. Demonstration of COA on a salted and unsalted ciphertext. (a) Input plaintext, (b) autocorrelation of the object window, (c) autocorrelation of the unsalted ciphertext, (d) autocorrelation of the salted ciphertext, (e) result of COA against the unsalted ciphertext and (f) result of COA against the salted ciphertext.

$o(x, y)$ is an amplitude only object, that its support is well known or the number of non-zero pixels in the plaintext [13].

From equation (12), we see that the amplitude of the FT of the object cannot be retrieved from the salted ciphertext, making unfeasible some of the known COA with phase retrieval.

The autocorrelation of the ciphertext speckle pattern contains information about the energy spectral distribution (ESD). Some approaches to COA take advantage of this fact to retrieve the plaintext. This approach has been used in imaging through turbid media [21] and in experimental implementations of COA attacks [15, 16].

In figure 6, we show the results of a COA attack on the ciphertext of the letter A before and after salting with a random amplitude mask. First, we calculate the autocorrelation of the unsalted (figure 6(c)) and salted ciphertext (figure 6(d)). The autocorrelation of the object window is show in figure 6(b) for comparison. We note that the ESD of the ciphertext is almost equal to the ESD of the object window, while the ESD obtained with the salted ciphertext is quite different. We attempted COA by using a hybrid input–output algorithm with the autocorrelations of figures 6(c) and (d). We assumed that the number of non-zero pixels and the support of the plaintext is known to the attacker. With this information, the COA is successful against the unsalted ciphertext, as shown in figure 6(e). However, the attack fails against the salted ciphertext (figure 6(f)).

6. Conclusions

Cryptographic salting can be applied to any DRPE scheme, even though our demonstration deals with the JTC cryptosystem. In a salting cryptosystem, the end user would know the encryption key, the salted ciphertext and potentially the salt plain text. In an ideal setup, the salt ciphertext and the unsalted ciphertext are never known to any party, neither the sender nor the receiver, and the salt is changed each time the system encrypts a new data to maintain security.

Our proposal can be modified by multiplexing the salt and object ciphertext with other methods rather than by direct summation. By demonstrating a method to increase the security of the DRPE systems, this proposal opens a new avenue of research for the cryptanalysis of optical security systems, and invites the possibility of developing methods to attack multiplexed packages which may be used in actual real-world implementations of optical encryption.

Acknowledgments

This research was performed under grants from Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), CONICET Nos. 0849/16 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I215 (Argentina). John Fredy Barrera Ramírez acknowledges the support from the International Centre for Theoretical Physics ICTP Associateship Scheme.

ORCID iDs

Alejandro Velez Zea https://orcid.org/0000-0001-7525-9541

References

[1] Refregier P and Javidi B 2015 Optical image encryption based on input plane and Fourier plane random encoding *Opt. Lett.* **20** 767–9
[2] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Photon.* **6** 120–55
[3] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001
[4] Velez A, Barrera J F and Torroba R 2017 Innovative speckle noise reduction procedure in optical encryption *J. Opt.* **19** 055704
[5] Frauel Y, Castro A, Naughton T J and Javidi B 2007 Resistance of the double random phase encryption against various attacks *Opt. Express* **15** 10253–65
[6] Carnicer A, Montes-Usategui M, Arcos S and Juvells I 2005 Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys *Opt. Lett.* **30** 1644–6
[7] Vilardy J M, Millán M S and Perez-Cabré E 2013 Improved decryption quality and security of a joint transform correlator-based encryption system *J. Opt.* **15** 025401
[8] Falaggis K, Ramírez A A H, Gaxiola L J G, Gutierrez Ojeda C and Porras-Aguilar R 2016 Optical encryption with protection against Dirac delta and plain signal attacks *Opt. Lett.* **41** 4787–90
[9] Peng X, Zhang P, Wei H and Yu B 2006 Known-plaintext attack on optical encryption based on double random phase keys *Opt. Lett.* **31** 1044–6
[10] Barrera J F, Vargas C, Tebaldi M, Torroba R and Bolognini N 2010 Known-plaintext attack on a joint transform correlator encrypting system *Opt. Lett.* **35** 3553–5
[11] Tashima H, Takeda M, Suzuki H, Obi T, Yamaguchi M and Ohyama N 2010 Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack *Opt. Express* **18** 13772–81
[12] Zhang C, Liao M, He W and Peng X 2013 Ciphertext-only attack on a joint transform correlator encryption system *Opt. Express* **21** 28523–30
[13] Liu X, Wu J, He W, Liao M, Zhang C and Peng X 2015 Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding *Opt. Express* **23** 18955–68
[14] Guo C, Muniraj I and Sheridan J T 2016 Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems *Appl. Opt.* **55** 4720–8
[15] Liao M, He W, Lu D and Peng X 2017 Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium *Sci. Rep.* **7** 41789
[16] Li G, Yang W, Li D and Situ G 2017 Cyphertext-only attack on the double random-phase encryption: experimental demonstration *Opt. Express* **25** 8690–7
[17] Morris R and Thompson K 1979 Password security: a case history *Commun. ACM* **22** 594–7
[18] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture *Opt. Eng.* **39** 2031–5
[19] Rueda E, Barrera J F, Henao R and Torroba R 2009 Optical encryption with a reference wave in a joint transform correlator architecture *Opt. Commun.* **282** 3243–9
[20] Schnars U and Jueptner W 2005 *Digital Holography: Digital Hologram Recording, Numerical Reconstruction, and Related Techniques* 1st edn (Berlin: Springer)
[21] Katz O, Heiddman P, Fink M and Gigan S 2014 Non-invasive single-shot imaging through scattering layers and around corners via speckle correlations *Nat. Photon.* **8** 784–90