Supplemental Document

Optics Letters

# Non-interferometric key recording applied to a joint transform cryptosystem: supplement

**CARLOS VARGAS-CASTRILLÓN,* ALEJANDRO VELEZ-ZEA, AND JOHN FREDY BARRERA-RAMÍREZ**

*Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226 Medellín, Colombia*
**Corresponding author: andres.vargas@udea.edu.co*



Supplement DOI: https://doi.org/10.6084/m9.figshare.21766460

Parent Article DOI: https://doi.org/10.1364/OL.478132

# Supplemental document

## 1. Robustness of the recovered key against random occlusion effects and additive noise

After the key is retrieved, it is then sent to the authorized user using existing communication channels, where the information can be lost or affected by noise. In this supplement, we analyze the effects of random occlusion and additive noise that could be added during the transmission to the encrypted object.

### 1.1 Random occlusion effects

The occlusion effects are examined by randomly covering part of the encrypted object, this corresponds to a possible pixel lost during the transmission. We randomly change a portion of the encrypted object pixels to a zero value. Fig. S1 shows the 2D correlation coefficient of the decrypted object as a function of the percentage of changed pixels for the numerical results, considering the arbitrary object [Figs. 3(b) and 3(d) in the paper]. The behavior between the original key and the retrieved one using the proposed algorithm is the same.

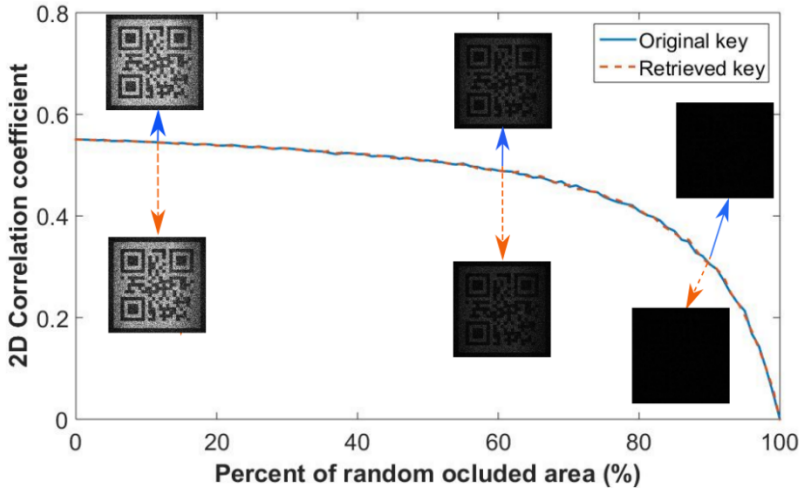



Fig. S1. 2D correlation coefficient vs occlusion area of the encrypted object considering the numerical results. The indent images correspond to a 10%, 60% and 90% of random occlusion.

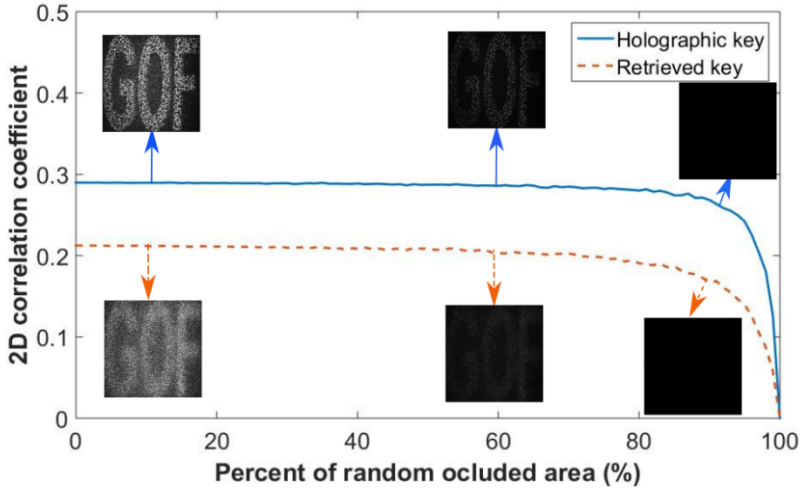



Fig. S2. 2D correlation coefficient vs occlusion area of the encrypted object considering the experimental results. The indent images correspond to a 10%, 60% and 90% of random occlusion.

Same analysis was made on the experimental data, as shown in Fig. S2 considering the arbitrary object [Figs. 4(b) and 4(d)

in the paper]. The behavior using the retrieved key is compared with one obtained using the holographic method is similar. However, the decrypted object using the retrieved key has lower quality and the initial value of the 2D correlation coefficient is smaller (0.21) compared with the decrypted one using the holographic key (0.28). The low intensity of the indent images in Figures S1 and S2 for high occlusion area percentages is due to the energy lost. This demonstrates the high tolerance to random loss, caused by the redundancy present in holographic recordings.

### 1.2 Additive noise effects

In this analysis, we added random noise to the encrypted object using the equation

$$E_n(u,v) = E(u,v) + A_n \exp\left[2\pi i \alpha(u,v)\right], \tag{S1}$$

where $E(u,v)$ is the original signal, $E_n(u,v)$ is the signal after adding the noise, $A_n$ is the noise amplitude and $\alpha(u,v)$ is a random phase. The noise is measured in dB as

$$R_n = (20dB)\log\left(\frac{A_n}{E_{\max}}\right), \tag{S2}$$

where $E_{\max}$ is the maximum amplitude of the original signal. Fig. S3 displays the effect of different additive random noise amplitude over the quality of the decrypted object when noise with different amplitude is added, considering the numerical results for the arbitrary object [see Figs. 3(a) and 3(d) in the paper].

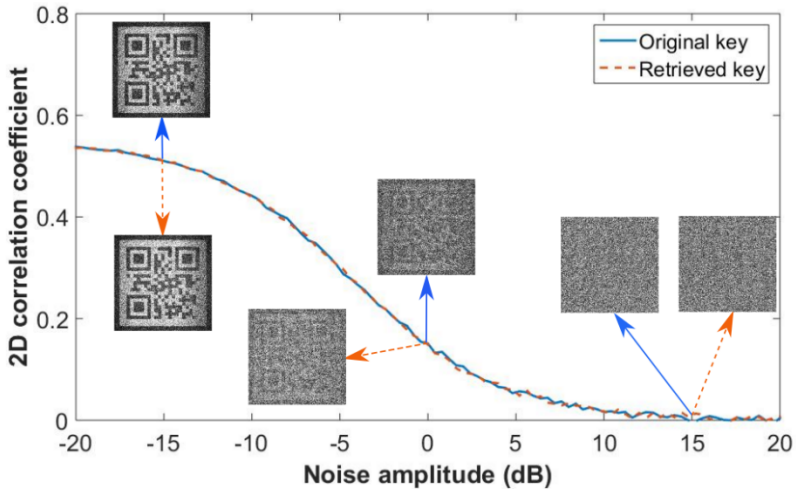



Fig. S3. 2D correlation coefficient vs amplitude noise added to the encrypted object considering the numerical results. The indent images correspond to a -15 dB, 0 dB and 15 dB of additive noise amplitude.

Fig. S4 shows the same analysis applied to the experimental arbitrary object [see Figs. 4(a) and 4(d) in the paper]. Again, the behavior between the holographic and the recovered keys are similar, with exception of the starting value. In the numerical and experimental situations, the 2D correlation coefficient is mostly constant when the random noise amplitude is in the range of -20dB to -10 dB. This indicates that there is minor degradation over the decrypted data. However, if the noise amplitude is greater than -10 dB, the 2D correlation coefficient values decrease and the quality of the decrypted object degrades considerably.

Finally, we can conclude that the retrieved key has similar behavior as the original key when the encrypted objet is subjected to random occlusion or additive noise effects; validating the robustness of the key obtained using the proposed method.

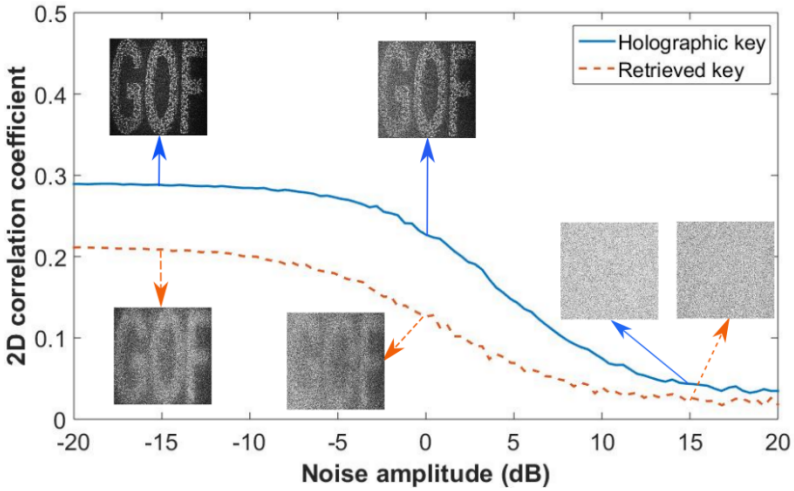
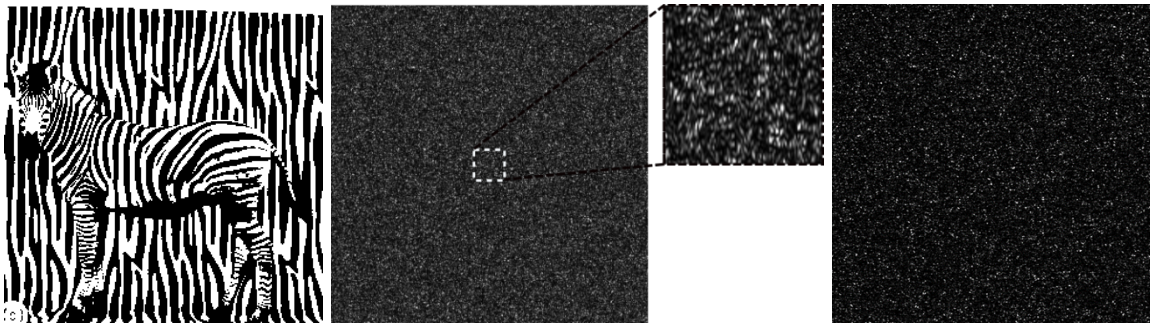



Fig. S4. 2D correlation coefficient vs amplitude noise added to the encrypted object considering the experimental results. The indent images correspond to a -15 dB, 0 dB and 15 dB of additive noise amplitude.

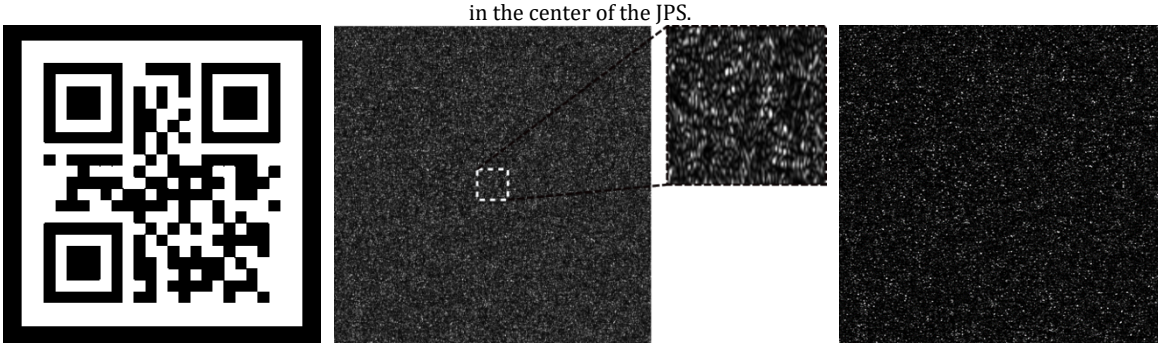
## 2. Joint power spectrums and cypher-texts of the objects used in the paper.

In this section, we show for each object used in the manuscript its JPS and its encrypted pair (cypher-text) to complement the information presented there. For the object in Fig. 3(a) of the paper this information is shown in Fig. S5, for the object in Fig. 3(b) of the paper is shown in Fig. S6, for the object in Fig. 4(a) of the paper is shown in Fig. S7, and for the object in Fig. 4(b) of the paper is shown in Fig. S8. All the figures include the respective object.



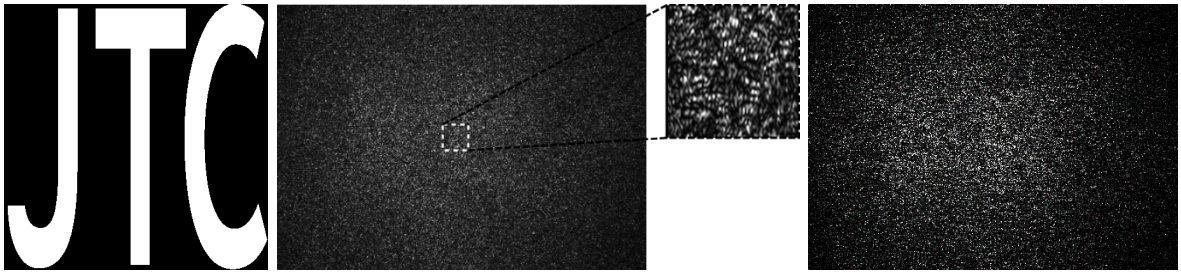
(a) (b) (c)

Fig. S5. (a) Object used in Fig. 3(b), (b) its JPS, and (c) its cypher-text pair. The indent in (b) illustrates interference fringes in the center of the JPS.



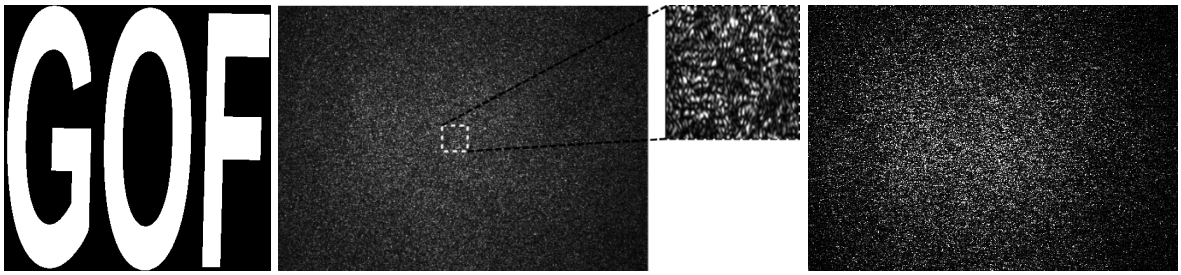
(a) (b) (c)

Fig. S6. (a) Object used in Fig. 3(b), (b) its JPS, and (c) its cypher-text pair. The indent in (b) illustrates interference fringes in the center of the JPS.



(a) (b) (c)

Fig. S7. (a) Object used in Fig. 4(a), (b) its JPS, and (c) its cypher-text pair.



(a) (b) (c)

Fig. S8. (a) Object used in Fig. 4(a), (b) its JPS, and (c) its cypher-text pair.