# A Dual Encryption Scheme of Images Using Polarized Light

Ayman Alfalou, C. Brosseau

# A Dual Encryption Scheme of Images Using Polarized Light

**A. Alfalou[1,*] and C. Brosseau[2]**

[1] *Département Optoélectronique, Laboratory L@BISEN, ISEN-BREST, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France*

[2] *Université Européenne de Bretagne, Université de Brest, Lab-STICC and Département de Physique, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France*

**Corresponding author:ayman.al-falou@isen.fr*

Motivated by recent interest in polarization encoding, we propose and analyze a dual encryption/decryption scheme. Compared to standard optical encryption methods which are based on phase and amplitude manipulation, this encryption procedure relying on Mueller-Stokes formalism provides a large flexibility in the key encryption design. The effectiveness of our algorithm is discussed thanks to a numerical simulation of the polarization encryption/decryption procedure of a 256 gray-level image. Of additional special interest is the immunity of this encryption algorithm to brute force attacks.

*OCIS codes:* 100.2960, 260.5430, 100.3010, 110.2960

The development of advanced coding methods is an extremely active research area of great visibility and importance (see for a recent review [1]). In particular, much effort has been devoted to searching for new types of encryption methods which can be implemented in an optical setup [2-5]. These efforts are aimed at combining the excellent control possible with spatial light modulators, with the miniaturization, parallelism, and integrability of optical devices. Despite their efficiency, many processing techniques remain uneasy to be implemented using optical techniques, can lead to complex-valued encoded images, and can be potentially insecure against attacks.

On the other hand, the interplay between encryption and polarization has piqued the interest of optical physicists for several decades [6-11]. Since the early work of Dolfuss and co-workers [6] dealing with polarization imaging, several polarization encryption methods were considered (see [3-4,8-9] and references therein).

In this Letter, we propose an alternative scheme. The method is based on Mueller-Stokes formalism and serves as a good starting point toward ultimate understanding of secure transmission of optical images using polarization encoding. The Letter is organized as follows: the principle of the polarization algorithm is first described. Next, we shall illustrate the effectiveness of this approach by working out an example of a 256 gray-level image. We further test the strength of this encryption algorithm against unauthorized decryption.

Some preliminary notation is in order. Let us consider a narrow band stochastic field which can be represented by an ensemble of realizations, which we shall assume to be statistically stationary, at least in the wide sense. Each realization of the fluctuating electric field vector is represented by a complex analytic signal. The four Stokes parameters, $S_j$, defined as the covariances of the analytic signal components, are the observables of the field vector at optical frequencies [12-13]. Let $\boldsymbol{S} = \left(S_0 \quad S_1 \quad S_2 \quad S_3\right)^T$, where $T$ means the transpose, denote the Stokes vector and $\boldsymbol{M}$ is the Mueller matrix of a polarization element. Let the input

and the output states of polarization parametrized by the Stokes vector $\boldsymbol{S}$ and $\boldsymbol{S}$'. We assume that the matrix $\boldsymbol{M}$ acts on the input state $\boldsymbol{S}$ by matrix multiplication to give the output state $\boldsymbol{S}' = \boldsymbol{MS}$, where $\boldsymbol{M}$ is a $4\times 4$ matrix with real elements $m_{\mathrm{ij}}$ that characterize the interaction of the light with the optical element. To illustrate these formulas, let us consider the problem of characterizing the state of polarization at the output of the cascaded polarization elements- linear polarizer, wave plate retarder- displayed in Fig. 1. It is convenient for us to define the product of the Mueller matrix of a linear polarizer $\boldsymbol{M}_{pol}(\varphi)$ and that of a retarder $\boldsymbol{M}_{ret}(\theta)$, where $\varphi$ is a polarization angle and $\theta$ is a phase shift

$$\boldsymbol{M}^{pr}(\varphi,\theta) = \boldsymbol{M}_{pol}(\varphi)\boldsymbol{M}_{ret}(\theta) =$$
$$\frac{1}{2}\begin{pmatrix} 1 & \cos(2\varphi) & \sin(2\varphi) & 0 \\ \cos(2\varphi) & \cos^2(2\varphi) & \cos(2\varphi)\sin(2\varphi) & 0 \\ \sin(2\varphi) & \cos(2\varphi)\sin(2\varphi) & \sin^2(2\varphi) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\theta) & \cos(2\theta)\sin(2\theta) & -\sin(2\theta) \\ 0 & \cos(2\theta)\sin(2\theta) & \sin^2(2\theta) & \cos(2\theta) \\ 0 & \sin(2\theta) & -\cos(2\theta) & 0 \end{pmatrix},$$
$$= \begin{pmatrix} m_{00}^{pr} & m_{01}^{pr} & m_{02}^{pr} & m_{03}^{pr} \\ m_{10}^{pr} & m_{11}^{pr} & m_{12}^{pr} & m_{03}^{pr} \\ m_{20}^{pr} & m_{21}^{pr} & m_{22}^{pr} & m_{03}^{pr} \\ m_{30}^{pr} & m_{31}^{pr} & m_{32}^{pr} & m_{33}^{pr} \end{pmatrix} \tag{1}$$

We find for the right-hand side of Eq. (1): $m_{00}^{pr} = \frac{1}{2}$, $m_{01}^{pr} = \frac{1}{2}\left(\cos(2\varphi)\cos^2(2\theta) + \sin(2\varphi)\cos(2\theta)\sin(2\theta)\right)$, $m_{03}^{pr} = m_{13}^{pr} = m_{23}^{pr} = m_{33}^{pr} = 0$, etc. The state of polarization of the output signal is completely determined by the nominal values of $\theta$ and $\varphi$. This optical system functions as a polarization encoder, encoding the pixels of the signal (image) by $\theta$ and $\varphi$.

The basis of the experiment is depicted schematically in Fig. 2. The concept is first demonstrated quantitatively using the Mueller-Stokes formalism. Consider first the partially

polarized wave $\boldsymbol{S}_I = \begin{pmatrix} S_{I0} & S_{I1} & S_{I2} & S_{I3} \end{pmatrix}^T$ incident on the object to be encrypted (target image *I*). The state of polarization is determined by the configuration of the polarization elements shown in Fig. 1. Using Eq. (1), one finds that the output Stokes vector is

$$S_I^{'} = \begin{pmatrix} S_{I0}^{'} \\ S_{I1}^{'} \\ S_{I2}^{'} \\ S_{I3}^{'} \end{pmatrix} = \begin{pmatrix} m_{00}^{pr} S_{I0} + m_{01}^{pr} S_{I1} + m_{02}^{pr} S_{I2} + m_{03}^{pr} S_{I3} \\ m_{10}^{pr} S_{I0} + m_{11}^{pr} S_{I1} + m_{12}^{pr} S_{I2} + m_{13}^{pr} S_{I3} \\ m_{20}^{pr} S_{I0} + m_{21}^{pr} S_{I1} + m_{22}^{pr} S_{I2} + m_{23}^{pr} S_{I3} \\ 0 \end{pmatrix}. \tag{2}$$

Analogously, an encryption wave is sent to a key image *k* $\boldsymbol{S}_k = \begin{pmatrix} S_{k0} & S_{k1} & S_{k2} & S_{k3} \end{pmatrix}^T$. A gray-level image with $256 \times 256$ pixels randomly distributed in the range $[0-255]$ will be considered next for illustrative purpose. Then, the wave is passed through the similar set of polarization elements shown in Fig. 1. The output signal (image) is $S_k^{'}$. For the current discussion we will consider only the simplest situation of unpolarized signals, i.e. $\boldsymbol{S}_I = \begin{pmatrix} S_{I0} & 0 & 0 & 0 \end{pmatrix}^T$, $\boldsymbol{S}_k = \begin{pmatrix} S_{k0} & 0 & 0 & 0 \end{pmatrix}^T$. A more comprehensive treatment would consider nonzero values of the other Stokes parameters. We set $\varphi_1 = \varphi_2 = 0$ and $\theta_1 = \theta_2 = \pi/2$, where $\varphi_1$ and $\varphi_2$ denote the polarization angles of Pol(1) and Pol(2), and $\theta_1$ and $\theta_2$ are the phase shifts of Ret(1) and Ret(2), respectively. Hence $\boldsymbol{S}_I^{'} = \begin{pmatrix} S_{I0}^{'} & S_{I1}^{'} & S_{I2}^{'} & S_{I3}^{'} \end{pmatrix}^T = \frac{1}{2}\begin{pmatrix} S_{I0} & S_{I0} & 0 & 0 \end{pmatrix}^T$ and $\boldsymbol{S}_k^{'} = \begin{pmatrix} S_{k0}^{'} & S_{k1}^{'} & S_{k2}^{'} & S_{k3}^{'} \end{pmatrix}^T = \frac{1}{2}\begin{pmatrix} S_{k0} & S_{k0} & 0 & 0 \end{pmatrix}^T$. Fig. 2 shows that the two output signals are multiplexed using a beam-splitter. Accordingly, the resulting signal is $\boldsymbol{S}_R^{'} = \boldsymbol{S}_I^{'} + \boldsymbol{S}_k^{'} = \frac{1}{2}\begin{pmatrix} S_{I0} + S_{k0} & S_{I0} + S_{k0} & 0 & 0 \end{pmatrix}^T$. Fig. 2 shows also the transformation of this image to a new polarization state via a matrix of linear polarizers (Pol(3); each of them is characterized by angle the randomly chosen angle $\varphi_{rand} = \pi rand$ in the range [-π,π]. Consequently, each pixel of the encrypted image is given by $I_C^{'}(i, j)$

$$
\begin{aligned}
\boldsymbol{I}_C^{'}(i,j) &= \begin{pmatrix} I_{C0}^{'}(i,j) \\ I_{C1}^{'}(i,j) \\ I_{C2}^{'}(i,j) \\ I_{C3}^{'}(i,j) \end{pmatrix} = \boldsymbol{M}_{Pol}\left(\varphi_{rand}^{i,j}\right)\boldsymbol{S}_R^{'}(i,j) \\
&= \frac{1}{2}\begin{pmatrix} 1 & \cos\left(2\varphi_{rand}^{i,j}\right) & \sin\left(2\varphi_{rand}^{i,j}\right) & 0 \\ \cos\left(2\varphi_{rand}^{i,j}\right) & \cos^2\left(2\varphi_{rand}^{i,j}\right) & \cos\left(2\varphi_{rand}^{i,j}\right)\sin\left(2\varphi_{rand}^{i,j}\right) & 0 \\ \sin\left(2\varphi_{rand}^{i,j}\right) & \cos\left(2\varphi_{rand}^{i,j}\right)\sin\left(2\varphi_{rand}^{i,j}\right) & \sin^2\left(2\varphi_{rand}^{i,j}\right) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\frac{1}{2}\begin{pmatrix} S_{I0}(i,j)+S_{k0}(i,j) \\ S_{I0}(i,j)+S_{k0}(i,j) \\ 0 \\ 0 \end{pmatrix} \\
&= \frac{1}{4}\left[S_{I0}(i,j)+S_{k0}(i,j)\right]\begin{pmatrix} 1+\cos\left(2\varphi_{rand}^{i,j}\right) \\ \cos\left(2\varphi_{rand}^{i,j}\right)+\cos^2\left(2\varphi_{rand}^{i,j}\right) \\ \sin\left(2\varphi_{rand}^{i,j}\right)\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right) \\ 0 \end{pmatrix},
\end{aligned}
\tag{3}
$$

The measured intensity of the encrypted image, stored with a CCD camera (Fig. 2), in this case is given by

$$
I_C(i,j) = I_{C0}^{'}(i,j) = \frac{1}{4}\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right)\left[S_{I0}(i,j)+S_{k0}(i,j)\right]. \tag{4}
$$

Two important points should be considered when interpreting the images. First, we remark that only real numbers, i.e. Eq. (4), are considered since we used the Mueller matrix formalism. This is at odds with the standard encoding methods, e.g. the double-random phase encryption technique, which transform the input image into a complex-amplitude stationary white noise [2]. Second, the decryption method is a two-step process. On the one hand, the encrypted signal is passed through a linear polarizer $\mathrm{Pol}_{\mathrm{decry}}(4)$ whose polarization angle is oriented such that the term $\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right)$ in Eq. (4) vanishes. At the output of $\mathrm{Pol}_{\mathrm{decry}}(4)$ the Stokes vector is

$$I_{decry}(i,j) = M_{pol\_decry}\begin{pmatrix} \frac{1}{4}\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right)\left[S_{I0}(i,j)+S_{k0}(i,j)\right] \\ 0 \\ 0 \\ 0 \end{pmatrix}$$
$$= \frac{1}{8}\left[S_{I0}(i,j)+S_{k0}(i,j)\right]\begin{pmatrix} \left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right) \\ \cos\left(2\varphi_{decry}^{i,j}\right)\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right) \\ \sin\left(2\varphi_{decry}^{i,j}\right)\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right) \\ 0 \end{pmatrix} = \begin{pmatrix} S_{0\_decryp}^{'} \\ S_{1\_decryp}^{'} \\ S_{2\_decryp}^{'} \\ S_{3\_decryp}^{'} \end{pmatrix} \quad (5)$$

From Eq. (5) it is clear that the image, $(S_{0\_decryp}^{'})$, is still encrypted. The decryption process can be implemented by extracting one particular component of the relevant Stokes vector, Eq. (5). Here, $S_{1\_decryp}^{'} = \frac{1}{8}\cos\left(2\varphi_{decry}^{i,j}\right)\left\{\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right)\left[S_{I0}(i,j)+S_{k0}(i,j)\right]\right\}$ was used, and the decryption polarization angles $\varphi_{decry}^{i,j}$ are designed such that the polarization angles of the encryption polarizer Pol3 satisfy $\left|1+\cos\left(2\varphi_{rand}^{i,j}\right)\right|^{-1} < 1$, i.e. $\varphi_{rand}^{i,j}$ must be chosen between $-\pi/4$ and $\pi/4$, such that $\cos\left(2\varphi_{decry}^{i,j}\right)\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right) = 1$. Lastly, the encryption key $S_{k0}$ is removed to return to the primary image.

The encryption procedure described above is quite general and can be implemented both optically and numerically. In order to test our method, we simulated numerically the different steps of this procedure with a 256 gray-level original image (Fig. 3(a)). The results of the simulation for the encrypted (resp. decrypted) images in the aforesaid steps are depicted in Fig. 3 (c) (resp. Fig. 3 (d)). The key image (Fig. 3(b)) is also completely depolarized. It can be seen that the target image is not recognizable. Based on the above described decryption procedure and the knowledge of the two encryption keys (key image and angles of the encrypting polarizers Pol(3)), the target image is clearly observed in Fig 3 (d).

The value of a general and reliable image encryption/decryption algorithm depends on a clear understanding and control of all possible attacks, i.e. plain-text, ciphertext, statistical, and brute force attacks. Here, we argue that our system show an excellent resistance against a specific type of brute force attack. A more extensive analysis will be reported elsewhere. A first example where our results are applicable occurs where the target image has a spatially uniform intensity. From the above derivation, we get $I_C(i,j)=\frac{1}{4}\left(1+\cos\left(2\varphi_{rand}^{i,j}\right)\right)\left[1+S_{k0}(i,j)\right]$, where the $S_{k0}(i,j)$ elements contain the information on the key image and $\varphi_{rand}^{i,j}$ denote the angles of the encrypting polarizers Pol(3). Hence, it is impossible for the attacker to have access either in the key image and in the set of angles of Pol(3).

In a second case, we assume that the attacker has the ability to trick a legitimate user of the system into encrypting images ((s)he knows the key image), has a priori knowledge of the principle of the polarization algorithm, and know the nominal values of the polarization angles of Pol(1) and Pol(2) and also the phase shifts of Ret(1) and Ret(2). For the evaluation of the decryption quality, the mean square error (MSE) was used which can be calculated by $MSE=\frac{1}{N\times N}\sum_{i}^{N}\sum_{j}^{N}\left|S_{1-decryp}^{'}(i,j)-S_{I0}(i,j)\right|^2$. Here $i, j$ label the pixels; $S_{1-decryp}^{'}$ characterizes the output decrypted image (Eq. (5)), and $S_{I0}$ denotes the intensity of the unpolarized input image, respectively. As can be seen from Figs. 3 (e)-(f) we find no significant variation in the magnitude of the *MSE*. This result leads to the conclusion that the attacker is unable to find the target image even after more than 5 $10^5$ trials.

In summary, the numerical results demonstrated that the proposed encryption/decryption procedure of images based on Mueller-Stokes formalism has several interesting features. First of all, it was demonstrated that the polarization algorithm based on a dual encryption scheme is very general. Secondly, we showed that our encryption scheme

remains robust under brute force attacks. All aspects of this scheme can be optically implemented using current state-of-the art technology. We note that, in a real optical implementation, the difficulty to manipulate and measure the involved polarimetric quantities adds some challenges to the attacker. Because these ideas have a broad significance they are also expected to impact related areas demanding secure data.

This work was supported by Lab-STICC which is Unité Mixte de Recherche CNRS 3192.

## References


[1] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods”, Adv. Opt. Photon. **1**, pp. 589-636 (2009).

[2] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, pp. 767-769 (1995).

[3] U. Gopinathan, M. Pohit, and K. Singh, “A polarization encoded optical encryption system using ferroelectric spatial light modulator”, Opt. Commun. **185**, pp. 25-31 (2000).

[4] U. Gopinathan, T. J. Naughton, and J. T. Sheridan, “Polarization encoding and multiplexing of two-dimensional signals: application to image encryption”, Appl. Opt. **45**, pp. 5693-5700 (2006).

[5] A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," Appl. Opt. **48**, pp. 5933-5947 (2009).

[6] A. Dollfus, T. Fauconnier, M. Dreux, P. Boumier, T. Pouchol, and O. Croin, “Video-polarimeter and its applications in physics and telescopic observations”, C. R. Acad. Sci. Paris **308**, Série II, pp. 19-24 (1989).

[7] G. Biener, N. Avi, V. Kleiner, and E. Hasman, “Space-variant polarization scrambling for image encryption obtained with subwavelength gratings,” Opt. Commun. 261, pp. 5-12 (2006).

[8] O Matoba and B. Javidi, “Secure holographic memory by double-random polarization encryption”, Appl. Opt. **38**, pp. 6785-6790 (1999).

[9] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, “Secure optical memory system with polarization encryption”, Appl. Opt. **40**, pp. 2310-2315 (2001).

[10] P. C. Mogesen and J. Glückstad, “A phase-based optical encryption system with polarization encoding”, Opt. Commun. **173**, pp. 177-183 (2000).

[11] M. Richert, X. Orlik, and A. De Martino, "Adapted polarization state contrast image," Opt. Express **17**, pp. 14199-14210 (2009).

[12] C. Brosseau, *Fundamentals of Polarized Light* (Wiley, New York, 1998).

[13] E. Wolf, *Introduction to the Theory of Coherence and Polarization of Light* (Cambridge, University Press, Cambridge, 2007)

## Figure captions

FIG. 1: Schematic of an optical system that encodes a signal in the polarization domain. An input signal (image) is transformed to a gray level value.

FIG. 2: Experimental setup of polarization-encoded encryption system: Target: object to be encrypted; Key: random encrypting key; Ret(1), Ret(2): wave plate retarder; Pol(1), Pol(2), Pol(3): linear polarizers; BS: beamsplitter; M: mirror; CCD: CCD camera.

FIG. 3: Comparison of the different encrypted and decrypted images of the illustrative example chosen to validate our algorithm. (a) The image to be encrypted, (b) the key image, (c) the encrypted image, (d) the decrypted image encrypted with the procedure displayed in Fig. 2, (e) the ciphered image after 500 000 trials, (f) the mean square error (MSE) error as a function of the trial number.

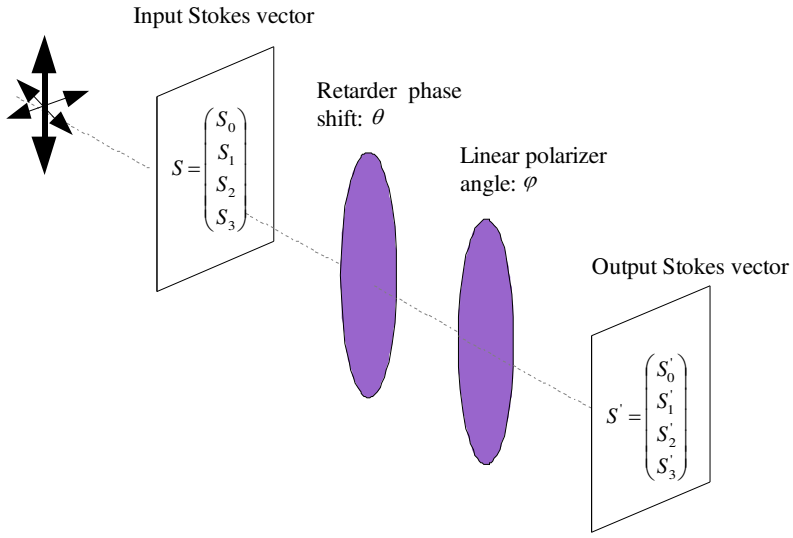


FIG. 1 : Alfalou and Brosseau

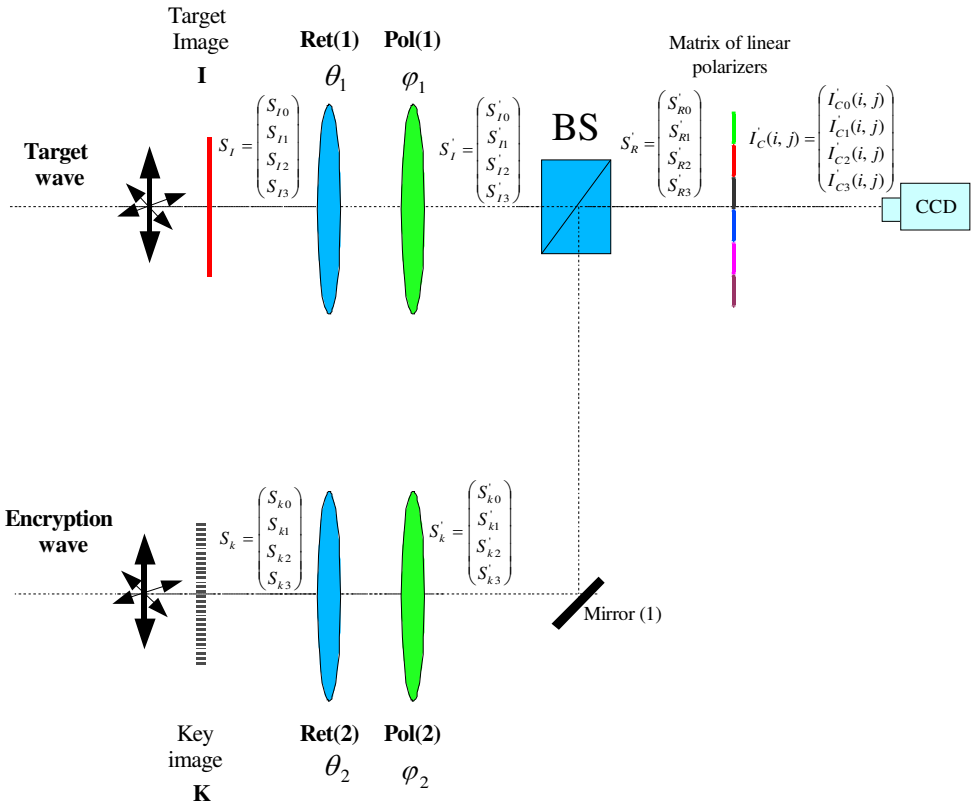


FIG. 2 : Alfalou and Brosseau

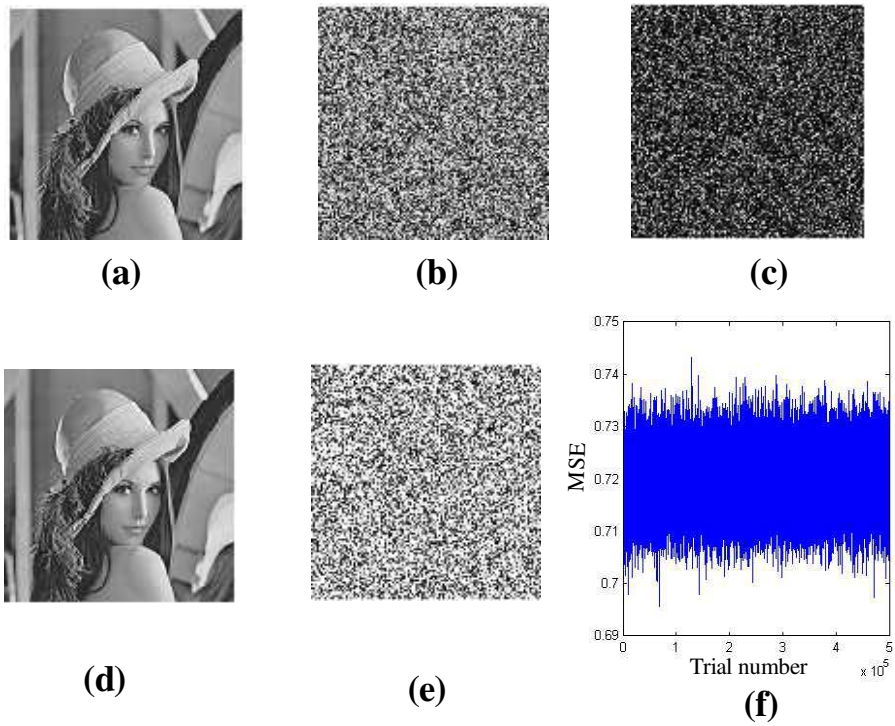


FIG. 3 : Alfalou and Brosseau