Simultaneous verification of optical triple-image encryption using sparse strategy

E. A. Mohammed and H. L. Saadon
Laser Applications Research Group (LARG), Department of Physics, College of Science, University of Basrah, Iraq
*Corresponding author: emadn73@yahoo.com

Abstract. A simultaneous optical triple-image encryption and verification method based on sparse information strategy was proposed. The information of the encoded images could be integrated into a sparse representation. Only sparse (partial) data from the encrypted information were adopted for verification process. In sparse strategy, the partial data was extracted from the encrypted distribution. For complex-valued distribution, the sparse strategy was applied to the amplitude; thus, only the sparse amplitude pixels kept the phase data for verification process. Therefore, the proposed method can effectively facilitate optical information transmission and storage, as only part of the encrypted information was adopted. In addition, the simultaneous encryption and authentication verification of three images was achieved. The results proved that the proposed method was feasible and effective, and can provide an additional security layer for optical security systems. Moreover, the method that demonstrated secure optical triple-image can lead to a high flexibility and variety compared to that of photon counting technique which required a specific device.

1. Introduction
The Optical information processing techniques are presented for data security applications in communication systems and computer technology extensively in the recent years. Due to high speed of parallel processing and multidimensional capabilities, several optical encryption methods have been proposed [1-3]. A considerable work in this filed is the double random phase encoding (DRPE) technique has proposed by Refregier and Javidi [4]. The experimental application of the DRPE has been firstly fulfilled in a 4f system [5]. Other expansions have been developed in the Fresnel [6], Fractional Fourier [7] and gyrator (GT) domains [8]. In addition, the DRPE has been found vulnerable to some attacks, therefore many improvements have been developed to overcome this difficulties [9-13]. However, the technique has been used to encrypt one input image by two random phase masks. In the last years, optical encryption systems have been developed into multiple-image encryption (MIE) owing to economic memory occupation and efficient transmission [14-16]. These developments have been permitted to encrypt multiple images in one encrypted image [8, 17] and also store in optical memory [18].

Recently, double image encryption with quantum imaging or photon-counting has been presented in a single encrypted image [19]. This technique performs security authentication of the data with far fewer photons than conventional techniques. Because the quantum imaging technology does not exit, this
technique is still limited and not widespread. In order to overcome this limitation, double image encryption with sparse representation has integrated for information authentication which permitted to increase the security of the method and reduced data transmission to achieve the requirements of protection, storage [20].

In this paper, a novel information verification which based on optical triple-image encryption with sparse strategy is proposed. The three input images will be firstly encrypted to get one encrypted image with similar spatial resolution as the primary images. In the second step, the sparse technique is applied to the magnitude component of the complex encrypted distribution; consequently, only the sparse amplitude pixels keep the phase information for verification stage. Simultaneous authentication process is presented for triple-image encryption. Therefore, the proposed method will be effective and achievable, and can provide a highly secure optical system.

In what follows, a method of triple image encryption and authentication with sparse strategy will be presented in Section 2. Section 3 describes two numerical simulations, the first one encrypts three images, and the other one verifies the sparse encrypted data. The conclusions are outlined in Section 4.

2. Triple-image encryption and authentication with sparse strategy
The proposed method encrypts three primary images with one random phase mask (RPM) by combined nonlinear joint transform correlator (JTC) and a classical 4f-correlator. A block diagram of the method is shown in figure 1.

Figure 1. Block diagram of the optical triple image encryption and authentication verification with sparse strategy.

The three input images \( O_1(r) \), \( O_2(r) \) and \( O_3(r) \) are first normalized with maxima as 1 and then phase encoded. The functions containing these images are given by the equations:

\[
\begin{align*}
    f_1(r) &= \exp[i\pi O_1(r)], \\
    f_2(r) &= \exp[i\pi O_2(r)], \\
    f_3(r) &= \exp[i\pi O_3(r)].
\end{align*}
\]
where \((r)\) denotes the spatial coordinate in one-dimensional notation and \(f_1(r), f_2(r)\) and \(f_3(r)\) are phase encoded functions. Suppose \(n(r)\) is to be independent random white sequences uses to encrypt the information of the images,

\[
n(r) = \exp(i2\pi \rho(r)),
\]

where \(\rho(x,y)\) is normalized positive function distributed in the range \([0,1]\). The encrypted function \(\psi(r)\) including the triple images and phase mask are depicted as

\[
\psi(r) = \{f_1(r) \cdot f_2(r) \ast f_3(r)\} \ast F^{-1}[n(r)]
\]

where the notation \(\ast\) denotes the convolution operation and \(F^{-1}\) is the inverse Fourier transform. The sparse information is to be generated by randomly selected the sparse encrypted data. The sparse data is applied to the magnitude values of the encrypted image and kept the phase information. The operation could be mathematically expressed as

\[
\psi_{sp}(r) = |\psi(r)|_{sp} \cdot \varphi_{\psi}(r)
\]

In the authentication step, let \(g_1(r), g_2(r)\) and \(g_3(r)\) are the input images. These images are compared to the set of reference images \(f_1(r), f_2(r)\) and \(f_3(r)\), respectively, and let \(n(r)\) is known by this processor.

![Schematic optical setup for the authentication verification process. L is lens; CCD: charge coupled device.](image)

In the verification authentication, a three-step optoelectronic hybrid setup was carried out, as shown in figure 2. First, a JTC technique is applied to the encrypted distribution \(\psi_{sp}(r)\) which is sited side by side with the first input image \(g_1(r)\). The second input image \(g_2(r)\) was put against the screen, where the \(g_1(r)\) was placed. Then, the joint power spectrum \(I(u)\) was recorded by CCD camera in the Fourier plane which can be given by:

\[
I(u) = |FT[\psi(r) + g_1(r)]|^2
\]
where symbol \((u)\) is the spatial frequency coordinate. Secondly, the joint power spectrum \(I(u)\) can be digitally modified by a variety of nonlinear technique to adjust the discrimination capability. Therefore, equation (5) is converted to

\[
NL^\omega[I(u)] = I(u)[I(u)]^{\omega-1},
\]

(6)

where \(\omega\) is the strength of the applied nonlinearity, and it can vary from the linear \((\omega=1)\) to the phase extraction case \((\omega=0)\). Lastly, the third input image \(g_3(r)\) and the phase mask \(n(r)\) are placed in the input plane and the Fourier plane of the 4\(f\)-classical correlator, respectively. Afterward, the resultant nonlinearity of the second step was displayed on the Fourier plane of the 4\(f\)-system. Thus, the output correlation intensity in the recording plane was recorded by a CCD camera and described by [20]

\[
G_3(u) \left[ NL^\omega[I(u)] \right](u),
\]

(7)

where the capital letter function indicates the Fourier transform of the small letter function. Equation (7) will carry the correlation signals and lead to spatially separate the distributions in the output plane. The developments of equation (7) will lead to the term of interest for optical processor corresponds to the cross-correlation of the autocorrelation (AC) signals as follows [20]:

\[
|AC_{POF}[f_2(r)] \otimes AC_{PPC}[f_1(r)f_3(x,y)] \otimes AC_{CMF}[N(r)]|^2
\]

(8)

The symbol \(\otimes\) is the cross correlation, sub-indices CMF (classical matched filter), POF (phase-only filter), and PPC (pure phase correlation) represent the kind of filter contributed in the autocorrelation signal [21]. When the input images and the corresponding reference images are correct \([g_i(r) = f_i(r), g_2(r) = f_2(r) and g_3(r) = f_3(r)]\) and \(\omega=0\), one remarkable peak can be generated in the output plane and a positive validation is satisfied. Also, if the input images compare with reference images are incorrect \([g_i(r) \neq f_i(r), g_2(r) \neq f_2(r) and g_3(r) \neq f_3(r)]\), a negative validation occurs and the output is broader and less intensity than the AC peak.

3. Results and discussion

In the encryption process, we adopt three grayscale input images as illustrated in figure 3(a), (b), (c) to demonstrate the effectiveness of the proposed method. All images have dimensions of 512 x 512 pixels. The random phase mask is generated in the computer on the platform of MATLAB 8.6.

![Figure 3](image-url)

Figure 3. The original images (a), (b) and (c) to be encrypted.

Using equation 3, the encrypted image is generated by the three images and phase key. It is clear that the three images are encrypted into one image with white noise amplitude distribution. Figure 4 shows
the magnitude $|\psi(r)|$ and phase $\varphi_\psi(r)$ information of the encrypted image. The sparse encrypted image is generated by randomly selected the sparse information as shown in figure 5. The sparse data is applied to the magnitude component of the encrypted image and kept the phase information as shown in figure 1. Here, the total summation of selected pixels is equal to 1% of each original encrypted image as illustrated in figure 5a. The corresponding encrypted image from sparse encrypted data $\psi_{sp}(r)$ is shown in figure 5b which was used to validate the information of the triple-image encrypted distribution.

![Figure 4](image1.png)

Figure 4. (a) Magnitude distribution of the encrypted function $|\psi(r)|$ (b) phase distribution of the encrypted function $\varphi_\psi(r)$.

![Figure 5](image2.png)

Figure 5. (a) Sparse representation sample with 1% sparse distribution of the image pixel size. (b) sparse data for amplitude encrypted image.

In order to validate the proposed method, the output intensity distribution of the encrypted data with phase extraction nonlinearity ($\omega=0$) is computed by equation (8). The key phase code $\eta(r)$ is correctly provided from the system database. Figure 6(a) shows the output intensity distribution when $g_1(r) = f_1(r)$, $g_2(r) = f_2(r)$ and $g_3(r) = f_3(r)$ which confirms that the positive validation. From this figure, a high and sharp autocorrelation peak is observed. Consequently, the system is confirmed the simultaneous verification with free of noise and distortions. Figure 6(b) depicts the output intensity distribution when
the false images as shown in figure 7 are used. In this case, it is obtained only a noisy background without any remarkable correlation peak when \( g_1(r) \neq f_1(r), g_2(r) \neq f_2(r) \) and \( g_3(r) \neq f_3(r) \). Thus, the output intensity distribution had cross correlation signal and confirmed the negative validation. From figure 6, it is noted that the proposed method authorized the true images and unauthorized the false images even though the information loss due to the sparse strategy.

Figure 6. Authentication verification of encrypted function; (a) autocorrelation peak when input images is matched with correct images (figure 3) and (b) cross-correlation peak when input images is matched with incorrect images (figure 7). The correct RPM is used.

Figure 7. The input images (a), (b) and (c) to be compared with the primary reference images of figures 3(a,b,c).

To achieve a good performance of the proposed method, the most appropriate applied nonlinearity \( \omega \) and the suitable amount of sparse data, the discrimination ratio (DR) and the peak-to-correlation energy (PCE) [21] as a function of the sparsity ratio have been computed at different values of \( \omega \). Figure 8 depicts the DR value, which computed from the set of numerical simulations versus percentage of the sparse information with various \( \omega \) values. It is shown clearly from figure 8 that the DR value rapidly decreases with decreasing the sparse data, particularly when sparsity ratio is smaller than of 1\%, while, the value of DR increases at sparsity ratio higher than 1\%. Moreover, the results show a good discrimination with the sparsity ratio \( sp > 1\% \) and the parameter \( \omega < 0.6 \), where the DR > 0.5. For this...
case, $\omega = 0$ and $sp = 1\%$ give the best results in terms of DR and a good recognition for the verification system has been remarked for $DR = 0.9$.

Figure 9 shows the mean PCE values versus percentage of the sparse information. From this figure, it can be observed that the PCE increases semi-linearly for $\omega = 0$. PCE increases for increasing sparse information and has a high value when $\omega < 0.6$.

![Figure 8: DR results with different values of nonlinear parameter $\omega$ used in triple-image authentication.](image-url)
Figure 9. PCE results for different values of nonlinear parameter $\omega$ used in triple-image authentication.

4. Conclusion
An optical triple-image encryption and authentication verification method by using sparse strategy was proposed. This method could be encrypted three grayscale images into one image at the same time. In sparse strategy, the partial data was randomly extracted from the resultant encrypted distribution. The resulting encrypted function could be verified by introduced the nonlinear operation in the Fourier plane for authentication stage. The simulation results have been performed to verify its validity. The results indicated that the nonlinear parameter and sparsity ratio effected in the performance of the correlation system and $\omega < 0.6$ achieved a good result for optical security system. Finally, it was concluded that the results demonstrated the feasibility and effectively of the three image encryption and authentication method.

References
[1] Chen W, Javidi B, and Chen X, Advances in optical security systems. Adv. Opt. Photon, 2014. 6: p. 120-154.
[2] Liu S, Guo C, and Sheridan J T, A review of optical image encryption techniques. Opt. & Las. Tech., 2014. 57: p. 327-342.
[3] Javidi B, Roadmap on optical security. J. Opt., 2016. 18(8): p. 83001-83039.
[4] Refregier P and Javidi B, Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett., 1995. 20: p. 767-769.
[5] Goodman J W, Introduction to Fourier Optics. 3rd ed. 2004: McGraw-Hill.
[6] Situ G, Pedrini G, and Osten W, Strategy for cryptanalysis of optical encryption in the Fresnel domain. Appl. Opt., 2010. 49: p. 457-462.
[7] Unnikrishnan G, Joseph J, and Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett., 2000. 25: p. 887-889.
[8] Liu Z, et al., Double-image encryption based on the affine transform and the gyrator transform. J. Opt., 2010. 12: p. 035407.
[9] Carnicer A, et al., Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett., 2005. 30: p. 1644-1646.
[10] Gopinathan U, et al., A known-plaintext heuristic attack on the Fourier plane encryption algorithm. Opt. Express, 2006. 14: p. 3181-3186.
[11] Kumar P, Joseph J, and Singh K, Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack. J. Opt., 2012. 14: p. 045401.
[12] Peng X, et al., Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett., 2006. 31: p. 1044-1046.
[13] Frauel Y, et al., Resistance of the double random phase encryption against various attacks. Opt. Express, 2007. 15: p. 10253-10265.
[14] Millán M S, Pérez-Cabrè E, and Javidi B, Multifactor authentication reinforces optical security. Opt. Lett., 2006. 31: p. 721-723.
[15] Alfalou A and Mansour A, A new double random phase encryption scheme to multiplex and simultaneous encode multiple images. Appl. Opt., 2009. 48: p. 5933-5947.
[16] Tao R, Xin Y, and Wang Y, Double image encryption based on random phase encoding in the fractional Fourier domain. Opt. Express, 2007. 15: p. 16067-16079.
[17] Liu Z and Liu S, Double image encryption based on iterative fractional Fourier transform. Opt. Commun., 2007. 275: p. 324-329.
[18] Matoba O and Javidi B, Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt. Lett., 1999. 24: p. 762-764.
[19] Pérez-Cabrè E, et al., Photon-counting multifactor optical encryption and authentication. J. Opt., 2015. 17: p. 025706.
[20] Mohammed E A and Saadon H L, Optical double-image encryption and authentication by sparse representation. Appl. Opt., 2016. 55(35): p. 9939-9944.
[21] Kumar B V K V and Hassebrook L, Performance measures for correlation filters. Appl. Opt., 1990. 29: p. 2997-3006.