University of Thi-Qar Journal of Science (UTsci)
The 4th Scientific Conference of Science College/ University of Thi_Qar
Volume (7), No.2

Secure Optical Identity Tag with Quick Response Code Based on Sparse Phase Information

* Emad A. Mohammed Haitham L. Saadon
Department of Physics,
College of Science,
University of Basrah
Basrah , Iraq.
* emad.mohammed@uobasrah.edu.iq
haitham.saadon@uobasrah.edu.iq

***Abstract*— We propose, an optical identity tag authentication using quick response code with the primary information based on sparse encrypted data. The optical identity tag approved with a high security verification in some purposes such as credit cards and passports. The primary information contained in the identity tag is compressed by applying sparse representation technique to the data of encrypted function. From this proposal, an optical identity tag is implemented for authentication. Only users with correct information can achieve the authentication process whereas illegal users with false information cannot, so that the security of the system is improved. Numerical simulations and results are presented to demonstrate the performance of this optical identity tag. The performance of the system was studied by subjecting the double-image encryption and verification authentication method for occlusion attack. The obtained results explain the system was able to validate the proposed optical identity tags though when it's under the effect of occlusion.**

***Keywords*— Optical information security, optical encryption and authentication, optical ID tags, optical recognition**

I.INTRODUCTION

All aspects of our lives are influenced by technology of the optical information security. This is due to the complex processes regarding the property of the documents, economic operations, and data *information*. Optical information processing systems have gained more attention from researchers for optical security applications including an encryption, recognition, anti-counterfeiting, and authentication. A great advantage for this system, likes parallel processing, high-speed, amplitude, phase, wavelength, and polarization (Javidi, 2005; Cristóbal *et al.*, 2011; Chen *et al.*, 2014; Liu *et al.*, 2014; Javidi, 2016). In this case, different techniques were proposed, such as a double random phase encoding (DRPE) technique (Refregier *et al.*, 1995) under a classical 4f correlator (Goodman, 2004), a phase processor (Towghi *et al*., 1999), and a joint transform correlator (JTC) architecture (Abookasis *et al.*, 2001). The classical DRPE technique has security flaws due to the linearity in encryption and decryption processes. To overcome this difficulty, Markman *et al.* proposed a new system by applying photon counting imaging technique to the encrypted image to enhance the security for the whole process (Markman *et al.*, 2014). Recently, Mohammed et al. proposed a new method by integrating the sparse representation technique into double image encryption scheme (Mohammed *et al.*, 2019).

In general, the optical identity (ID) tags are useful tool to be achieved many purposes of identification by high secure verification (Javidi, 2003; Kim, 2010). The ID tags designed to improve low security and useful reading under circumstances. A lot of systems use both amplitude and phase components of the encrypted data, but there is limitation in the practical applications. In this situation, the amplitude encrypted function is remained constant and only the phase values are considered for authentication stage (Mogensen *et al.*, 2000; Mogensen *et al.*, 2001). In addition, if the optical ID tags are attacked by occlusion, the retrieved information of the input images can be lost, which is made the authentication process difficult when using a correlation system (Barrera *et al.*, 2014; Barrera *et al.*, 2014). Therefore, the optical encryption technique is combined with the QR (Quick Response) coding to enhance the recovered information process (Barrera *et al*., 2013; Markman *et al.*, 2014). QR Code is the module for a two dimensional code presented for industry purposes. In addition, the QR was widely spread outside the industry due to its fast readability and high storage capacity compared to the classical UPC (Universal Product Code) barcodes. The code consists of black square dots distributed on a white background. QR codes can be scanned by smartphones or tablets with the suitable applications.

In this paper, a double-image secure scheme based on special properties of JTC and 4f classical setup is proposed, which is conformed to high security protocol. A user uses their own QR to encrypt the plaintext in the encryption process. we combine two techniques to enhance the optical

security method. The first one is to use QR code in the optical encryption technique and the other is sparse phase strategy. The encrypted information is stored in an optical identity (ID) tag, and considered for validation process. Numerical results are presented to test the performance of the verification process and the effect of occlusion attacks in this ID tag.

II. THEORETICAL ANALYSIS

Two authenticators were dedicated to satisfy the double-image encryption and authentication method. The authenticators involve input image and its respective QR code as primary images and two random phase masks. The two reference primary images f(x,y) and g(x,y) are phase encoded and considered for encryption stage. Two phase masks m(x,y) and n(x,y) are used to encrypt the information of the primary images,

$$m(x,y) = exp[i\pi R_1(x,y)], \quad (1a)$$

$$n(x,y) = exp[i\pi R_2(x,y)], \quad (1b)$$

where $R_1(x,y)$ and $R_2(x,y)$ represent the two independent functions randomly distribution with in [0,1]. The two random phase masks with complex transmittance are put at input and Fourier planes, respectively, as illustrated in Fig. 1. Then, the whole encryption process could be mathematically described by the equation as (Mohammed *et al.*, 2016):

$$\psi(x,y) = \{f(x,y).g(x,y) * m(x,y)\} * IFT[n(x,y)], \quad (2)$$

where *IFT* represents inverse Fourier transform, *f(x,y)* and *g(x,y)* denote the two phase encoded input images, denotes multiplication and denotes convolution operation.

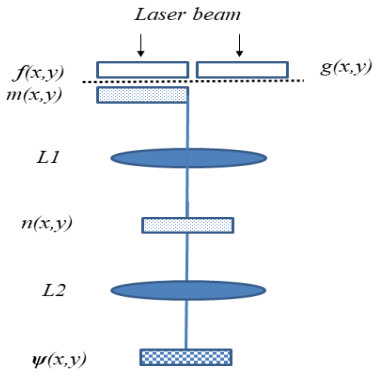


Fig. 1. A schematic setup for the proposed encryption system. L: lens; m and n are the key codes.

Phase-only function of encrypted data will be implemented by kept the phase component. That can be done by extracted the phase values from the encrypted function $[\psi(x,y)]$. Afterwards, sparse data of phase values encrypted function $[\phi_\psi(x,y)]$ can be achieved by a double-image encryption method which proposed by Mohammed et al. (Mohammed *et al.*, 2016), and the mathematical operation is described by the relationship as

$$\phi_\psi^{sp}(x,y) = \phi_\psi(x,y).\beta(x,y), \quad (3)$$

where $\beta(x,y)$ is the random binary distribution function and $\phi_\psi(x,y)$ is the phase value, so it can generate the sparse phase encrypted function $\phi_\psi^{sp}(x,y)$.

In the authentication step, let *f*(*x*,*y*) and *g*(*x*,*y*) are the plaintext image and its QR code, respectively. These images are compared to the set of reference images *p*(*x*,*y*) and *q*(*x*,*y*), respectively, and let *n*(*x*,*y*) and *m*(*x*,*y*) are known by this processor. A schematic setup of the proposed authentication verification method with the sparse phase information is shown in Fig. 2. This method allows the simultaneous authentication of double-image with only partial randomly selected of phase encrypted information.

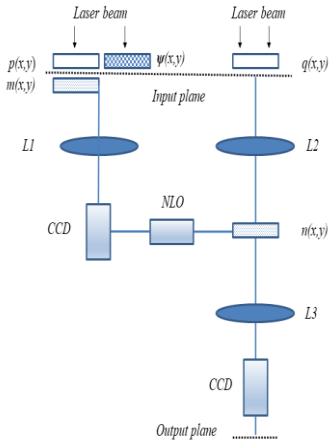


Fig. 2. A schematic setup for the proposed authentication system. L: lens; CCD: charge-coupled device; NLO: non-linear operator.

To establish the authentication system, the true images and false are taken. When the reference images are the same as the true images, a correct authentication validate. The result decides the authentication conclusion which can be expressed as (Mohammed *et al.*, 2016)

$$|AC_{POF}[g(x,y)] \otimes AC^*_{PPC}[f(x,y)m(x,y)] \otimes AC^*_{CMF}[N(x,y)]|^2, \quad (4)$$

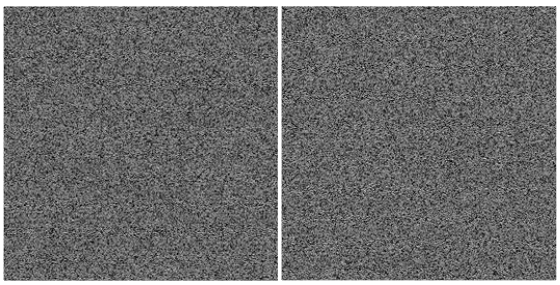
here, $\otimes$ is the cross correlation and the sub-indices *CMF*, *POF* and *PPC* are the types of filter contributed in the autocorrelation signal, where, the *CMF* denotes the classical matched filter, *POF* represents the phase-only filter, and *PPC* is the pure phase correlation (Mohammed *et al.*, 2016). From Eq. (4), it is to be expected that a significant peak could be noted in the output plane. In addition, if the reference images to be compared with false images, the authentication failure is concluded due to the noisy distribution in the output plane.

III. RESULTS AND DISCUSSIONS

In the encryption process, we adopt binary image with its QR code as illustrated in Fig. 3 to demonstrate the effectiveness of the proposed method. All images have dimensions of 512 x 512 pixels. The random phase masks are generated in the computer on the platform of MATLAB 8.6 as shown in Fig. 4. From these figures, the encrypted function $\psi(x,y)$ is obtained by applying Eq. (2) [see Figure 5]. Then, the phase only component of an image encrypted will be proposed and the amplitude component remains constant. Therefore, the Figure 5(b) will play the important role in this work.

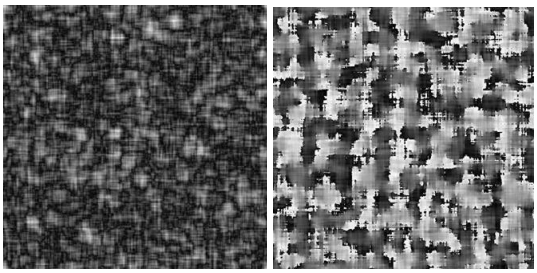
(a) (b)

Fig. 3. (a) Representation of the input image [*f(x,y)*] and (b) its respective QR code [*g(x,y)*].



(a) (b)

Fig. 4. The key codes: (a) *m(x,y)* and (b) *n(x,y).*



(a) (b)

Fig. 5. (a) Magnitude function of the encrypted distribution $[|\psi(x,y)|]$ and (b) phase function of the encrypted distribution $[\varphi_\psi(x,y)]$

The sparseness is applied to the phase-only information of encrypted function; therefore, only the randomly selected pixels keep the phase data (Mohammed *et al.*, 2019; Sui *et al.*, 2019). Figure 6 depicts the phase-only sparse information which generated by randomly selecting 2.7% of phase component for the encrypted image. At this stage, the OID tag is presented to contain the information of the encrypted images $\psi(x,y)$ and it will be consider for verification process.

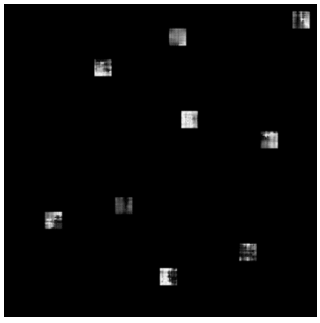


Fig. 6. The proposed optical ID (OID) tag of sparse phase information function $\phi_\psi^{sp}(x,y)$.

To verify the data of the proposed OID, a sparse phase encrypted function $\phi_\psi^{sp}(x,y)$ is used. Optical authentication method, as demonstrated in Eq. (4), is applied to validate the sparse phase-only information for the double-image encryption. Thus, the output correlation of the sparse data with phase extraction nonlinearity is computed. This is done using 2.7% partial of the phase encrypted function. Figure 7 shows that a significant autocorrelation peak is obtained for the reference images with true images. From other hand, a noisy distribution is noted when false images (see Fig. 8) are compared with the reference images; thus, cross-correlation is observed as shown in Fig. 9. As shown in Fig. 7, a successful authentication was satisfied with only 2.7% of the encrypted data. This result implies an advantage of the proposed method that could be simultaneously authorized double-image from a single phase ciphertext even though data loss due to the sparse technique.

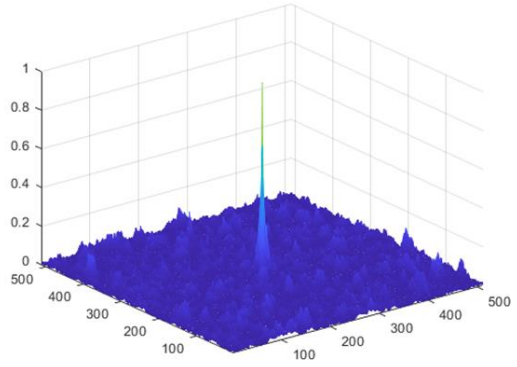


Fig. 7. Output correlation for positive validation when *p(x,y)= f(x,y)* and *q(x,y)= g(x,y).*

(a) (b)

Fig. 8. (a) The fake image and (b) its respective QR code.

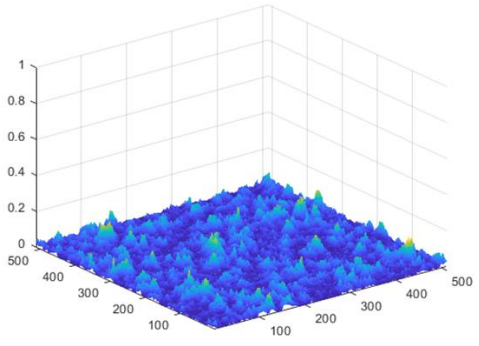


Fig. 9. Output correlation for negative validation when *p(x,y) ≠ f(x,y)* and *q(x) ≠ g(x,y).*

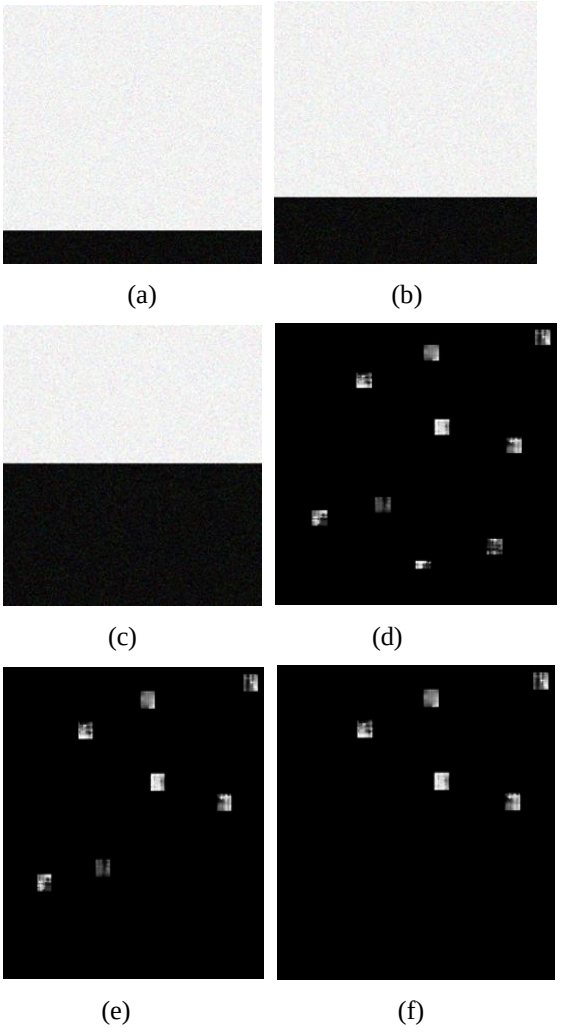
IV. EFFECTS OF OCCLUSION ATTACKS

In this work, we study the robustness of the proposed optical ID tags against the effect of occlusion attacks. For occlusion attack, the removing of some pixels from the optical ID tag is implemented. The cropping of the proposed ID tag is presented as a binary function $\rho(x,y)$, where the value at pixel (x,y) is one if this pixel is cropped and zero otherwise. The occluded ID tag is defined as

$$\varphi_\psi{}'(x,y) = \varphi_\psi(x,y) \,.\, [1 - \rho(x,y)] \quad (5)$$

To test the performance of the cropping ID tag, we calculate the output correlation intensity for a phase extraction nonlinearity. The simulation results for occluded ID are shown in Fig. 10. Figure 10(a–c) show the occluded parts with 12.5%, 25% and 50 % content losses. Figure 8(d–f) show the corresponding occluded OID tag of the encrypted data, respectively. In addition, the autocorrelation peaks is noted as shown in Fig. 8(g–i). From these figures, we can infer that the positive validation is satisfy even with 50 % of the phase OID has been lost. Moreover, it can be noted that the validated results are sensitive to the occlusion attacks. This behavior indicates that the performance of the correlation system is not effective against occlusion attacks.

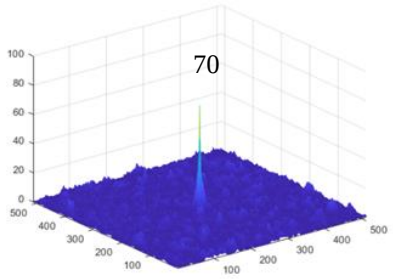
Finally, the proposed OID tag based on QR code is robust against occlusion attacks caused by cropping and achieves the requirement of high storage efficiency.



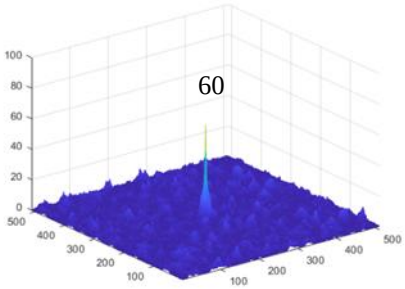
(a) (b)

(c) (d)

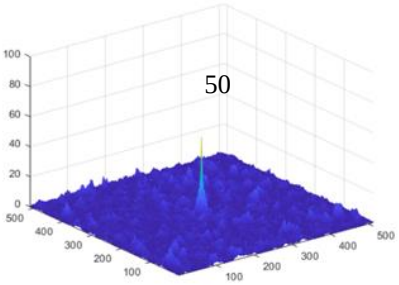
(e) (f)



(g)



(h)



(i)

Fig. 10. Simulation results for the proposed OID tag against occlusion attacks. The sparse ID tags (d-f) and the output correlation planes (g-i) obtained from the occluded images (a-c): (a) 12.5 % occluded; (b) 25 % occluded; (c) 50 % occluded.

V. CONCLUSIONS

An optical ID tag verification authentication using QR code based on sparse encrypted data has been proposed. By use the QR code, we add an extra security measure against intruder attack. We also are able to encrypt and compress the QR code of original information by applying sparse representation technique to the data of encrypted function. From the simulation results, we prove that the proposed optical ID tag is able to validate authenticity of the correct information. In addition, the robustness of the phase optical ID tags against occlusion attacks have been studied. Furthermore, the proposed OID tag based on QR code and sparse strategy is more secure and robust to the cropping, even under severe compression of sparse representation technique.

VI. REFERENCES

Abookasis, D.; Arazi, O.; Rosen, J. and Javidi, B. (2001). Security optical systems based on a joint transform correlator with significant output images. Opt. Eng. 40: 1584-1589.

Barrera, J.F.; Mira, A. and Torroba, R. (2013). Optical encryption and QR codes: Secure and noise-free information retrieval Opt. Express 21(5): 5373-5378.

Barrera, J.F.; Mira, A. and Torroba, R. (2014). Experimental QR code optical encryption: noise-free data recovering. Opt. Lett. 39(10): 3074-3077.

Barrera, J.F.; Vélez, A. and Torroba, R. (2014). Experimental scrambling and noise reduction applied to the optical encryption of QR codes Opt. Express 22(17): 20268-20277.

Chen, W.; Javidi, B. and Chen, X. (2014). Advances in optical security systems. Adv. Opt. Photon 6: 120-154.

Cristóbal, G.; Schelkens, P. and Thienpont, H. (2011). Optical and Digital Image Processing: Fundamentals and Applications, Wiley-VCH.

Goodman, J.W. (2004). Introduction to Fourier Optics, McGraw-Hill.

Javidi, B. (2003). Real-time remote identification and verification of objects using optical ID tags. Opt. Eng. 42: 2346-2348.

Javidi, B. (2005). Optical and Digital Techniques for Information Security, Springer.

Javidi, B. (2016). Roadmap on optical security. J. Opt. 18(8): 83001-83039.

Kim, C. (2010). Simple distortion-invariant optical identification tag based on encrypted binary-phase computer-generated hologram for real time vehicle identification and verification. Opt. Eng. 49: 115801-115806.

Liu, S.; Guo, C. and Sheridan, J. T. (2014). A review of optical image encryption techniques. Opt. & Las. Tech. 57: 327-342.

Markman, A. and Javidi, B. (2014). Full phase photon counting double random phase encryption. J. Opt. Soc. Am. A 31: 394-403.

Markman, A.; Javidi, B. and Tehranipoor, M. (2014). Photon counting security tagging and verification using optically encoded QR codes. IEEE Photon. J. 6: 6800609.

Mogensen, P. and Gluckstad, J. (2000). Phase-only optical encryption. Opt. Lett. 25: 566-568.

Mogensen, P. and Gluckstad, J. (2001). Phase-only optical decryption of a fixed mask. Appl. Opt. 40: 1226-1235.

Mohammed, E.A. and Saadon, H.L. (2016). Optical double-image encryption and authentication by sparse representation. Appl. Opt. 55(35): 9939-9944.

Mohammed, E. A. and Saadon, H. L. (2019). Sparse phase information for secure optical double-image encryption and authentication. Opt. Las. Tech. 118: 13-19.

Refregier, P. and Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 20: 767-769.

Sui, L.; Zhao, X.; Huang, C.; Tian, A. and Anand, A. (2019). An optical multiple-image authentication based on transport of intensity equation. Opt. Las. Eng. 116: 116-124.

Towghi, N.; Javidi, B. and Luo, Z. (1999). Fully phase encrypted image processor. J. Opt. Soc. Am. A 16: 1915-1927.