J. Meas. Sci. Instrum., 2024, 15(3): 338-343. http://jmsi.publish.founderss.cn
DOI: 10.62756/jmsi.1674-8042.2024035 jmsi@nuc.edu.cn

A holographic optical communication system based on RSA algorithm and quaternion function

YANG Peng[1*], HAN Jianning[2]

1. Department of Electronic Engineering, Taiyuan Institute of Technology, Taiyuan 030008, China;
2. School of Information and Communication Engineering, North University of China, Taiyuan 030051, China

***Corresponding author:** YANG Peng (yangpeng@tit.edu.cn)

Received: February 27, 2024 **Revised:** May 24, 2024 **Accepted:** May 31, 2024

Abstract: A facile encryption way was successfully applied to the holographic optical encryption system with high speed, multi-dimensionality, and high capacity, which provided a better security solution for underwater communication. The reconstructed optical security system for information transmission was based on wavelength λ and focal length f that were keys to encryption and decryption. To finish the secure data transmission (λ, f) between sender and receiver, an extended Rivest-Shamir-Adleman (ERSA) algorithm for the encryption was achieved based on three-dimension quaternion function. Therein, the Pollard's rho method was used for the evaluation and comparison of RSA and ERSA algorithms. The results demonstrate that the message encrypted by the ERSA algorithm has better security than that by RSA algorithm in the face of unpredictability and complexity of information transmission on the unsecure acoustic channel.

Key words: holography; quaternion; Fourier lens; extended Rivest-Shamir-Adleman (ERSA); Pollard's rho method

0 Introduction

With the rapid development of modern communication technology, optical encryption technology based on holography has made great process relying on a new technology that has many advantages such as high speed, multi-dimensionality, and high capacity[1-3]. Subsequently, optical information security technology is rapidly developing and has the potential for providing reliable security for data transmission. Hence, this technology has gradually attracted more attention and been considered as an enabling technology[4-6].

In recent years, optical encryption system, especially holographic optical encryption system, has been widely used for achieving preferable security. It is a new and an outstanding solution for protecting the data and data transmission, and openes up a new field of optical information security[7-16]. Numerous researches in this field have devoted their efforts to strengthening the security of data transmission. For example, Li et al.[17] applied holographic technology to optical image encryption by combining optical encryption with image-hiding technology.

The encryption system based on RSA public key was classic, which was initially proposed by Rivest et al. in 1978[18]. However, the research on RSA was blank until RSA system was developed by Elkamchouchi et al. based on Gaussian integers in 2002[19]. This system is similar to the probabilistic scheme proposed by Kuwakado et al in 2007[20]. Both of them contain the same modulus equations[19,21].

In early study, the encryption system based on the extension of Rivest-Shamir-Adleman (RSA) algorithm was implemented by complex function[22]. In this work, to improve the encryption algorithm based on RSA, we proposed a more appropriate method with quaternion function. The quaternion function is one of hyper complex numbers, which has been widely used in computer graphics and encrypted data transmission. Here, the motivation of using quaternion function is that, firstly, it is complex function with 3-vector and one-scaler parameters; secondly, it has noncommutative property by which the highest security of data transmission can be achieved[23].

This paper presents a new scheme of encryption system using a quaternion function for extended RSA (ERSA) algorithm. The paper is organized as follows: in Section 1, a brief introduction to system design is made. In Section 2, the ERSA algorithm is implemented to send a cipher to the receiver. The computer simulation is descripted in Section 3, including encryption and decryption processes. In Section 4, the security of data transmission using ERSA

© The Author(s) 2024. Published by Publishing Center of North University of China. The articles published in this open access journal are distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

and RSA algorithms are evaluated by Pollard's rho method. Finally, the conclusions are listed in Section 5.

1 System design

As shown in Fig.1, it is an optical digital holographic system for encryption and decryption, among which a space light modulator (SLM) and a Fourier lens-based optical collimators are significant components[24].

The Fourier lens is a special lens on which the output wave is focused[25]. The focal length f is determined by the sender, and it is an important factor for strengthening the security of the system. The system implements virtual holographic method together with an object wave and a reference wave, and then the encryption and decryption methods of object information can be performed.

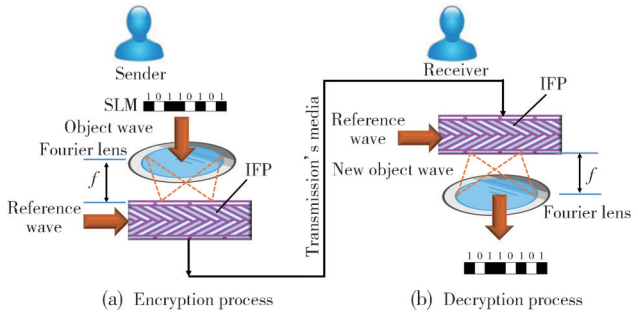

Fig. 1 An optical encryption & decryption digital holographic system

The reference wave is expressed as

$$\boldsymbol{U}_{\mathrm{R}}(x,y)=|\boldsymbol{U}_{\mathrm{R}}|\mathrm{e}^{-\frac{\mathrm{i}ky^2}{2R(x)}}, \tag{1}$$

where $|\boldsymbol{U}_{\mathrm{R}}|$ is the real amplitude of the reference wave, $k=2\pi/\lambda_{\mathrm{R}}$ is the wave number of the reference wave, λ_{R} is the wave length of the reference wave, and $R(x)$ is a radius of curvature.

The SLM is used in the system settings, which behaves like a periodic diffraction grating, encoding the information $u(x)$ (e. g. "10110101") into the object wave. When the object wave is preceded through the Fourier lens, the object wave $\boldsymbol{U}_{\mathrm{O}}(u,f)$ is calculated by[26]

$$\boldsymbol{U}_{\mathrm{O}}(u,f)=\frac{1}{\sqrt{\lambda_{\mathrm{O}}f}}\int_{-\infty}^{\infty}u(x)\mathrm{e}^{\frac{-2\pi\mathrm{i}xu}{\lambda_{\mathrm{O}}f}}\mathrm{d}x, \tag{2}$$

where λ_{O} is the object wavelength, f is the focal length, $u/(\lambda_{\mathrm{O}}f)$ is the spatial frequency, and $\boldsymbol{U}_{\mathrm{O}}(u,f)$ is at the focal plane $x=f$.

In Fig. 1(a), the object wave comes across the reference wave, which assists the generation of an interference fringe pattern (IFP) at the sender side.

The IFP can be calculated by determining its intensity as

$$\boldsymbol{I}(x,y)=|\boldsymbol{U}_{\mathrm{R}}+\boldsymbol{U}_{\mathrm{O}}|^2=$$

$$\boldsymbol{U}_{\mathrm{O}}\boldsymbol{U}_{\mathrm{R}}^*+|\boldsymbol{U}_{\mathrm{R}}|^2+|\boldsymbol{U}_{\mathrm{O}}|^2+\boldsymbol{U}_{\mathrm{O}}^*\boldsymbol{U}_{\mathrm{R}}, \tag{3}$$

where $\boldsymbol{U}_{\mathrm{O}}^*$ and $\boldsymbol{U}_{\mathrm{R}}^*$ are the complex conjugates of $\boldsymbol{U}_{\mathrm{O}}$ and $\boldsymbol{U}_{\mathrm{R}}$, respectively. The IFP is considered as a cipher that carries object information $u(x)$. This process is called encryption.

Then, the IFP is transmitted to the receiver at a very small divergence angle within the communication channel to achieve fast data transmission and high safety considering long-distance underwater turbulence and diffraction loss.

In Fig.1(b), at the receiver side, the IFP is illuminated only by the reference wave to produce an image of new object $\boldsymbol{I}'(x,y)$, which is given by

$$\boldsymbol{I}'(x,y)=\boldsymbol{I}(x,y)\boldsymbol{U}_{\mathrm{R}}=$$

$$\boldsymbol{U}_{\mathrm{O}}|\boldsymbol{U}_{\mathrm{R}}|^2+|\boldsymbol{U}_{\mathrm{R}}|^2\boldsymbol{U}_{\mathrm{R}}+|\boldsymbol{U}_{\mathrm{O}}|^2\boldsymbol{U}_{\mathrm{R}}+\boldsymbol{U}_{\mathrm{O}}^*\boldsymbol{U}_{\mathrm{R}}^2. \tag{4}$$

It can be seen that $\boldsymbol{I}'(x,y)$ contains four parts representing light waves from the hologram. Among them, the first part $\boldsymbol{U}_{\mathrm{O}}|\boldsymbol{U}_{\mathrm{R}}|^2$ is proportional to $\boldsymbol{U}_{\mathrm{O}}$ and it is part of the reconstructed object wave. This process is called decryption.

In the encryption and decryption processes, the reference waves at both sides of the sender and the receiver should have the same value, and the wavelength λ_{R} of reference wave is considered as the first key. In the Fourier lens model, the output signal as new cipher can be taken as a primary factor, and thus the focal length f is regarded as the second key.

2 ERSA algorithm

To finish the secure transmission of data message (λ,f) between the sender and the receiver, an extended process focusing on encryption is proceeded using the three-dimension quaternion function and ERSA algorithm. As shown in Fig.2, ERSA algorithm is used to deliver the message (λ,f) as the cipher to the receiver side.

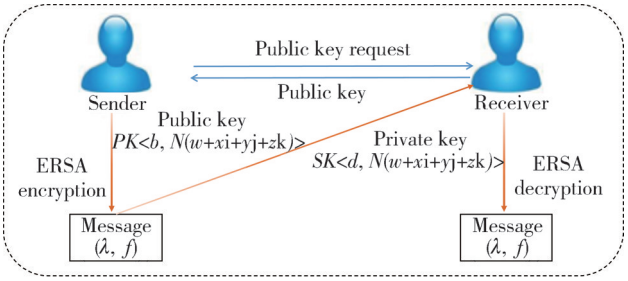

Fig. 2 Schematic diagram of ERSA algorithm

The ERSA algorithm is used to send the cipher (λ,f) to the receiver after the following encryption steps shown in Algorithm 1, where a public key $\langle b,N\rangle$ based on

three-dimension quaternion function and a private key $\langle d, N \rangle$ are obtained.

Algorithm 1 Calculation of <Keys>

1. Input $p, q \in \mathbf{C}$, $b \in \mathbf{Z}$
2. $N=(x_p+y_p\mathrm{i}+w_p\mathrm{j}+z_p\mathrm{k})(x_q+y_q\mathrm{i}+w_q\mathrm{j}+z_q\mathrm{k})$
3. $\varphi(p)=(x_p^2+y_p^2+w_p^2+z_p^2)-1$
4. $\varphi(q)=(x_q^2+y_q^2+w_q^2+z_q^2)-1$
5. $\varphi(N)=\varphi(p)\varphi(q)$
6. $d \equiv b^{-1} \bmod \varphi(N)$
7. Output $PK\langle b, N(w+x\mathrm{i}+y\mathrm{j}+z\mathrm{k})\rangle$, $SK\langle d, N(w+x\mathrm{i}+y\mathrm{j}+z\mathrm{k})\rangle$

In Algorithm 1, both p and q are quaternion function with 3-complex vectors and one scaler as $p=x_p+y_p\mathrm{i}+w_p\mathrm{j}+z_p\mathrm{k}$, and $q=x_q+y_q\mathrm{i}+w_q\mathrm{j}+z_q\mathrm{k}$, and their squared absolute value $|p|^2$ and $|q|^2$ are prime number.

At the sender side, the cipher c is calculated based on the public key, and then it carries the message m to be sent to the receiver, as shown in Algorithm 2. The value of m is calculated by the private key, this decrypted message is then delivered to the receiver, as shown in Algorithm 3.

Algorithm 2 <Encryption>

1. Input m (λ, f)
2. $c = m^b \bmod N$
3. Output c

Algorithm 3 <Decryption>

1. Input c
2. $m = c^d \bmod N$
3. Output m (λ, f)

3 Simulation

3.1 Encryption process

The simulation was carried out with the tools of Fourier lens and hologram from software COMSOL Multiphysics[27]. The parameters were set as follows: inset wavelength λ_O was 550 nm; wave length λ_R was 550 nm resulting from the absorption window with a wavelength of 550 nm during underwater transmission; focal length f was 6.20 mm because the light of the Fourier lens-based optical collimator has a very small divergence angle for long-distance transmission; the hologram was designed as a rectangle with the horizontal sizw (L_x) and vertical size (L_y) of 120 μm and 30 μm, respectively.

Suppose that a digital message $u(x)$, e. g. "10110101", to be sent from the sender to the receiver. As displayed in Fig. 3, the reference wave is introduced first, and then the object wave appears on the top of this system.

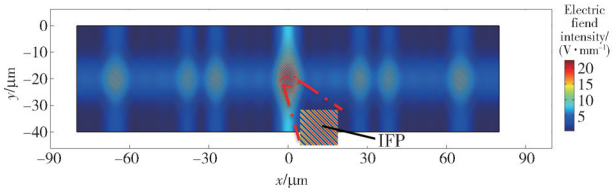

Fig. 3 Encryption and electric field intensity at $\lambda_O=\lambda_R=550$ nm, (inset: IFP with 45°)

Fig. 3 shows the results of encryption process. The IFP arises due to the interaction between the object wave and the reference wave, and λ_O and λ_R are the same value. Therefore, IFP is set to be 45° and regarded as a cipher to record the encrypted message.

3.2 An example of ERSA algorithm

There is an example of message transmission from the sender to the receiver based on ERSA algorithm with $\lambda=550$ nm and $f=6.20$ mm. According to Algorithms 1 to 3 described in section 2, a security system is built.

Firstly, the keys are obtained according to Algorithm 1:

1) Setting two different quaternion functions, p and q, are expressed as

$$p=22+13\mathrm{i}+4\mathrm{j}+5\mathrm{k}, \tag{5}$$

$$q=22+14\mathrm{i}+7\mathrm{j}+2\mathrm{k}, \tag{6}$$

where $|p|^2$ and $|q|^2$ are prime number.

2) The value of N is calculated by

$$N=pq=270+588\mathrm{i}+244\mathrm{j}+123\mathrm{k}. \tag{7}$$

3) Selecting an integer b with $1<b<\varphi(N)$, $\varphi(N)=491\,904$ can be got. Especially, b is a coprime to $\varphi(N)$, that is, $gcd(b, \varphi(N))=1$, where gcd(•) is great common divider.

4) d can be calculated according to the congruence relation as

$$bd = 1 \bmod \varphi(N), \tag{8}$$

where b is 71, and d is calculated as 214 775.

The public key is defined as $PK\langle b, N\rangle$, so the pair $\langle 71\,270+588\mathrm{i}+244\mathrm{j}+123\mathrm{k}\rangle$ is the public key obtained. The private key is defined as $sK\langle d, N\rangle$, so the pair $\langle 214\,775,\ 270+588\mathrm{i}+244\mathrm{j}+123\mathrm{k}\rangle$ is the private key obtained.

Then, the message $m(\lambda, f)$ is encrypted according to Algorithm 2.

1) At the sender side, $m(\lambda, f)$ is encrypted using the public key $\langle b, N\rangle$ as $\langle 71\,270+588\mathrm{i}+244\mathrm{j}+123\mathrm{k}\rangle$, and then

$$c = m^b \bmod N. \tag{9}$$

2) The encrypted message c will be sent to the receiver as the cipher.

Finally, the cipher c is decrypted according to Algorithm 3.

1) At the receiver side, the cipher c is decrypted by

$$m=c^d \bmod N, \tag{10}$$

where d=214 775 and N=270+588i+244j+123k.

2) In this way, the encrypted message are decrypted, and the result is m (550 nm, 6.20 mm).

3.3 Decryption process

As shown in Fig. 4, the decryption process is well conducted when permitting the reference wave to pass through the hologram. The output will be a new object wave that carries the information sent by the sender. Meanwhile, the value of reference wave of the sender should be kept the same as that of the receiver.

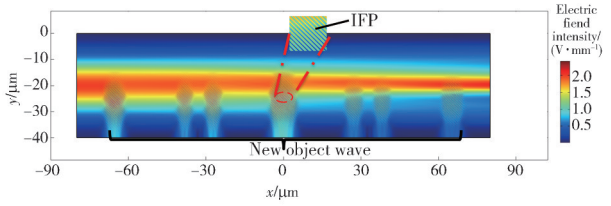

Fig. 4 Decryption and electric field intensity at λ_R= 550 nm, (inset: IFP with 45 ℃)

The reference wave is shown on the hologram, which is used for IFP decryption. Then, new object wave is created when λ_R is selected as 550 nm. Here, λ_R is identified as the first key in the process of decryption.

Afterwards, the focal length f of 6.20 mm as the second key is sent after ERSA encryption, so that a new object wave is created via the transformation with a digital stream (10110101). Finally, the decrypted code is compared with the original code when f=6.20 mm, as shown in Fig.5.

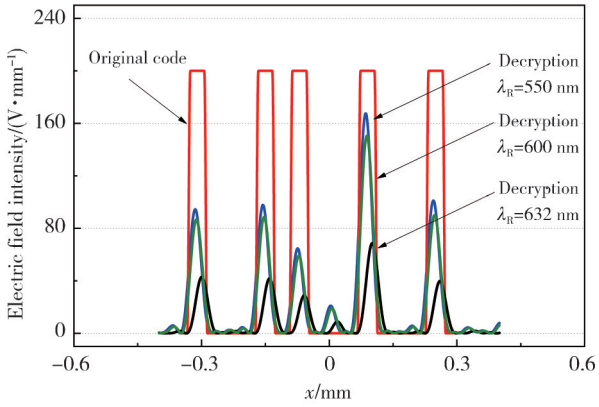

Fig. 5 Comparison between original code and decrypted code

It can be seen that the reference wave with λ_R= 550 nm has the largest amplitude and exhibits an optimal electric field strength, which means that the signal (blue color) matches with period of the original code best.

4 Quality evaluation

The public key of ERSA algorithm consists of modulus N and encryption exponent b. Among them, modulus N is composed of the product of two quaternion numbers, as shown in Table 1. The importance of modulus N is to increase the complexity of the public key and to strengthen the security from trap door attacks.

Table 1 Details of N and key size of RSA, RSA-C, and ERSA

Algorithm	Modulus N	Size of key
RSA	$x_p x_q$	$Length(x)$
RSA-C	$(x_p+y_p\mathrm{i})(x_q+y_q\mathrm{i})$	$Length(x)+Length(y)$
ERSA	$(x_p+y_p\mathrm{i}+\mathrm{w}_p\mathrm{j}+z_p\mathrm{k})(x_q+y_q\mathrm{i}+\mathrm{w}_q\mathrm{j}+z_q\mathrm{k})$	$Length(x)+Length(y)+Length(w)+Length(z)$

Pollard's rho method[28] is a special-purpose factorization algorithm for solving the discrete logarithm problem and for finding small factors of a composite number. Hence, after modulus N is decomposed by Pollard's rho method, if the average output loop in the same key length has the highest level, ERSA will provide better security. The modulus N and key size of RSA, RSA-C[22] and ERSA are compared, as shown in Table 1.

The calculation method of private key is demonstrated in Algorithm 4, processing time t and output loop n of c with various key sizes.

Algorithm 4 <Pollard's rho method>

1. Input m, c, N
2. s.t $m=c^d \bmod N$, Start=time. Clock
3. $n=0$
3. Repeat
4. $n++$
5. Choose $a_n,\beta_n\in[0,|N|^2-2]$ randomly
6. $m_n=(c)^{a_n}g^{\beta_n} \bmod (|N|^2-1)$
7. until $\exists_l$ s.t. $1\leqslant l\leqslant n, m_l=m_n$
8. $d=(\beta_l-\beta_n)(\alpha_n-\alpha_l)^{-1} \bmod (|N|^2-1)$
9. t=time. Clock − Start
10. Output d, n, and t.

To verify the security of c, the Pollard's rho method is utilized to analyze the value of c. Herein, if more $\overline{n}$ is

available, which means better security, the average output loops $\bar{n}$ can be calculated for RSA and ERSA. In addition, RSA and ERSA are evaluated on the average processing time t to ensure the efficiency. It is possible to calculate the private key with small amount of data from $m=c^d \bmod N$ by personal computer. However, it is difficult to calculate it with huge data for long c by personal computer, and maybe super computer is needed. As shown in Fig.6, the Pollard's rho method is used to obtain $\bar{n}$ of c for 8 bit, 12 bit, 16 bit, and 32 bit, respectively, revealing the average processing time t under different private key d.

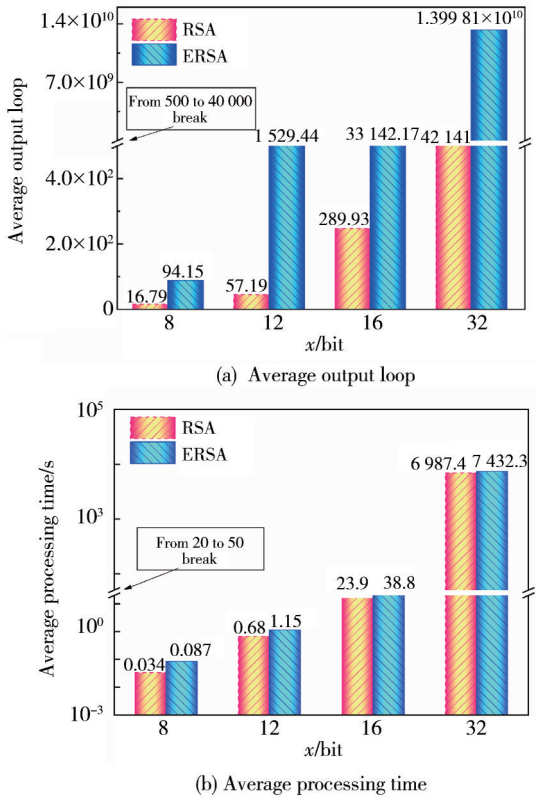

Fig. 6 Performance comparison of RSA and ERSA

The results show that the average output loop $\bar{n}$ and time t calculated by Pollard's rho method are reasonable. It can be seen from Fig.6(a) that ERSA has better security than RSA when the size is higher than 12 bit, which proves ERSA is more suitable for strengthening the security. Comprehensively considering the processing time, efficiency and security between RSA and ERSA, ERSA is superior although it takes slightly longer processing time to decompose c code. Therefore, using ERSA algorithm to encrypt message (λ, f) is a more appropriate method for strengthening the security of data transmissions in this work.

5 Conclusions

This paper presents a new method of encrypting system information (λ, f) using ERSA algorithm based on three-dimension quaternion function. The encryption & decryption model has been successfully simulated in the optical system. The optical system has two keys, wavelength λ is considered as the first key, and focal length f is considered as the second key. For encryption and decryption, the two keys need to be coherent. The results are evaluated by Pollard's rho algorithm and ERSA algorithm has better security because the ERSA algorithm with quaternion function is a complex function with 3-vector and one-scaler parameters, which is non-commutative and can achieve the highest data transmission security. Therefore, the obtained encryption system is a more appropriate method to ensure the security of data transmission.

Acknowledgement

This work was supported by Young Academic Leaders Program of Taiyuan Institute of Technology (No. 2022XS06) and Scientific Research Funding Project of Taiyuan Institute of Technology (Nos. 2022LJ028, 2022KJ103).

Declaration of conflicting interests

The authors declare no conflict of interests.

References

[1] GUO J J, ZHANG Y P, HAO Y, et al. Spatially structured-mode multiplexing holography for high-capacity security encryption. ACS Photonics, 2023, 10(3): 757-763.

[2] WANG X G, WANG W Q, WEI H Y, et al. Holographic and speckle encryption using deep learning. Optics Letters, 2021, 46(23): 5794-5797.

[3] ZHANG S J, MA H W, YANG Y, et al. End-to-end real-time holographic display based on real-time capture of real scenes. Optics Letters, 2023, 48(7): 1850-1853.

[4] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters, 1995, 20(7): 767-769.

[5] BARRERA J F, MIRA A, ROBERTO T. Optical encryption and QR codes: secure and noise-free information retrieval. Optics Express, 2013, 21(5): 5373-5378.

[6] JI Z Y, CHANG J, HUANG Y, et al. Multi-key optical encryption based on two-channel incoherent scattering imaging. Optics Express, 2023, 31(13): 21507-21520.

[7] TAJAHUERCE E, MATOBA O, VERRALL S C, et al. Optoelectronic information encryption with phase-shifting interferometry. Applied Optics, 2000, 39(14), 2313-2320.

[8] JAVIDI B, NOMURA T. Securing information by use of digital holography. Optics Letters, 2000, 25(1): 28-30.

[9] YU L F, CAI L I. Multidimensional data encryption with digital holography. Optics Communications, 2003, 215(4/5/6): 271-284.
[10] NISHCHAL N K, JOSEPH J, SINGH K. Fully phase encryption using digital holography. Optical Engineering, 2004, 43(12): 2959-2967.
[11] XIANG P, YU L F, CAI L L. Double-lock for image encryption with virtual optical wavelength. Optics Express, 2002, 10(1): 41-45.
[12] XIANG P, CUI Z Y, TAN T. Information encryption with virtual-optics imaging system. Optics communications 2002, 212(4/5/6): 235-245.
[13] MENG X F, CAI L Z, XU X F, et al. Two-step phase-shifting interferometry and its application in image encryption. Optics Letters 2006, 31(10), 1414-1416.
[14] MENG X, CAI L, XU X, et al. Full-phase image encryption by two-step phase-shifting interferometry. Optik, 2008, 119(9): 434-440.
[15] TOWGHI N, JAVIDI B, LUO Z. Fully phase encrypted image processor. Journal of the Optical Society Of America A—Optics Image Science and Vision, 1999, 16(8): 1915-1927.
[16] WANG X G, ZHAO D M. Fully phase multiple-image encryption based on superposition principle and the digital holographic technique. Optics Communications 2012, 285(21/22): 4280-4284.
[17] LI J, LI J S, SHEN L, et al. Optical image encryption and hiding based on a modified Mach-Zehnder interferometer. Optics Express, 2014, 22(4): 4849-4860.
[18] RONALD L R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126.
[19] ELKAMCHOUCHI H, ELSHENAWY K, SHABAN H. In extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers//The 8th International Conference on Communication Systems, November 26-28, 2002, Singapore. New York: IEEE, 2002: 91-95.
[20] CASTAGNOS G. An efficient probabilistic public-key cryptosystem over quadratic fields quotients. Finite Fields and Their Applications 2007, 13(3): 563-576.
[21] HIDENORI K, KOYAMA K, TSURUOKA Y. A new RSA-type scheme based on singular cubic curves $(y-\alpha x)(y-\beta x)=x3 (\mathrm{mod}\ n)$. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1995, 78(1): 27-33.
[22] YANG P, NAGASE T, SHAN Y, et al. A VOHE system for underwater communications. Electronics, 2020, 9(10): 1557.
[23] NAGASE T, KOIDE R, ARAKI T, et al. A new quadripartite public-key cryptosystem//IEEE International Symposium on Communications and Information Technology, October 26-29, 2004, Sapporo, Japan. New York: IEEE, 2004: 74-79.
[24] YANG P, NAGASE T, KANAMOTO T, et al. A virtual optical holographic encryption system using expanded Diffie-Hellman algorithm. IEEE Access, 2021, 9: 22071-22077.
[25] YANG P, XUE W S, FAN C Q, et al. In promoting a hybrid cryptosystem system's security based on fresnel lens and RSA algorithm//2022 8th International Conference on Systems and Informatics, December 10-12, 2022, Kunming, China. New York: IEEE, 2022: 1-6.
[26] DENIZ M, ZHAO Y F, TABASSUM A, et al. Diffractive interconnects: all-optical permutation operation using diffractive networks. Nanophotonics, 2023, 12(5): 905-923.
[27] YANG P, NAGASE T. In analysis of a virtual optical encryption holographic system: decrypted code using the multiple-bit virtual optical encryption holographic system based on the comsol multiphysics//2019 6th International Conference on Systems and Informatics, November 2-4, 2019, ShangHai, China. New York: IEEE, 2019, 799-803.
[28] JOHN M P. Monte Carlo methods for index computation. Mathematics of Computation, 1978, 32(143): 918-924.

基于四元数扩展的RSA算法的全息光通信系统

杨　鹏[1*], 韩建宁[2]

1. 太原工业学院 电子工程系, 山西 太原 030008;
2. 中北大学 信息与通信工程学院, 山西 太原 030051

摘　要: 针对目前水下光通信安全难题, 提出了一种具有高速、多维、大容量等诸多优点的新型全息光学加密系统。该系统将光学传播波长λ和傅里叶透镜焦距f作为构建安全数据传输、实现加密和解密过程的关键秘钥。为确保发送方和接收方数据传输的安全性, 基于三维四元数函数实现了扩展RSA(Extended RSA, ERSA)的加密过程。最后, 采用Pollard's Rho方法评估了RSA算法和ERSA算法的安全性。结果表明, 针对不安全声信道上传输消息的不可预测性和复杂性问题, ERSA算法加密比RSA算法加密具有更高的安全性。

关键词: 全息术; 四元数; 傅里叶透镜; 扩展RSA; Pollard's rho方法

引用格式: YANG Peng, HAN Jianning. A holographic optical communication system based on RSA algorithm and quaternion function. Journal of Measurement Science and Instrumentation, 2024, 15(3): 338-343.