RESEARCH ON SIGNAL PROCESSING FOR A VIRTUAL OPTICAL ENCRYPTION SYSTEM

YANG PENG

A Dissertation Submitted to the Graduate School of Science and Technology. In Partial Fulfillment of the Requirements for the degree of Doctor of Philosophy (Ph.D.) in Engineering

Graduate School of Science and Technology

Hirosaki University, Japan

2021

ABSTRACT

In recently rapid development of computers and information technology, the digital information on the public networks is often unable to resist unauthorized attacks. To make a system more secure, a robust encryption algorithm should be designed an encryption system that encryption keys are unique and unpredictable. Some existent systems are using long-size encryption key, however, a long size encryption key will create another problem which is the speed and the efficiency of the encryption process. It means that increasing security of a message will scarify in the processing speed. The optical encryption technology based on holographic is relying on a new technology that has many advantages such as high speed, multi-dimensional and high capacity.

This research's work presents a new method for encrypting holographic information based on optical and acoustic signals called a Virtual Optical Holographic Encryption (VOHE) system for underwater communications that can be applicable for communications between deep submergence research vehicles. The optical encryption system provides essential parameters for constructing secure communications such as the propagation wavelength (λ) and focal length (*f*) of the Fourier lens, which are considered as keys for implementing encryption and decryption processes. The transmission's media such as optical signals and acoustic signals are implemented as means for sending interference fringe pattern (IFP) that carries object information to a receiver. The optical signal is used to encrypt the object information, and the encrypted signal is carried by an acoustic signal, and then the signal will be transmitted to the acoustic channel for a long-distance transmission.

The VOHE system employs virtual optical encryption system was simulated based on COMSOL Multiphysics simulation software. The encrypted signal of precedent VOHE systems was based on a

symmetric key encryption method. In this method, two users such as a sender and a receiver select a VOHE system's key (λ, f) in advance then they use the VOHE system's key to communicate a system's cipher (IFP) over a public channel. Occasionally, users can exchange system's keys periodically. However, the VOHE system may lose system's keys during keys exchange processes. To solve this problem and to strengthen the security over VOHE, hybrid algorithms of Diffie-Hellman (DH) and RSA are introduced.

Both RSA and the DH algorithms are recently used as the foundation for the security we use today. However, these technologies are limited for reinforcing security for data transmission. In this research's project, we introduce two encryption systems, the first one is based on RSA algorithm called an expanded RSA (ERSA) algorithm, and the second one is based on an expanded Diffie-Hellman (EDH) algorithm. Both systems are using complex functions for sending crucial data such as system's key (λ, f) for ERSA algorithm and encrypted holographic information (IFP) for EDH algorithm, respectively.

To evaluate the security and efficiency of the proposed ERSA algorithm and EDH-C algorithm, an expanded Pollard's Rho method was applied and the obtained results have been investigated.

In the VOHE system, the ERSA algorithm for encrypting system's key (λ, f) and the EDH-C algorithm for encrypting system information (IFP), respectively, are more appropriate methods for strengthening the security of the data transmissions.

To determine accuracy of the information retrieved by the proposed technique, the minimum mean square error (MMSE) was conducted to evaluate the accuracy of the received signal. Numerous results of comparison between the EDH algorithm and the traditional DH algorithm have been acquired. From the results of MMSE, we have perceived higher MMSE for traditional DH than EDH algorithm. We

concluded that the EDH method has the highest performance than DH method in view of MMSE.

Finally, the National Institute of Standards and Technology (NIST) method is applied to evaluate the security of proposed ERSA and EDH-C algorithms in view of randomness, unpredictability and complexity of the transmitted message over an insecure channel. The results have showed that both ERSA and EDH-C are capable to provide highest security than RSA and conventional DH, respectively.

In our future research, we will broaden our investigation by comparing EDH-C algorithm and ERSA algorithm with other various hyper-complex number systems. We considered in this paper that the encryption process was done between only two nodes. In future research, we will further investigate the security of data transmissions over multi-node network systems.

Keywords: Optical encryption, Holographic, Fourier lens, EDH algorithm, ERSA algorithm, Pollard's Rho, NIST.

ACKNOWLEDGMENTS

First of all, I would like to express my sincere gratitude and appreciation to my supervisor Professor Dr. Tsutomu Zeniya and Associate Professor Dr. Tomoyuki Nagase for giving me an opportunity to work towards Ph. D in their laboratory and for their helpful suggestions academically, professionally, and personally to go forward during my Ph. D program.

I would like to thank Professor Dr. Toshiki Kanamoto, Hirosaki University, for his kind suggestions and helpful discussion on my research.

I would like to thanks Professor Dr. Guoqing Guan and Professor Dr. Abuliti Abudula, Hirosaki University, for their helpful advices, good suggestions and supports of my study.

I would like to thank all members in our group for their helps and supports to my research.

Finally, I would like to thank my dear family for their support. My wife has supported me every step of the way, and without her I wouldn't be where I am today. Words cannot express my gratitude.

Thank you all.

YANG PENG

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

VOHE	Virtual Optical Holographic Encryption
RSA	Rivest Shamir Adleman
ERSA	Expanded RSA
DH	Diffie-Hellman
EDH	Expanded Diffie-Hellman
MSE	Mean Square Error
NIST	National Institute of Standards and Technology
SLM	Spatial Light Modulator
CCD	Charge Coupled Device
SNR	Signal to Noise Ratio
IFP	Interference Fringe Pattern
MOD	Holographic refractive index modulator function
FT	Fourier Transformation
PK	Public key
SK	Shared Key
HK17	Hecht and Kamlofsky 2017
ST	Secret text

Chapter 1

INTRODUCTION

1.1. General Introduction

The origins of optical information processing can be traced back to holograms proposed in the late 1940s, optical transmission in the 1950s, and lasers invented in the 1960s. It is a new interdisciplinary subject which is continually developing for numerous fields. The advantages of optical information processing are mainly reflected in the advantages of high-parallelism, high-speed processing and large-capacity storage, so optical information processing is widely utilized in the image processing, feature recognition, security authentication, information storage, holographic display, data computing and other areas in digital information processing.

In recent years, with the rapid development of the Internet technology, the demand for information transmission and processing for daily life has been widely increased. Regardless of recent improvement and development of computer and communications technology, it’s still need for providing high secure data transmissions. Mathematical theories are becoming more challenge for providing remarkably resilient base for information security. However, make it difficult for traditional conventional cryptology meet the needs of today's information security which is required a more serious or higher level of data protection. Optical information security technology is rapidly developing and it has the potential for providing reliable security for data transmission.

The light is used as the carrier of information, which has a unique advantage in the process of information processing. Firstly, the transmission of light has high-speed, parallel characteristics, wide

spectrum of the wavelength and it's able to carry a massive information capacity. Secondly, the light also has a variety of properties such as amplitude, phase, and polarization and so on. These advantages fully demonstrate the right advantages of using optical information processing technology to transmit and protect data compared to electronic means.

Optical information processing technology has been applied to the field of information security since the 1980s. The specific parameters of optical system provide a strong safeguard guarantee for optical information processing in the field of information security, such as wavelength of light, properties of optical elements, transmission distance, polarization state, diffraction, interference, optical modulation such as Amplitude Modulation (AM), Phase Modulation (PM), Frequency Modulation (FM), multi-dimensional, multi-degree-of-freedom physical parameters and various forms of transformation, which provide a broad platform for optical information security.

In recent years, various electronic devices such as the performance of a spatial light modulator (SLM) and a charge coupled device (CCD) have been improved in view of providing high performance. The optical information technology has been utilized in the information security. The information processing system which include photo-electricity, optics and digital processing has become a hot topic and an important part of contemporary research. Recently, various strategies have been proposed, which are widely used in the fields of information hiding, information storage, image recognition, image encryption, security authentication, copyright protection and other fields [1, 2].

Many researches have been dedicated for optical encryption, one of these research is a double random phase encoding optical encryption model proposed by Refregier and Javidi, optical information processing has become an important means to protect information security and has been widely used and studied [3]. Recently, due to the unique advantages of optical technology in

information processing, great attention has been paid to the field of optical information security, especially in the field of double random phase coding system which is one of the most widely studied optical information security systems. These systems are designed for greatly improving the flexibility, efficiency and security of optical cryptoscopic systems [4].

The benefits of optical cryptosystem are summarized below [5]:

(1) Optical devices, such as spatial light modulators and lenses, have the characteristics of parallel processing, and the optical hardware has high processing performances, e, g, in an image processing system, it can process each pixel of the input image simultaneously, which exhibits higher performance when compared to electronical devices.

(2) Various optical parameters such as wavelength, polarization and phase thus far have been studied as keys for the optical encryption system.

(3) Generally, optical encryption systems are used to store and process of information security, and a typical optical security system typically contains specific optical devices such as light sources, lenses, detectors, and spatial light modulators.

Combined with the current research status of optical information processing technology, this section focuses on the development of optical information security technology in recent years, such as optical information security certification (in subsection 1.1.1); optical encryption based on double random phase coding (in subsection 1.1.2); optical encryption based on the coherent diffraction imaging (in subsection 1.1.3); and optical cryptography system security analysis (in subsection 1.1.4).

1.1.1. Optical information security certification

Optical information processing technology has been widely used in the fields of information security certification and information protection over the past few decades. Among them, Javidi *et al*. [6] has

made a series of research achievements, promoting their wide attention. In 1990s, based on the random phase encoding for image encryption and security certification, the technology with high security, robustness and other advantages were widely used in credit cards, passports and other products were proposed. In 1999, the safety certification technology of optical nonlinear joint transformation correlation (NJTC) proposed by Weber *et al.*[7], which not only showed great advantages in the anti-counterfeiting detection and identity security authentication of personal files, but also could be well applied to the security authentication of network information. Subsequently, a number of researchers published high-speed fingerprint recognition based on joint transformation correlation [8], biometric identification [9] and other research results.

In recent years, photon counting imaging technology has also been widely used in optical information security certification systems, and has become a hotspot of scholars [10-12]. In 2011, a new optical information security certification scheme in combination with photon counting imaging and double random phase coding has been proposed by Javidi *et al*. for the first time, and a sparse matrix distribution will be produced in the encryption process. Decrypted images cannot see any information through visual inspection, only through nonlinear correlation operations can be displayed, the proposal of this scheme is a good solution to the double random phase coding system and it can protect data from vulnerable attacks [12]. Subsequently, based on the principle of interference and Hash functions, He *et al*. [13] proposed optical hierarchical authentication technology in which password keys, one-way Hash functions and phase keys can be used as conditions for verification, thus providing greater security. Nishchall *et al.* [14] proposed optical image encryption and authentication schemes based on fractional joint transformation correlations. Simultaneously, he has proposed an optical information encryption and authentication scheme using the asymmetric key. [15]. Recently,

based on phase recovery algorithm and double random phase coding system, Chen and Wang *et al*. [16-18] proposed an authentication scheme using photon counting. Zhao *et al.* [19] proposed an information verification system based on the double random phase coding system with fingerprint which was used as a key, the recipient could decrypt the authenticity of the document by decrypting the fingerprint.

1.1.2. Optical encryption based on the double random phase encoding

In 1995, an optical image encryption system based on the theory of a 4*f* system proposed by Refregier and Javidi was constructed with double random phase encoding as key, and successfully realized the function of encrypting and decrypting data by optical method. Since then, the obtained results have been improved and continuously advanced levels of this technology have been presented. Based on further research on the double random phase coding system, Wang *et al*. [20] proposed a method that could change the performance of the system. At the same time, based on the double random phase coding technology was extended to the fraction Fourier transformation domain. Unnikrishnan *et al*. [21] introduced the fraction Fourier transformation order as the key of the system by expanding the key space and improving the security of the system. Liu *et al*. [22] proposed an optical image encryption scheme for multi-fractional Fourier Transformation (MFRFT), which is a broad score Fourier transformation. In addition to retaining the original fraction Fourier transformation key, the extended period can also be used as a system key. In 2004, a double random phase coding encryption technique in the Fresnel domain was proposed by Zhang and Situ *et al*. [23, 24], where the system keys were considered distances between planes, light wavelength and phase codes. Subsequently, Pei *et al.* [25] extended the double random phase encryption technology to cascading fractional Fourier transformation and multi-parameter discrete fractional Fourier transformation

respectively, which played a great role in further research. In 2007, based on the integral variation of the fractional Fourier transformation, Liu *et al.* [26] proposed an optical image encryption method, which can be easily implemented by single-lens or double-lens optical devices. Tao *et al*. [27] proposed a double image encryption scheme in the fractional Fourier transformation domain by using the double random phase coding technology. In 2008, they expanded double random phase coding technology to multi-parameter fraction Fourier transformation domains [28]. Then, based on the multi-parameter fraction Fourier transformation, the scholars put forward a series of image encryption schemes, which have greatly enriched the application of the transformation algorithm in the field of image encryption [29-34]. Based on the study of the weighted-type fractional Fourier transformation, Ran *et al*. [35-38] proposed a modified multi-parameter fractional Fourier transformation, which improved the security of the system without increasing the cost of hardware. Subsequently, they proposed a system that was based on expanding a transform order from a real number to a real vector, while expanding the key spatial dimensionality to provide greater security.

In recent years, research are paying attention to the encryption of various color images based on the double random phase coding, which include RGB pixel displacements [39], the affine transformation in gyrator transform [40], the sine chaotic mapping and DNA coding scheme [41], the chaotic tent map image cipher [42], the double self-adaptive encryption scheme [43], and Block-based light-colored code [44].

1.1.3. Optical encryption based on the coherent diffraction imaging

Recently, the image encryption scheme based on optically coherent diffraction theory is a new hot spot in the field of optical information security [45]. This method has the advantages of simple encryption/decryption operations and high security, and has attracted the wide attention of experts in

this field [46]. Based on the coherent diffraction technology, Zhang *et al*. encrypt a plain text image into two phases, the decryption processed only CCD or other light-strength detectors to recover plain text information [47, 48]. Subsequently, based on diffraction imaging technology, Chen *et al.* proposed an optical color image encryption scheme [49, 50]. The feasibility of interference theory in image encryption that was verified by Zhu *et al.*, has been experimented and extensively studied that is related to an optical information security [51, 52]. In 2010, based on optical interference principle combined with phase recovery algorithm, a multi-image encryption scheme was proposed by Niu *et al.* [53]. Also, the class flow ciphers for the encryption system were also investigated by Chen *et al*. [54].

Several studies have been investigated in optical image encryption, such as the "Silhouette problem" which is derived from optical interference methods in two phases [55, 56]. The Jigsaw transformation method which was used by Kumar *et al*. [57] for re-encrypt the two phases, thereby solving the "Silhouette problem". Wang *et al*. [58, 59] have further studied the application of optical interference technology to encrypt known plain text images for three phases, which is also a good way for removing "Silhouette problem". Compared with the traditional method that is based on the principle of enhanced optical interference, Liu *et al.* [60] proposed an optical color image encryption scheme, which was based on phase recovery algorithm and linear phase color-blend technology, thus completely eliminating the silhouette problem.

1.1.4. The security analysis of the optical encryption system

The unique advantages of optics in information processing, optical cryptoscopic system security analysis were studied by more and more scholars. Until 2005, Carnicer *et al*. [61] first proposed a chosen - cipher text attacks for double random phase encoding, and they successfully obtained the system key by designing the cipher text. Based on the linear characteristics of the double random phase

coding system, the linear equation system between plain text and cipher text was utilized by Frauel *et al*. [62]. The solution satisfied the linear equation system that was considered as a key to recover plain text information, thereby cracking the system successfully. Subsequently, according to the simulated annealing (SA) algorithm, Gopinathan *et al.* [63] proposed a known plain text attack scheme for the double random phase coding system, and successfully obtained the frequency domain key under a condition for obtaining the real amplitude encoding.

In 2006, according to the HIO (hybrid input-output) algorithm, Peng *et al*. [64] proposed a known plain text attack scheme for double random phase coding systems. In this scenario, the HIO algorithm was firstly used by the attacker to obtain a key for the airspace. Therefore, the first random phase encoding and the linear correspondence of the system were used to obtain the frequency domain key [65]. Meanwhile, based on the Fresnel domain, they also proposed the choice of plain-text attack scheme. The biggest advantage of this scenario is that the decryption results of the attack scenario are non-destructive. Subsequently, the double random phase coding system was further studied by them, and the attack scheme of the only secret text was proposed [66]. This scenario was employed a hybrid iteration method, from which plain text information can be obtained directly from the cipher text. Based on POCS (projection-onto-constraint-sets) algorithm and double random phase coding system analysis, Situ *et al*. [67-69] obtained the system key using multiple sets of known plain text-cipher text.

In 2008, based on multi-parameters Discrete Fraction Fourier transformation domains, Youssef *et al*. [70] proposed a known plain text attack scheme for double random phase encoding image encryption systems. In this scheme, a linear equation system is established according to the linear relationship between plain text and the cipher text, and the system is solved by solving the linear equation system.

In 2009, Qin and Peng *et al*. [71] utilized phase retrieval algorithms to propose a known-plaintext attack scheme for the double random phase coding system of the Fraction Fourier transformation domain, and has successfully obtained the phase encoding key and the order key. In 2010, Fredy *et al*. [72] that was based on a joint transformation correlation encryption system, they proposed a chosen plain text attack scheme in which three sets of plain texts were required to obtain the system key. In 2011, Qin *et al*. [73] proposed a chosen plain text attack scheme based on the joint transformation correlation encryption system, which requires only a set of plaintext-ciphertext to obtain the key to the system. Simultaneously, the authors found a collision in a further study of the optical cryptosystem, that is, the same output was produced by two different plaintext inputs [68, 74, 75]. Recently, several security analysis for cryptosystems have been investigated, such specific attack scheme [76], Common attacks [77], and Hybrid attacks [78] for image encryption systems based on phase-truncated Fourier transformations.

1.2. Cryptology

Cryptology is a method for securing data and data communications in the presence of third parties called adversaries [79]. As shown in Fig. 1.1, the field of cryptology which the scientific study of cryptography and cryptanalysis splits into two main branches: Cryptography and Cryptanalysis. Among cryptography, the algorithm is divided into three main branches： Symmetric Algorithms, Asymmetric (or Public-Key) Algorithms and Cryptographic Protocols. Furthermore, cryptanalysis is use for the analyzing information systems to study the hidden aspects of the systems, which is the breach cryptographic security systems to obtain the contents of encrypted messages under unknown cryptographic key. To create a cryptography, it should be taken into consideration of cryptanalysis. According to the results of cryptanalysts, the cryptanalysis can be roughly classified into the following

four categories: Cipher text only, Known plaintext, Chosen plaintext and Chosen cipher text as described in Fig. 1.2.

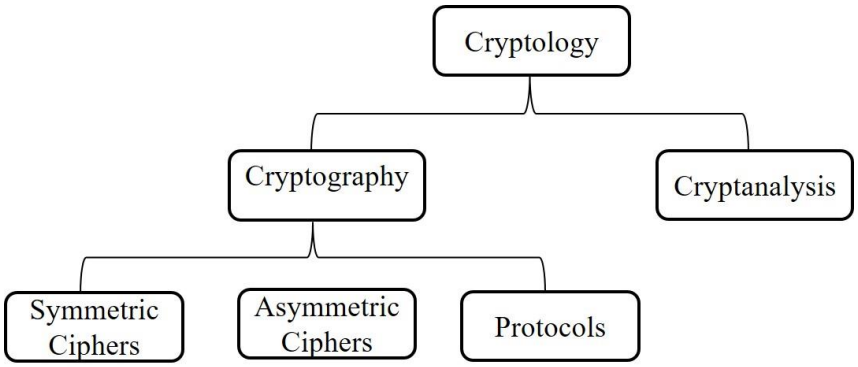

Figure 1.1. Overview of the field of cryptology

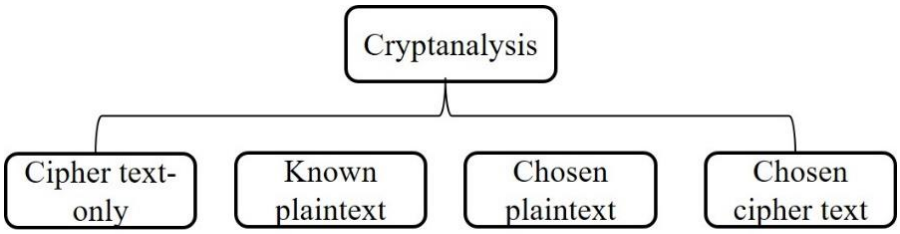

Figure 1.2 The classification of cryptanalysis

1.2.1. Symmetric cryptography

Symmetric cryptographic algorithms are known as symmetric key, secret key, or a single key algorithms. Symmetric key algorithms are used the same cryptographic keys to encrypt plaintext and decrypt the cipher text. These keys may be the identical, or they may be simply converted between the two keys [80]. One of the main disadvantages is both parties are required to obtain the same key's value, in contrast to symmetrical key encryption, asymmetrical key encryption requires both parties having different key's value.

Symmetry key algorithms can be divided into two types of operation, one is stream ciphers, which operates on a single bit of plaintext, and the other is the block-based ciphers, which operates on a set of bits in plaintext [81].

In the symmetrical cryptography system shown in Fig.1.3, there are five components: Plaintext, Encryption algorithm, Keys, Cipher text and Decryption algorithm.

Plaintext：Original information.

Key：The key used in encryption and decryption algorithms, which directly affect the results of the transformation.

Encryption algorithms： A variety of transformation and conversion methods are implemented on plaintext using keys as parameters.

Cipher text：The results obtained by encrypting plaintext.

Decryption algorithm：The inverse transformation of the encryption algorithm for the cipher text, and the result obtained is the plaintext.

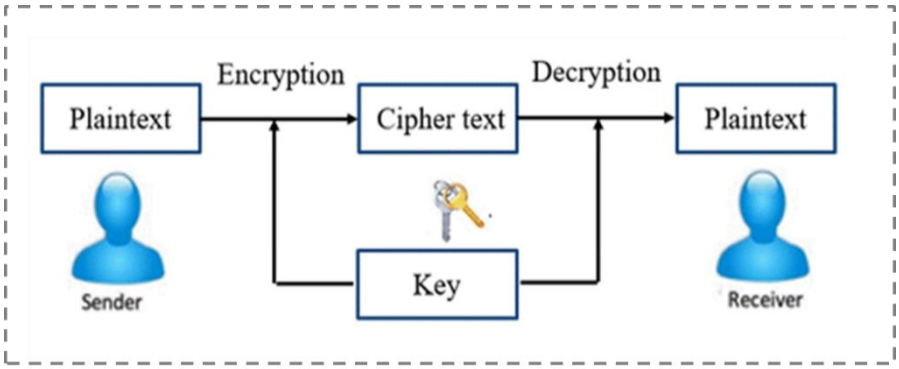

Figure 1.3. Symmetric cryptosystem

1.2.2. Asymmetric (or Public-Key) cryptography

Asymmetrical cryptography is a cryptographic system, which use key pairs: public keys (openly propagated) and private keys (only owner by the known). Therefore, effective security requires only keeping the private key private, and the public key can be publicly distributed without compromise [82]. The encryption and decryption process of the asymmetric cryptography system is shown in Fig. 1.4. The main feature of the system is that each user has two keys, a public key and a private key (the public key is exposed as an encryption key and the private key is kept private as a decryption key).

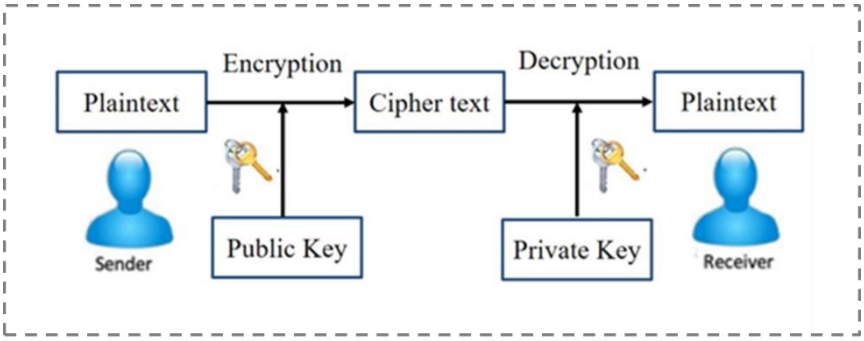

Figure 1.4. Asymmetric cryptosystem

At present, although there are many kinds of asymmetric cryptographic systems, and recently, two kinds of applications are widely applied: the first one is based on the decomposition of large integer factors, *eg*., the RSA public key algorithm [83], the other ones is based on discrete logarithm problem, *eg*., the elliptic curve (ECC) public key cryptographic algorithm [84, 85].

The difference between the symmetric and the asymmetric encryption algorithm could be summarized as follow. Firstly, the symmetric algorithm uses the same-key system for encryption and decryption process, however, the different keys are used for the asymmetric algorithm. Secondly, compared with asymmetric algorithm, symmetrical algorithm can complete the processing in shorter time.

According to the cryptographic system discussed above, a structural diagram of the classification of the cryptographic system can be drawn, as shown in Fig. 1.5.

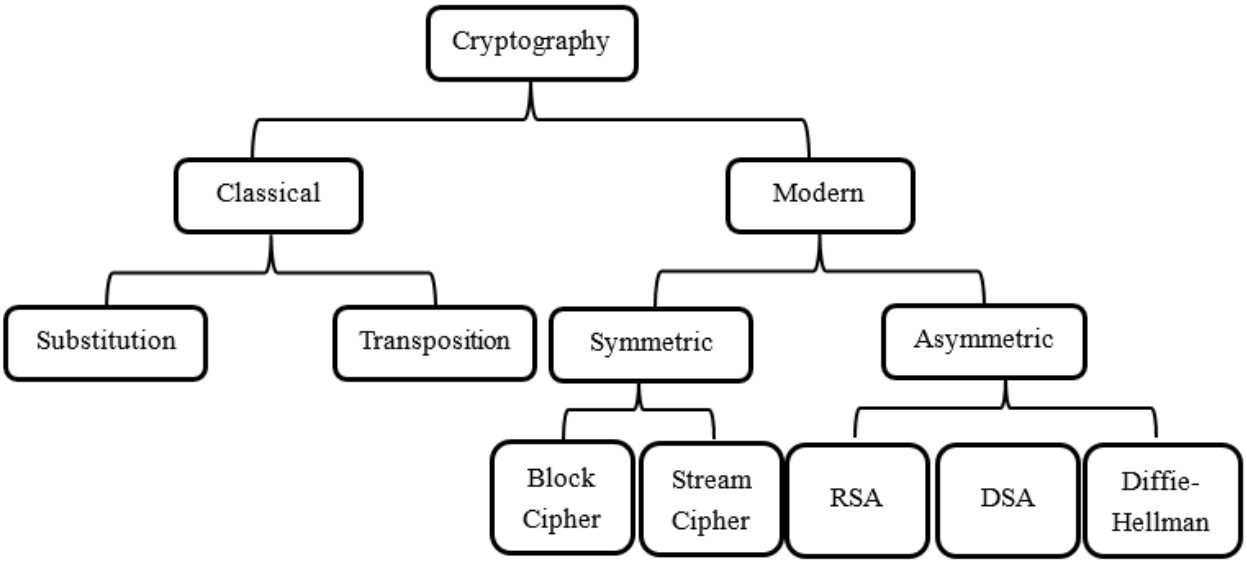

Figure 1.5. The classification of cryptosystem

1.2.3. Security and performance evaluation

Security and performance evaluation are important to study of crypto-algorithms. This section describes the quantitative parameters which are used in the evaluation that is shown in Appendix 1 and Appendix 2, respectively.

(1) Key size

In cryptography, key size or key length is the number of bits, which is used for a cryptographic algorithm (such as a cipher) [86, 87]. The key size usually indicates the security upper-bound of an encryption algorithm. Ideally, the key size will be consistent with the lower-bound of algorithm security. Indeed, most symmetric key algorithms are designed to have security equal to their key size.

Definition 1: The key size of a multi-dimensional (Integer and Complex number) is the total length of all its parts (real or imaginary numbers).

Table 1.1 The key size of integer and complex number

Item	Expression	The size of key
Integer	x	Length (x)

Complex number	$(x + iy)$	Length (x)+ Length (y)

(2) Security bit (S-bit)

To evaluate the security of a cipher, it is necessary to find a decryption algorithm that estimate how much effort is required to decrypt the cipher [88]. Hence, the security of a cipher is defined by the amount of computation required to decrypt the cipher using the most efficient algorithm. For instance, if the decryption complexity of a cipher is about 3^k, the security of the cipher is k-bit.

The safety of the algorithm proposed in our research is based on the difficulty of solving discrete logarithm problem. Therefore, the complexity of the calculation by calculating the remaining operation ($3^k \bmod g$). Hence, the complexity of the calculation is determined from the number of cyclic group's elements that can be generated from the generator.

Definition 2: S-bit is an element of a cyclic group that can be generated from Generator G = < g > for some element g.

$$\text{S.bit}[g] = \text{card}(<G>),\ G = <g>$$

As an example, the Pollard's rho method shows how to calculate private key a, out loop i and processing time t of PK_a. ($PK_a = g^a \bmod p$).

Pollard's rho method
Input: p :($\|p\|^2$ is prime number), $PK_a, g \in [0, \|p\|^2 - 1]$
s.t $PK_a = g^a \bmod p$.
Start = time. Clock
1: $i := 0$
2: Repeat
3: i ++
4: Choose $a_i, \beta_i \in [0, \|p\|^2 - 2]$ randomly
5: $c_i = (PK)^{a_i} g^{\beta_i} mod(\|p\|^2 - 1)$

6: until $\exists_j \text{ s.t. } 1 \le j \le i, c_j = c_i$

7: $a = (\beta_j - \beta_i)(\alpha_i - \alpha_j)^{-1} mod\ (|p|^2 - 1)$

8: t = time. Clock - Start

9: Output *a, i* and *t.*

(3) National Institute of Standards and Technology (NIST)

This section evaluates the security of a cipher based on a statistical test suite for random and pseudorandom number generators for cryptographic applications NIST test, as show in Table 1.2.

Table 1.2. NIST test

	Test Items	Definition
1	Frequency	The test is the proportion of zeroes and ones for the entire sequence
2	Block Frequency	The test is the proportion of ones within M-bit blocks.
3	Cumulative Sums	This test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (-1, +1) digits in the sequence.
4	Runs	The test focuses on the total number of runs in the sequence.
5	Longest Run	Test for the Longest Run of Ones in a Block
6	Rank	the test is the rank of disjoint sub-matrices of the entire sequence
7	Approximate Entropy	As with the Serial test, this test is the frequency of all possible overlapping m-bit patterns across the entire sequence.
8	Serial	This test is the frequency of all possible overlapping m-bit patterns across the entire sequence.
9	Linear Complexity	The test is to determine whether the sequence is complex enough not to be considered random.
10	FFT	The test is the peak height in the Discrete Fourier transformation of sequence.

1.3. Basic Theory and Research Methods

The development of digital holographic technology is emerging as an outstanding solution for protecting the data and data transmissions, and opened up a whole new field of optical information security [89-98].

In 2000, the method of combining digital holographic technology with double random phase encoding encryption proposed by Javidi *et al*. [90], which is a good way to store information. In the same year, E. Tajahuerce *et al*. [90] used digital holographic techniques to record 3D objects to extend

encryption to encrypted 3D objects.

Chen and Zhao *et al.* [99] applied holography to the color image encryption, which encrypted the color images into three holograms. The three pictures after decryption were synthesized to restore the original color picture. Li *et al*. [46] employed holographic technology to combine optical encryption with image-hiding technology to encrypt images. Compared with traditional optical holograms, digital holography have the advantage of an effective method of digitizing encrypted data.

1.3.1. The Fourier transform properties of the lens

As early as a century ago, the German scientist E. Abbe first proposed that the Fourier lens can realize the characteristics of Fourier transformation. Meanwhile theoretical and practical challenges have been accelerated to develop applications for optical information processing [2].

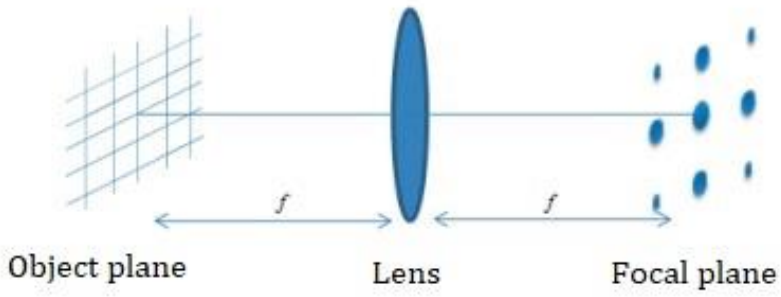

Figure 1.6. Fourier transform to achieve process for lens

The Fourier transformation implementation of the lens, as shown in Fig. 1.6. The wave passes through the Fourier lens with a focal length *f*. In Fourier optics, the process of the wave that is focused on Fourier lens, which is called a Fourier transformation. The amplitude of the complex field in the image plane is calculated by:

$$F(u,v) = \frac{1}{i\lambda f} e^{-i\frac{k}{2f}(1-\frac{d}{f})(u^2+v^2)} \cdot \iint f(x,y)P(x,y)e^{i2\pi(ux+vy)}\,dxdy \qquad (1.1)$$

Where, $P(x, y)$ represents the aperture function, but in general the default value is 1, considering that the input information passes through the lens unobstructed, λ is the wavelength, f is the focal

length, $f(x, y)$ is the signal of the object plane. When the incoming signal is on the front focal plane, there is $d = f$, at which point the formula (1.1) can be reduced to the standard Fourier transformation, i.e.:

$$F(u, v) = \frac{1}{i\lambda f} \iint f(x, y) e^{i2\pi(ux+vy)} \, dxdy \tag{1.2}$$

Where, (u, v) is the spatial coordinates in Fourier/image space, and (x, y) is the coordinates in the spatial domain. Optics have great advantages in information processing, and the use of optics can realize Fourier transformation quickly, efficiently and simultaneously, which can save time and greatly improve the computing efficiency in the process of two-dimensional information processing of large data volume. The spectrum information $F(u, v)$ obtained after Fourier transformations is generally a complex function that can be calculated by:

$$F(u, v) = |F(u, v)| e^{i\varphi(u,v)} \tag{1.3}$$

Optical information processing is developing rapidly due to the Fourier transformation characteristics of the lens. In recent years, optical information security has attracted the attention of many researchers, and a variety of optical system-based research results (such as security authentication, image encryption, watermarking technology, etc.) have been proposed.

1.3.2. The Fourier-transformed digital holography

In optical information processing, light-intensity detectors such as CCD can only record intensity information and cannot obtain phase information by using traditional imaging techniques. However, holographic techniques are used to record the distribution of the intensity in interference fringes, thereby it records the amplitude and phase of the object. The emergence of digital holographic technology has greatly promoted the development of optical information processing.

Digital holographic technology using light-strength detectors such as CCD cameras replaces

traditional holographic technology, which is a good way to avoid wet processing of the data medium in holographic technology. In digital holographic technology, computers are used to store the intensity spectrum recorded in photodetectors, which can easily realize the processing and transmission of information.

The optical schematics for the recording and reconstruction of the Fourier-transformed digital holography are shown in Fig. 1.7.

In the holographic recording process, the object wave U_o is calculated by:

$$U_o(x, y) = |U_o|e^{i\varphi_o(x,y)} \tag{1.4}$$

Where, $|U_O|$ is the real amplitude of the object wave, $\varphi_o(x,y)$ is the phase of the object wave.

The reference wave is calculated by:

$$U_R(u, v) = |U_R|e^{i\varphi_R(x,y)}e^{i2\pi f_o x} \tag{1.5}$$

Where, f_o is the wave front tilt of the reference wave, $|U_R|$ is the real amplitude of the reference wave, $\varphi_R(x,y)$ is the phase of the reference wave.

Thus, the interference fringe pattern (IFP) of the Fourier spectrum and reference wave recorded on the CCD, i.e. the Fourier Transformation Hologram, which is calculated by:

$$I(x,y) = |U_o(x,y) + U_R(x,y)|^2 = |U_o|^2 + |U_R|^2 + 2U_oU_R\cos[\varphi_o(x,y) - \varphi_R(x,y) + 2\pi f_o x] = a(x,y) + b(x,y)\cos[\varphi(x,y) + 2\pi f_o x] \tag{1.6}$$

Where, a (x, y) is the average strength of the interferogram, b (x, y) is the modulation of the interference fringes, $\varphi(x, y)$ is the phase difference between object and reference wave.

$$I(u, v) = a(x, y) + c(x,y)e^{i2\pi f_o x} + c^*(x,y)e^{-i2\pi f_o x} \tag{1.7}$$

Where, c (x, y) = $1/2\, b(x,y)e^{i\varphi(x,y)}$, c^* (x, y) is the complex conjugates of c (x, y). Fourier transform was applied to the above equation (3) to obtain the spectral distribution of the interferogram:

$$\text{FT}\ \{I\} = A(f_x, f_y) + C(f_x - f_o, f_y) + C^*(f_x + f_o, f_y) \tag{1.8}$$

Where, (f_x, f_y) is the domain coordinates of the interferogram in the spectrum.

FT $\{I(x, y)\}$ is a Fourier transformation of the inner part of the parentheses as shown in Fig. 1.7 (a); $a(x, y)$, $c(x, y)$ and $c^*(x, y)$ are transformed by FT to A, C, and C^*, respectively. A is the zero frequency component at the center optical axis, while C and C^* are located at coordinates $x = f_o$ and $x = -f_o$, representing the original image and the conjugate image, respectively, as shown in Fig.1.7 (b).

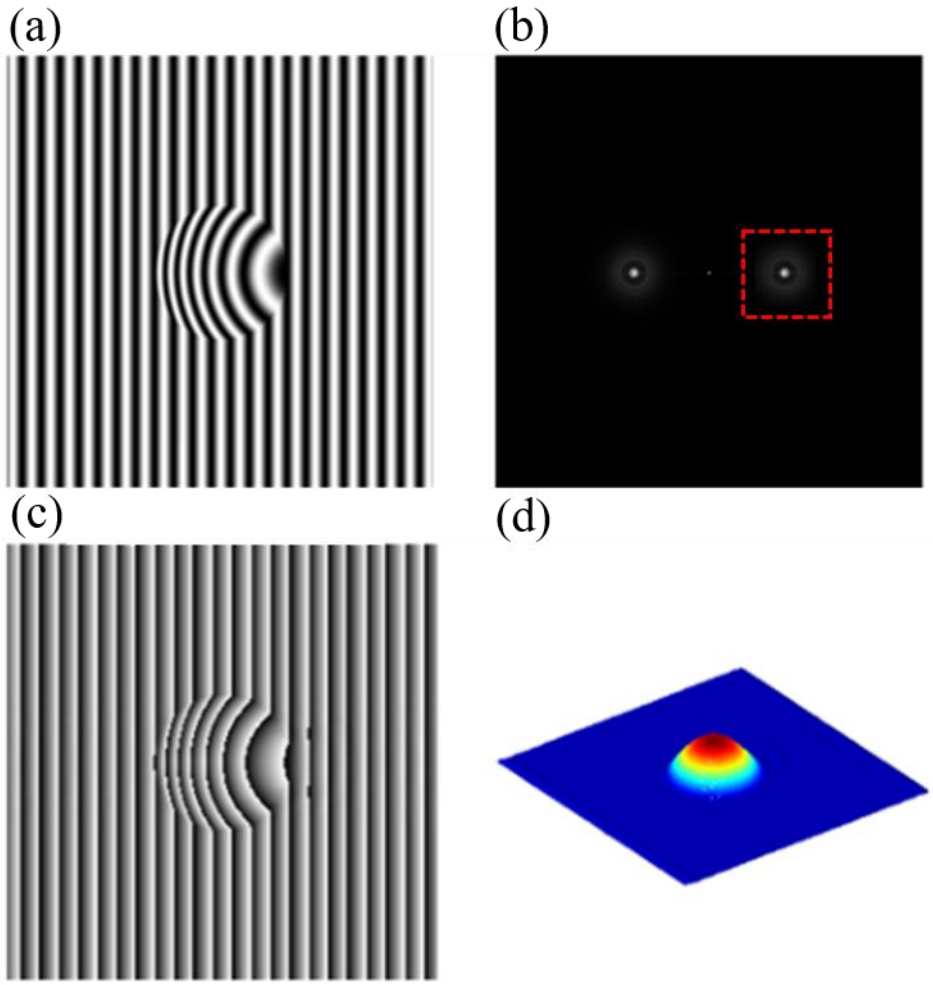

Figure 1.7. Fourier transform: (a) $I(x, y)$, (b) FT $[I(x, y)]$; Fourier transform: (c) the phase $[\varphi(x, y) + 2\pi f_o x]$, (d) the phase $\varphi(x, y)$.

Then, in the holographic reconstruction process: the bandpass filter is used to filter out the real image in the spectrum, which is marked by the red rectangle in Fig. 1.7 (b), and inverse Fourier

transform is applied to the filtering result to obtain the complex amplitude:

$$c'(x, y) = \text{IFT}\ [\ \text{FT}\ [I(x, y)]\cdot \text{H}] \tag{1.9}$$

Where, FT and IFT are Fourier transformations and reverse Fourier transformations, respectively, and H is a bandpass filter to filter out images in the spectrum.

Therefore, the phase $[\varphi(x, y) + 2\pi f_{\omega} x]$ of the $c'(x, y)$ is shown in Fig. 1.8 (c), which contains the tilt phase of $2\pi f_{\omega} x$. Then, the tilt phase of $2\pi f_{\omega} x$ is removed and the phase distribution $\varphi(x, y)$ of the object wave is obtained, as shown in Fig. 1.7 (d).

$$\varphi(u, v) = \arctan\ \left\{\frac{Im[c'(x,y)]}{Re[c'(x,y)]}\right\} - 2\pi\alpha x \tag{1.10}$$

Where, Im $[c'(x, y)]$ and Re $[c'(x, y)]$ represent the imaginary and real parts of $c'(x, y)$, respectively, and $2\pi f_{\omega} x$ is the tilt phase.

1.4. Objective of this Study

As reviewed above, optical encryption system especially the virtual optical holographic encryption (VOHE) system, has been widely used in recent years compared with other cryptographic systems for achieving preferable security. In summary, the VOHE system has many advantages and the optical system can not only adopt a method of building an optical light path, but also uses an encryption method as a means of providing high-end secure systems.

This work presents a new method for encrypting holographic information based on optical signals called a Virtual Optical Holographic Encryption (VOHE) system for underwater communications that can be applicable for communications between deep submergence research vehicles. The transmission medium is composed of a combination of optical signals and acoustic signals together to form the VOHE system for transmitting system information. The VOHE system provides essential parameters for constructing secure communications such as the propagation wavelength (λ) and focal length (f) of

the Fourier lens, which are considered as keys for implementing encryption and decryption processes. An asymmetric RSA algorithm is used to sends system information (λ, f) as a message to a receiver. Diffie-Hellman (DH) key exchange is one of the earliest algorithms for a key exchange, which enables both parties to securely exchange keys over unsecure.

In study, the use of Virtual Optical Holographic Encryption (VOHE) system has been intensively studied, investigated and reported [100-102]. One of our early investigation of the VOHE systems was the symmetric key encryption method. In this method, two users such as a sender and a receiver select a VOHE system's key in advance then they use the VOHE system's key to communicate a system's cipher over a public channel. Occasionally, users can able to exchange system's keys periodically. However, the VOHE system may lose system's keys during keys exchange process. To solve this problem and to strengthen the security over VOHE, the hybrid algorithms of Diffie-Hellman (DH) and RSA are introduced.

Both RSA and the DH algorithms are recently implementing for providing security for data transmission. However, the two technologies have limited related to a key's size. In RSA algorithm, the system's cipher is limited by the length of the key. The length of the VOHE system's cipher is greater than the length of the key. Hence, implementing the RSA algorithm is not suitable for sending the VOHE system's cipher as a message to the receiver. Therefore, when we periodically exchange the keys of the VOHE system, the RSA algorithm is implemented to send keys as a message to the receiver. In DH algorithm, two users set up a private and random key for the VOHE system, separately. The DH algorithm is implemented to send the VOHE system's cipher as a message to the receiver.

Furthermore, this research introduces an approach for data encryption over a VOHE system using an expanded asymmetric algorithm. The objective of this study is to develop a novel asymmetric

algorithm by adapting, remodeling and expending RSA and Diffie-Hellman algorithm, which are performed using two-dimensional complex functions. The main reason of using a complex function is to strengthen security over conventional RSA and Diffe-Hellman algorithms.

1.5. The Scope of this Dissertation

Chapter 1 reviews the past and the recent progress of development of various optical information processing for Cryptography, especially the virtual optical holographic encryption and states the objectives of this study.

In Chapter 2, the VOHE system's encryption, decryption process, RSA algorithm and Diffie-Hellman algorithm are briefly introduced, and then the additional simulation and evaluation of the VOHE system's encryption and decryption process are conducted based on COMSOL Multiphysics.

The Chapter 3 briefly introduces the ERSA (Expanded RSA) encryption algorithm, and then evaluates the security of the proposed ERSA algorithm by an extended Pollard's Rho method. We demonstrate the evaluation's process by give an example which shows how the ERSA encryption algorithm sends system information (λ, f) (for e.g., λ = 632.8 nm, f = 4.20 mm) to a receiver.

In Chapter 4, the EDH encryption algorithm is briefly introduced, and then the security of the proposed EDH algorithm is evaluated using an extended Pollard's Rho method. The example is presented of how the EDH encryption algorithm performs for generating a share key between a sender and a receiver.

In Chapter 5, the mean square error (MSE) is calculated between the original code and retrieved code; the randomness of the data transmission under EDH-C algorithm is conducted based on the National Institute of Standards and Technology (NIST) test suite for randomness. The NIST method tool is also applied to evaluate the security of the proposed ERSA algorithm.

Chapter 6 gives the general conclusions of this research and discusses the challenges and prospects for the future work.

Chapter 2

A VIRTUAL OPTICAL HOLOGRAPHIC ENCRYPTION SYSTEM

Recently, with the rapid development of optical processing technology and due to the rapid development of computers, the digital information on public networks is often unable to resist unauthorized attacks. To make a system more secure, a robust encryption algorithm should be designed with a long encryption key. However, a long size encryption key will create another problem which is the speed of the encryption process. It means that increasing security of a message will scarify in the processing speed. The optical encryption technology based on holographic is relying on a new technology that has many advantages such as high speed, multi-dimensional and high capacity [103-105]. For these reasons, the optical holographic encryption technology is gradually received great attention and considered as an enabling technology [90, 106].

A paper by Yu C *et al*., proposed a novel image encryption scheme, in which the positions of the values of image pixels were scrambled to confuse the relationship between the cipher text and the original image [107]. A new encryption technique has also been introduced by Hennelly [108] using juxtaposition of sections of the image in fractional Fourier domains. The Virtual optical encryption for holographic is a common kind of a new and a developing technology. It can handle very large computational domains which are able to increase sensitivity and reduce a signal-to-noise ratio (SNR) [109, 110].

A Virtual Optical Holographic Encryption (VOHE) technology has been widely used in recent years

for achieving better security especially in an uncommon transmission environment. Numerous research efforts have been devoted for developing encryption systems that are invulnerable to security breaches. E. Tajahuerce *et al.*, has used a holographic technique in image encryption which overcomes the difficulty of double random phase encoding [89]. In the same year, E. Tajahuerce *et al.* used a digital holographic technique to encrypt 3D objects [111]. Digital holography is often used to implement virtual optical encryption scheme. Hyun Kim *et al.* employed virtual optics to encrypt digital holograms of 3-D objects [112]. Wang *et al.* has proposed a new method for synthesizing and encrypting information using a digital holographic and a virtual optical technology [113].

The virtual optical holographic encryption (VOHE) system has been widely used in recent years compared with other cryptographic systems for achieving preferable security [106, 114].

In summary, the VOHE system has many advantages and the optical system can not only adopt a method of building an optical light path, but also uses an encryption method as a means of providing high-end secure systems [50, 115, 116].

The structure of VOHE system that is based on digital holographic is shown in Fig. 2.1. The main components of the system are a Fourier lens, a spatial light modulator (SLM) and a charge-coupled device (CCD). The Fourier lens is a special lens where the wave is focused and passed through the Fourier to generate Fourier transformation [117]. The SLM which is an electrically programmable device that modulates light wave corresponding to a special designed pattern [118]. The digital holography information is processed and collected by a charge-coupled device (CCD) [119].

The light source of VOHE system is selected from a He-Ne laser with a wavelength of 632.8 nm [120]. The laser wave passes through the wave splitter to produce two waves which are a reference wave and an object wave. Then, the object wave that passes through the SLM will acquire multi-bit

data (object information) and the output signal from SLM will proceed to the Fourier lens for focusing the object wave on the wave splitter. The output signal which is considered as a new object wave will join together with the reference wave to generate a complex interference fringe pattern (IFP). Finally, we utilize a CCD to collect IFP and transmit it to a receiver.

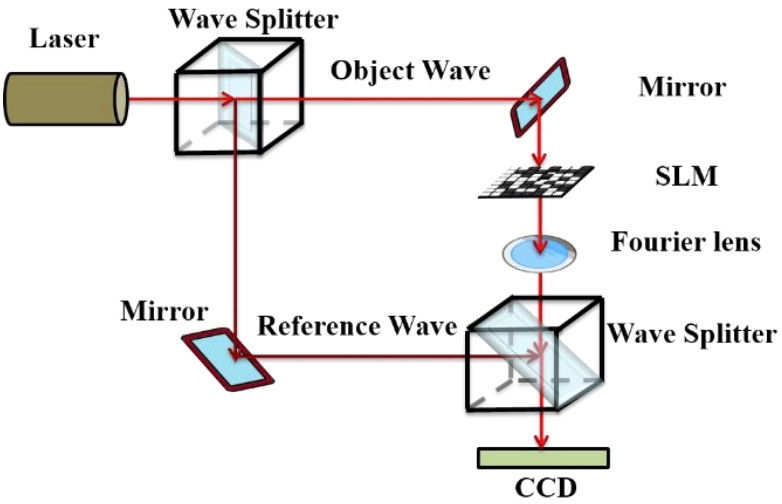

Figure 2.1. A VOHE system's model

The complex amplitude of the reference wave U_R and object wave U_o at plane $z = 0$, then U_R is given by:

$$U_R = |U_R| e^{-\frac{y^2}{w^2(x)}} e^{-\frac{inky^2}{2R(x)}} \text{ [121]} \tag{2.1}$$

Where, $|U_R|$ is the real amplitude of the reference wave; w (x) is the waist radius of the reference wave; $k = 2\pi n/\lambda_R$ is the wave number for a reference, λ_R is the reference wavelength, and n is the index of refraction of holographic material, $R(x)$ is the wave front curvature of the reference wave at distance x from the focal plane position and is defined by

$$R(x) = x[1 + (\frac{x_R}{x})^2] \tag{2.2}$$

Here, $x_R = \frac{n\pi w(x)^2}{\lambda_R}$ is the Rayleigh range.

In Fig. 2.1, firstly, the light will pass through SLM to carry object information and the output will be the object wave. Secondly, the object wave passes through the Fourier lens with a focal length *f*. In

Fourier optics, the process of the object wave that is focused by Fourier lens is called a Fourier transformation. Hence, the output from Fourier lens is U_O that is focused on holographic plane which is calculated by:

$$U_O = \frac{1}{\sqrt{\lambda_o f}} \int_{-\infty}^{\infty} E(x) e^{-i2\pi xu/\lambda_o f} dx \quad [122] \tag{2.3}$$

where, λ_o is the object wavelength, f is the focal length, $E(x)$ is object information e.g. "1011", u is the spatial coordinates in Fourier/image space and $u/\lambda_o f$ is the spatial frequency, respectively.

2.1. The Holographic Encryption and Decryption processes

To comprehend the process of a VOHE system, Fig. 2.2 is an example of how to implement Fourier Lens and digital holography for preforming encryption and decryption processes. We select a column of object's information (1011), which can be seen in the fifth row's pattern of the SLM device as shown in Fig. 2.1.

The transmission's media such as optical signals and acoustic signals are implemented as means for sending interference fringe pattern (IFP) that carries object information to a receiver [101]. The transmission's media such as optical signals combined with acoustic signals are implemented as means to send IFP, as shown Fig. 2.2, that carries object information to a receiver [123]. The optical signal is used to encrypt the object information, and the encrypted signal is carried by an acoustic signal, and then the signal will be transmitted to the acoustic channel for long-distance transmission.

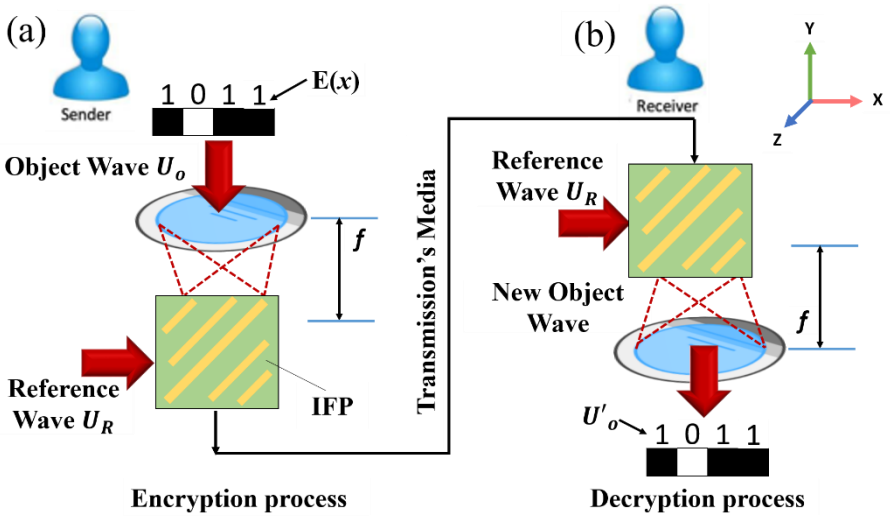

Figure 2.2. A schematic diagram of holographic encryption and decryption.

(a) Encryption process; (b) Decryption process

2.1.1. Holographic Encryption

At the sender site, Fig. 2.2 (a) shows the object wave that passes through the SLM is focused on the Fourier lens with a focal length of *f* which is considered as a first encryption key, and the output signal from the Fourier lens is regarded as an initial cipher. Then, the initial cipher will join the reference wave with a length of λ_R which is considered as a second encryption key for generating a second cipher called interference fringe pattern (IFP). This process is called the encryption process by which the IFP is transmitted to a receiver.

The electric field intensity of the IFP is calculated by:

$$I(x, y) = |U_R + U_O|^2 \tag{2.4}$$

2.1.2. Holographic Decryption

At the receiver site, in Fig. 2.2 (b), the decryption process is done by illuminating only the reference wave with a length of λ_R which is considered as a first decryption key to produce a new object wave. Then, the focal length *f* is referred as a second decryption key, and the new object wave that passes through the Fourier lens is transformed to a digital stream.

The decryption process is the inverse of the above encryption process. In the Fig. 2.2 (b), the IFP is modulated and illuminated only by the reference wave to produces an image of new object wave $I'(x, y)$ which is giving by:

$$I'(x, y) = \text{MOD}\,[I(x, y)] \times U_R \tag{2.5}$$

where MOD is a holographic refractive index modulator function, which modulates holographic material refractive index based on an above certain threshold value of electric field intensity [124]. Where, MOD = $n + dn \times ((I(x, y) / \max[I(x, y)])^2 > \text{TH})$, dn is modulation coefficient, the max operator calculates the maximum value within (x, y) domains, and TH is an exposure threshold.

To obtain the retrieved original image U'_o that is carried by $I'(x, y)$, the Fourier transformation in the Fresnel approximation is applied as

$$U'_o = \text{FT}\,[I'(x, y)] \tag{2.6}$$

where, FT represents Fourier transformation.

In the encryption and decryption processes, the reference wave should match and well-coordinated with these two processes to achieve a best outcome [100]. Hence, the wavelength of the reference wave λ_R is considered as first key. We would like to point out here is that the output signal from Fourier lens is considered as another new cipher. Therefore, the focal length f is regarded as a second key.

2.2. The Hybrid Encryption Algorithms

One of the VOHE systems was the symmetric key encryption method. In this method, two users such as a sender and a receiver select a VOHE system's key (λ, f) in advance then they use the VOHE system's key to communicate a system's cipher (IFP) over a public channel. Occasionally, users can able to exchange system's keys periodically. However, the VOHE system may lose system's keys during keys exchange process. To solve this problem and to strengthen the security over VOHE, the

hybrid algorithms of Diffie-Hellman (DH) and RSA are introduced.

Both RSA and the DH algorithms are recently implementing for providing security for data transmission. However, the two technologies have limited related to a key's size. In RSA algorithm, the system's cipher is limited by the length of the key. The length of the VOHE system's cipher is greater than the length of the key. Hence, implementing the RSA algorithm is not suitable for sending the VOHE system's cipher as a message to the receiver. Therefore, when we periodically exchange the keys of the VOHE system, the RSA algorithm is implemented to send keys as a message to the receiver. In DH algorithm, two users set up a private and random key for the VOHE system, separately. The DH algorithm is implemented to send the VOHE system's cipher as a message to the receiver.

2.2.1. RSA algorithm

As wavelength λ and focal length f are involved in the encryption and decryption systems, the wavelength λ and focal length f are required to be transmitted to the receiver using a secure channel, the RSA algorithm is implemented to send system information (λ, f) as a message to the receiver, as shown in Fig. 2.3. Firstly, a sender sends a request to a receiver for sending a receiver's public key. Then, the receiver sends its public key (b, N) to the sender. The sender will encrypt the message (λ, f) using the receiver's public key and send the encrypted message to the receiver. When the receiver receives the cipher, it decrypts using its private key (d, N) to get the message (λ, f).

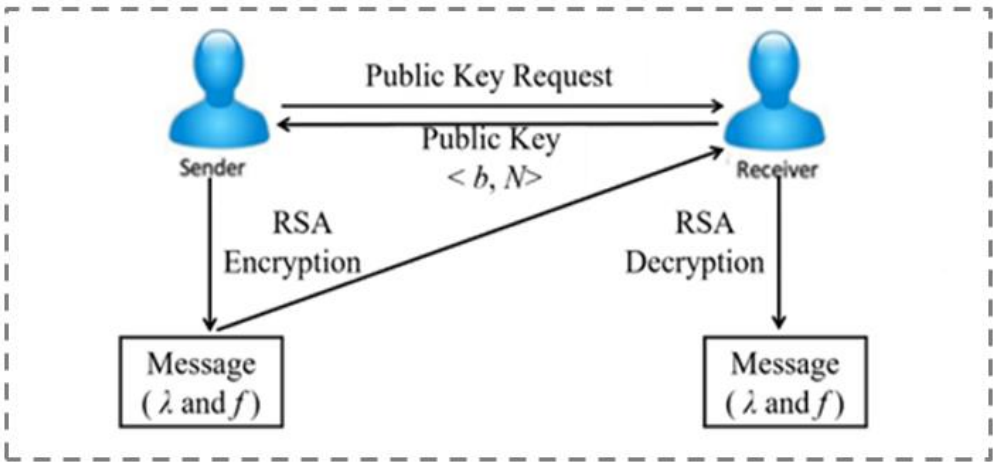

Figure 2.3. A schematic diagram of RSA algorithm

A private key (d, N) and a public key (b, N) are calculated as shown in Algorithm 2.1. The encryption and decryption processes are shown in Algorithm 2.2 and 2.3, respectively. A message m that includes information about λ, f is required to be send to the receiver through secure channel. As shown in Algorithm 2.2 the cipher c is sent to the receiver. At the receiver side, the receiver is using the private key to calculate the message m, as shown in Algorithm 2.3.

Algorithm 2.1 Calculate <Keys>
Input: p, q ∈ C, $1< b <\varphi$
1: $N = p \times q$
2: $\varphi(N) = (p\text{-}1) \times (q\text{-}1)$
3: $d = b^{-1} \bmod \varphi(N)$
4: Output Public Key (b, N)
Private Key(d, N)

Algorithm 2.2 <Encryption process>
Input: m (λ, f)
1: $c = m^b \bmod N$
2: Output: c

Algorithm 2.3 <Decryption process>
Input: c
1: m = c^d mod N
2: Output m (λ, f)

2.2.2. Diffie-Hellman algorithm

The sender's cipher (IFP) requires a secure channel to be transmitted to a receiver. The DH algorithm [125] is implemented to send cipher text (IFP) as a message to the receiver, as shown in Fig. 2.4. The sender and the receiver are communicating using a bitwise XOR operation for DH encryption.

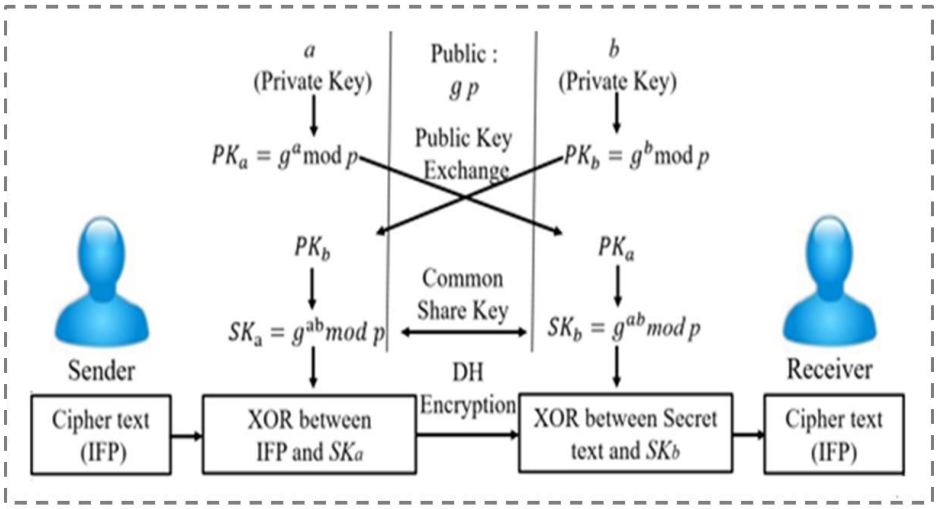

Figure 2.4. A schematic diagram of DH algorithm

In algorithms 2.4 and 2.5, first, two numbers p and g are selected, where p is the prime number and g is the real number. Second, select two random variables, such as a and b, as the private key. The public key (PK_a and PK_b) are then calculated using a modular operation. Finally, another key (SK_a and SK_b) called shared keys is generated by exchanging the public key (PK_a and PK_b) between the sender and the receiver, respectively.

Algorithm 2.4 DH < In sender side >
Input: g, p, a

1: $PK_a = g^a \bmod p$

2: Send PK_a and Wait PK_b

3: Get PK_b

4: $SK_a = (PK_b)^a \bmod p$

5: Output SK_a

Algorithm 2.5 DH < In receiver side >

Input: g, p, b

1: $PK_b = g^b \bmod p$

2: Send PK_b and Wait PK_a

3: Get PK_a

4: $SK_b = (PK_a)^b \bmod p$

5: Output SK_b

2.3. Experiment Results and Analysis

Simulation is conducted using COMSOL Multiphysics tool to simulate the process of the encryption and decryption [126]. As a numerical example, the parameters of the simulation are the object wavelength of λ_o = 632.8 nm, the reference wavelength of λ_R = 632.8 nm, the hologram material index n = 1.3 and a Fourier lens of focal length of f = 4.20 mm. A rectangle size of a hologram domain is selected where the horizontal size is L_x = 80 μm and the vertical size is L_y = 30 μm.

2.3.1. Encryption process

As shown in Fig. 2.5 (a), suppose that a 4-bit block object message which is required to be sent from sender to receiver e.g. “1011”. This object message is carried by object wave U_0. As the object wave pass through the Fourier lens with focal length of f = 4.20 mm, the output from Fourier lens is electric field amplitude U_O that is focused on holographic plane as shown in Fig. 2.5 (b).

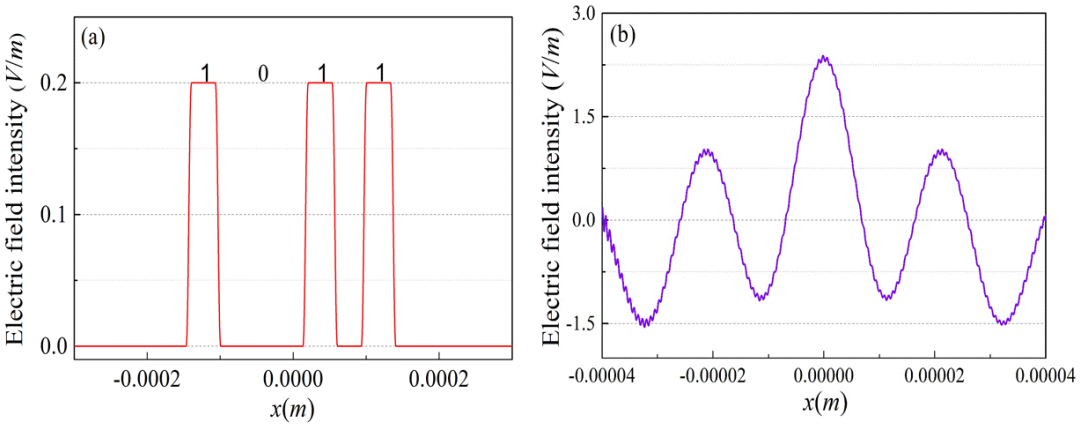

Figure 2.5. (a) The object message E (x) e.g. "1011". (b) The electric field amplitude U_{o}.

The layout of the wave is such that the reference wave U_R comes from the left, while the object wave U_O enters from the top side, as shown in Fig. 2.6. The output signal of the holographic material part is encrypted as holographic signal.

The Fig. 2.6 (a) shows the results of the encryption process. The IFP is produced by interactions between the object wave U_O and reference wave U_R, and as we proposed above that λ_o and λ_R are considered to have same values, hence the IFP will array at a 45 degree angle. The IFP is considered as a cipher pattern that records the encrypted information. The MOD [I (x, y)] is a holographic refractive index modulator function, which modulates holographic material refractive index based on an above certain threshold value of electric field intensity, as shown in Fig. 2.6 (b).

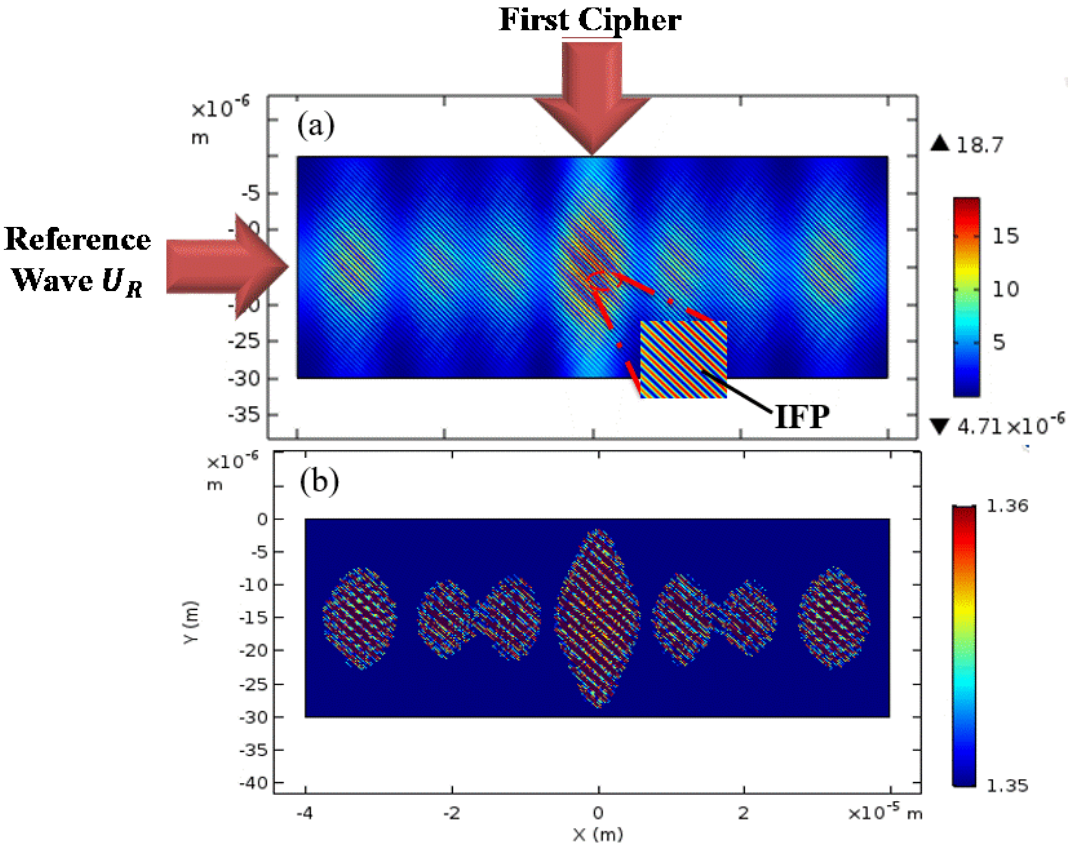

Figure 2.6. (a) The encryption strength and electric field at $\lambda_O = \lambda_R = 632.8$ nm (Inset: the IFP with at a 45-degree angle), (b) the electric field intensity MOD [$I(x, y)$].

2.3.2. Decryption process

The decryption process is shown in the Fig. 2.7. This process is done by turning off the object wave of the receiver and let the correct reference wave passes though the hologram and the output of this process will turn out to be a new object wave which carries information that has been sent by the sender. At the receiver side, the reference wave should be accurate to that of the reference wave of the sender.

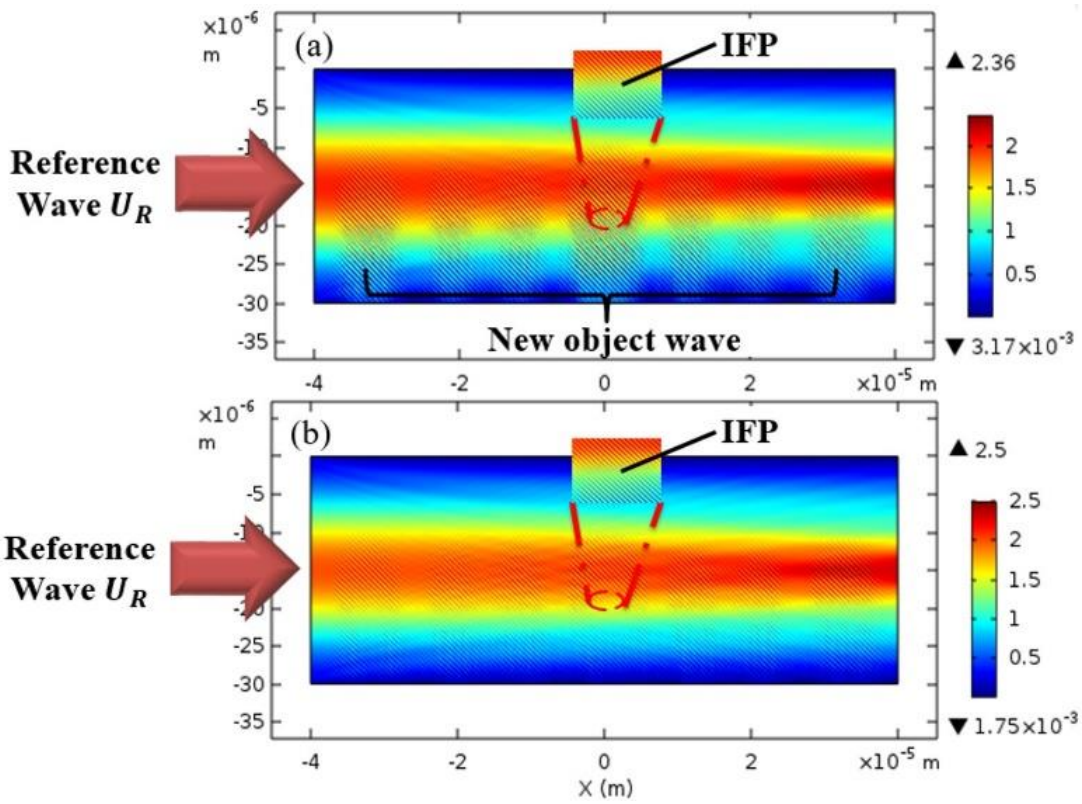

Figure 2.7. The decryption strength and electric field at: (a) $\lambda_R = 632.8$ nm, (b) $\lambda_R = 601.2$ nm.

(Inset: the IFP with at a 45-degree angle)

If the reference wave falls on the hologram that contains the IFP information then a new object wave will be created. Previously, we supposed that a decryption's key is chosen to be $\lambda_R = 632.8$ nm, as shown in Fig. 2.7 (a). The Fig. 2.7 (b) shows that the decryption process will fail a different key is selected, e.g. $\lambda_R = 601.2$ nm.

The simulation is also performed to verify an accurate system key (λ, f) during decryption process. In Fig. 2.8 (a), the original code is compared with the decrypted code of the first decryption key λ_R. We can see that the reference wave $\lambda_R = 632.8$ nm has the highest amplitude. The period of the signal is located within the original bit's period. In Fig. 2.8 (b), the original code is compared with the decrypted code of the second decryption key f. We can see that the focal length $f = 4.20$ mm does not have the highest amplitude. However, the signal is located within the original bit's period.

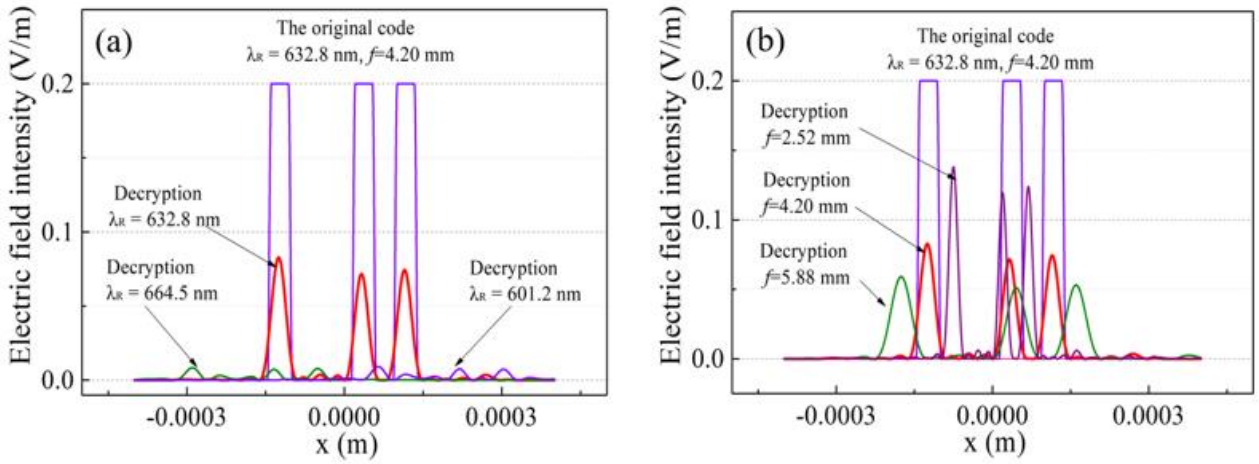

Figure 2.8. A comparison of the decrypted codes (a) with various λ_R, (b) with various *f*.

2.4. Conclusions

The encryption model has been successfully simulated using the COMSOL Multiphysics to simulate holograms and Fourier lens in the VOHE system. The system has two keys for encryption and decryption which are required to be coherent with each other. The wavelength λ was considered as a first VOHE system's key and the focal lengths *f* was considered as a second system's key. Two users such as a sender and a receiver select a VOHE system's key (λ, *f*) in advance then they use the VOHE system's key to communicate a system's cipher (IFP) over a public channel.

Both RSA and the DH algorithms are recently implementing for providing security for data transmission. The RSA algorithm is implemented for sending system information (λ, *f*) as a message to the receiver. The IFP that is generated at the sender side is required to be secured during a transmission process to the receiver over unsecure channel. The sender and the receiver are exchanging information (IFP) using the DH algorithm to construct a shared key. The XOR operations are performed between cipher text and the share key in the encryption / decryption processes.

Chapter 3

THE VIRTUAL OPTICAL HOLOGRAPHIC ENCRYPTION SYSTEM USING ERSA ALGORITHM

This Chapter is employing a VOHE system to encrypt information based on an extension of RSA (ERSA) algorithm using complex functions. The VOHE system provides essential parameters for constructing secure data transmissions such as the propagation wavelength (λ) and focal length (*f*) of the Fourier lens, which are considered as keys for implementing encryption and decryption processes. The expanded RSA (ERSA) algorithm which is based on a complex function is implanted to send system information (λ, *f*) as a message to a receiver.

Rivest, Shamir, and Adleman introduced the RSA public key encryption system in 1978 [83]. In addition to the standard RSA scheme, researchers have also devoted their studies to designing a system based on an RSA-based method with further efficiency and security considerations, such as the CRT-RSA scheme [127], the Prime Power RSA scheme [128], and the Kuwakado - Koyama - Tsuruoka RSA type scheme of singular cubic curve [129]. In 2002, Elkamchouchi *et al*. extended the RSA using Gaussian integers [130], which was similar to the method of Kuwakado, Koyama and Tsuruoka. Castagnos [131] proposed a probabilistic scheme based on RSA modulus in 2007, which also included the same modulus equations as the above two schemes [129, 130].

This Chapter 3 is organized as follows: in Section 3.1, the ERSA algorithm are briefly introduced. The complexity of the method based on Pollard's rho method is also given in Section 3.2. Section 3.3 contains examples of how to implement RSA and ERSA algorithms. Finally, the conclusions of the

study are summarized in Section 3.4.

3.1. The Expanded RSA (ERSA) algorithm

To achieve a resilient security of data transmission as both a sender and a receiver, this study implemented an expanded encryption process using complex function and based on the expansion of the RSA algorithm.

As wavelength λ and focal length f are concerned in the encryption and decryption systems, the wavelength λ and focal length f is required to be transmitted to the receiver using a secure channel. The ERSA algorithm is implemented to send system information (λ, f) as a message to the receiver, as shown in Fig. 3.1. The operation is as follows, firstly, a sender sends a request to a receiver for the receiver's public key (b, N). Then, the receiver sends its public key to the sender. The sender will encrypt the message (λ, f) using the receiver's public key and send the encrypted message to the receiver. When the receiver receives a cipher, it decrypts it using its private key (d, N) to get the message (λ, f).

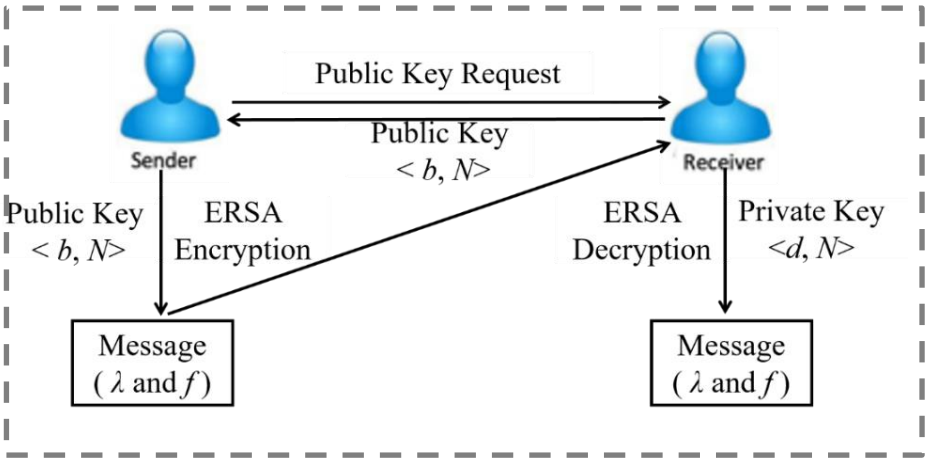

Figure 3.1. A schematic diagram of ERSA

The public and private keys' generation of the ERSA algorithm is done using the following steps:

1. Choose two random values for p and q where both are complex numbers [132, 133]: $p = x_p + iy_p$, $q = x_q + iy_q$

2. Multiply the p and q values to produce $N = p \times q$, where N is also a complex number. In the ERSA algorithm, the extended Euler function is $\Phi(N) = (|p|^2 - 1) \times (|q|^2 - 1)$ and, for the conventional RSA algorithm, the Euler function is $\Phi(N) = (p - 1) \times (q - 1)$. Hence, compared to the RSA Euler-phi function, the ERSA provides more security for extending Euler-phi functions than that of the conventional RSA. In contrast to the RSA algorithm, the ERSA includes complex numbers by which security can be strengthened.
3. A private key (d, N) and a public key (b, N) are calculated as shown in Algorithm 3.1. The encryption and decryption processes are shown in Algorithms 3.2 and 3.3, respectively. The message m that includes information about λ, f must be sent to the receiver through a secure channel. As shown in Algorithm 3.2, the cipher c, which is formed in a complex function, is sent to the receiver. At the receiver side, the receiver is using its private key to calculate the message m_1, which is also a complex number, as shown in Algorithm 3.3. Finally, the process to convert m_1 from a complex number to a real number m that contains information about λ, f is given in Algorithm 3.4.

Algorithm 3.1 Calculate <Keys>
Input: $p, q \in C, 1 < b < \varphi$
1: $N = (x_p + iy_p) \times (x_q + iy_q)$
2: $\Phi(N) = (\|p\|^2 - 1) \times (\|q\|^2 - 1)$
3: $d = b^{-1} \bmod \Phi(N)$
4: Output Public Key (b, N) Private Key (d, N)

Algorithm 3.2 <Encryption process>
Input: m (λ,f)
1: $c = m^b \bmod N$
2: Output: c ($x_c + y_c i$)

Algorithm 3.3 <Decryption process>
Input: c ($x_c + y_c i$)

1: $m_1 = c^d \bmod N$

2: m = C2R (m_1, N)

3: Output m (λ, f)

Algorithm 3.4 <C2R (m_1, N)>

Input: $m_1 = x_v + iy_v$, $N = x_N + iy_N$

1: $X' = x_v x_N + y_v y_N$

2: $Y' = y_v x_N - x_v y_N$

3: $|N|^2 = (x_N)^2 + (y_N)^2$

4: if $x_N > 0$: $X'' = X' \bmod |N|^2$

5: else: $X'' = X' \bmod (-|N|^2)$

6: if $y_N < 0$: $Y'' = Y' \bmod |N|^2$

7: else: $Y'' = Y' \bmod (-|N|^2)$

8: m = $(X'' + iY'')/(x_N - iy_N)$

9: Output m

3.2. The Expanded Pollard's rho method

To evaluate the security of the ERSA algorithm, an expanded Pollard's Rho method to calculate the complexity of finding the private key d for RSA and ERSA, respectively, and maintaining key-size c [86, 87]. Table 3.1 shows the c and its size for RSA and ERSA.

Table 3.1. Details of N, c and the key size of RSA and ERSA.

Algorithm	Modulus N	c	The size of key
RSA	$x_p \times iy_p$	x	Length (x)
ERSA	$(x_p + iy_p) \times (x_q + iy_q)$	$x + iy$	Length (x) + Length (y)

In the algorithm 3.5 shows how to calculate private key b, processing time t and out loop i of c with various key-size [134, 135]. To verify the security of the c, c is analyzed using Pollard's rho method. This method calculates average output loops $\bar{i}$ using the same key length for both RSA and ERSA, if the $\bar{i}$ value is high then c has better security. In addition, algorithm 3.5 can also evaluate the efficiency

of both RSA and ERSA that is based on average processing time parameter *t*.

Algorithm 3.5 Pollard's rho method
Input: m, *c*, *N*
s.t m = c^d mod *N*
Start = time. Clock
1: $i := 0$
2: Repeat
3: *i* ++
4: Choose $a_i, \beta_i \in [0, \|N\|^2 - 2]$ randomly
5: $m_i = (c)^{a_i} g^{\beta_i} mod(\|N\|^2 - 1)$
6: until $\exists_j$ s. t. $1 \leq j \leq i, m_j = m_i$
7: $d = (\beta_j - \beta_i)(\alpha_i - \alpha_j)^{-1}$ mod $(\|N\|^2 - 1)$
8: *t* = time. Clock - Start
9: Output *d, i, and t.*

It is possible to calculate small size of private key *d* from m =c^d mod *N* using a personal computer, but it is very difficult to calculate private key for long *c* key-size and the calculation required a super computer. As an example, Fig. 3.2 (a) shows the Pollard's rho method is used to compute $\bar{i}$ of *c* for 8 bits, 12 bits, 16 bits and 32 bits, respectively. Fig. 3.2 (b) shows the average processing time *t* for calculating private key b of *c* for 8 bits, 12 bits, 16 bits and 32 bits, respectively.

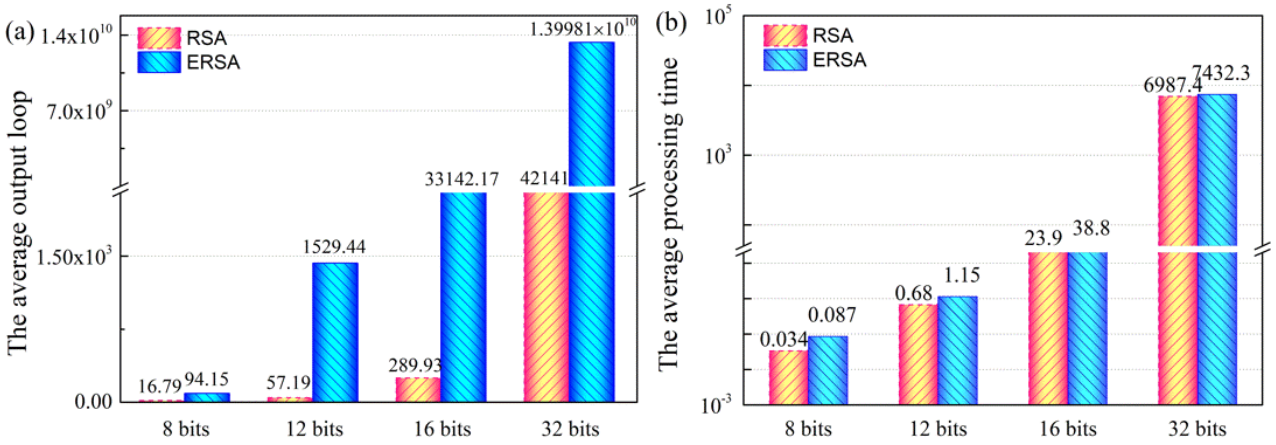

Figure 3.2. (a) The average output loop *i*. (b) The average processing time *t* (sec)

The obtained results exhibit the average output loop *i* and processing time *t* that are calculated by pollard Rho method. In Fig. 3.2 (a), the results show that ERSA is more secure than RSA when the key-size is higher than 12-bit that makes EDH-C more appropriate method for strengthen the security. The results in Fig. 3.2 (b) show the processing time for both RSA and ERSA, and because of the trade-off between efficiency and security, we need to make a balance between them. As the results show that ERSA method takes a slightly longer processing time to break down the *c* code than the RSA algorithm. Therefore, in this study, using the ERSA algorithm to encrypt system information (λ, *f*) is a more appropriate method for strengthening the security of the data transmissions.

3.3. The ERSA algorithm process

To understaned the processes of these two methods, the following are examples of how to implement RSA and ERSA algorithms. We consider *N* has same key-size for both algorithms.

1) RSA ALGORITHM

The RSA algorithm was implemented to send system information (λ, *f*) (for e.g., λ = 632.8 nm, *f* = 4.20 mm) to the receiver by implementing Algorithms 2.1 to 2.4, as mentioned in subsection 2.2.1 (in Chapter 2). Algorithm 2.1 was used to calculate the private and public keys. Algorithm 2.2 was implemented to encrypt the system information to be ready to send it to the receiver over the insecure

channel. Algorithm 2.3 was performed as the decryption process.

To comprehend the system's processes, the following are a numerical example of how to build a secure system.

(1) For the algorithm 2.1 , the keys are generated using the following steps:

Step 1 Choose two prime number such as p and q

$$p = 49277 \tag{3.1}$$

$$q = 47211 \tag{3.2}$$

Step 2 Determine the modulus N as

$$N = (p \times q) = 2326416447 \tag{3.3}$$

Step 3 Compute $\Phi(N)$

$$\Phi(N) = \Phi(p) \times \Phi(q) = 2326319960 \tag{3.4}$$

Step 4 Calculate d to satisfy the congruence relation $b \times d = 1 \pmod{\Phi(N)}$. Select an integer b such that $1 < b < \Phi(N)$, where b is a coprime to $\Phi(N)$. Selecting the value of b directly links 9883 so the calculation of d is 19066267.

The public key is (b, N) and the pair (9883, 2326416447) is considered as a public key. The private key is (d, N) and the pair (19066267, 2326416447) is regarded as a private key.

(2) For the algorithm 2.2, the system information is encrypted using the following step:

Step 1: At the sender end, the system information is encrypted using the formula 3.5

$$c = \mathrm{m}^{\,b} \bmod N \tag{3.5}$$

Where, m is a message that contains information about two secure parameters which are reference wave λ and focal length f. In above example, we assumed that λ = 632.8 nm and f = 4.20 mm.

Step 2: The message m = [632.8 nm, 4.20 mm] is converted to ASCII and will be

[54 51 50 46 56 110 109 44 52 46 50 48 109 109].

Step 3: In Eq. 3.5, the message m is encrypted using the public key (b, N) which is (9883, 2326416447). The encrypted message c which is cipher text is ready to be sent to the receiver.

c = [2077599405, 1450081011, 1186076528, 1587247192, 1813311281, 12423545, 1456844341, 747647951, 1414325377, 1587247192, 1186076528, 1796995776, 1456844341, 1456844341].

(3) For the algorithm 2.3, the system information is decrypted using the following step:

Step 1: At the receiver's end, the c is decrypted using the formula 3.6:

$$\mathrm{m} = c^{d} \bmod N \tag{3.6}$$

Where, d=19066267, N= 2326416447

$$\mathrm{m} = [632.8\ \mathrm{nm}, 4.20\ \mathrm{mm}] \tag{3.7}$$

2) ERSA ALGORITHM

The ERSA algorithm is implemented to send system information (λ, f) (for e.g., λ = 632.8 nm, f = 4.20 mm) to the receiver by implementing Algorithms 3.1 to 3.4, as mentioned in Section 3.2. Algorithm 3.1 is used to calculate the private and public keys. Algorithm 3.2 was implemented to encrypt the system information to be ready to send it to the receiver over insecure channel. Algorithm 3.3 is performed a decryption process. Algorithm 3.4 is used to convert the complex number to a real number.

To comprehend the system's processes, the following steps are a numerical example of how to build a secure system:

(1) For Algorithm 3.1, the keys are generated using the following steps:

Step 1 Choose two complex functions, such as p and q, where their square parameters are prime numbers:

$$p = 155 + 168i \tag{3.8}$$

$$q = 187 + 122i \tag{3.9}$$

Step 2 Determine the modulus N as

$$N = (p \times q) = 8489+50326i \tag{3.10}$$

Step 3 Compute $\Phi(N)$

$$\Phi(N) = \Phi(p) \times \Phi(q) = 2604667296 \tag{3.11}$$

Step 4 Calculate d to satisfy the congruence relation $b \times d = 1 \pmod{\Phi(N)}$. Select an integer b such that $1 < b < \Phi(N)$, where b is a coprime to $\Phi(N)$. If we select b value as 9883 then d will be 1170426739.

The public key is (b, N) and the pair $(9883, 8489 + 50326i)$ is considered as a public key. The private key is (d, N) and the pair $(1170426739, 8489 + 50326i)$ is regarded as a private key.

(2) For Algorithm 3.2, the system information is encrypted using the following step:

Step 1: At the sender end, the system information is encrypted using the formula (3.12)

$$c = \mathrm{m}^{\,b} \bmod N \tag{3.12}$$

Where, m is a message that contains information about two secure parameters which are reference wave λ and focal length f. In the above example, we assumed that λ = 632.8 nm and f = 4.20 mm.

Step 2: The message m = [632.8 nm, 4.20 mm] is converted to ASCII and will be

[54 51 50 46 56 110 109 44 52 46 50 48 109 109]

Step 3: In Equation (3.12), the message m is encrypted using the public key (b, N) which is (9883, 8489+50326i). The encrypted message c is a cipher text which is ready to be sent to the receiver.

c = [−2810 + 23293i, −26212 + 15233i, −29011 + 55884i, −25754 + 5107i, −23922 + 17208i, −35858 + 43449i, −34376 + 32569i, −17690 + 50076i, −12936 + 43603i, −25754 + 5107i, −29011 + 55884i, −36250 + 20784i, −34376 + 32569i, −34376 + 32569i]

(3) For Algorithm 3.3, the system information is decrypted using the following step:

Step 1: At the receiver's end, c is decrypted using the formula (3.13):

$$m_1 = c^{\,d} \bmod N \tag{3.13}$$

Where, d = 1170426739, N = 8489 + 50326i

m_1 = [−50272 + 8489i, −50275 + 8489i, −50276 + 8489i, −50280 + 8489i, −50270 + 8489i,

−50216 + 8489i, −50217 + 8489i, −50282 + 8489i, −50274 + 8489i, −50280 + 8489i,

−50276+ 8489i, −50278 + 8489i, −50217 + 8489i, −50217 + 8489i]

Step 2: the C2R (m_1, N) function (that converts complex numbers into real numbers) is used to convert the m_1 in complex number to ASCII code.

ASCII: [54 51 50 46 56 110 109 44 52 46 50 48 109 109]

The ASCII code is converted to a real message and will be

$$m = [632.8 \text{ nm}, 4.20 \text{ mm}] \tag{3.14}$$

(4) For Algorithm 3.4, C2R (m_1, N) is used to convert a complex value to text, and the following is a short example of how to convert one parameter of message m to an integer number.

m_1 = −50272 + 8489i, N = 8489 + 50326i

Step 1 $X' = x_v x_N + y_v y_N$ = 458406

Step 2 $Y' = y_v x_N - x_v y_N$ = 2602051793

Step 3 $|N|^2 = (8489)^2 + (50326)^2$ = 2604769397

Step 4 $N_x > 0$: 458406 mod (2604769397) = 458406

Step 5 $N_y > 0$: 2602051793 mod (−2604769397) = −2717604

Step 6 (458406 − 2717604i) / (8489-50326i) = 54 + 0i

Step 7 Output 54

3.4. Conclusions

The expanded RSA (ERSA) algorithm was been applied a complex function for sending system information (λ, f) (for e.g., λ = 632.8 nm, f = 4.20 mm) as a message to a receiver. The evaluation results, which were based on Pollard's rho method, indicate that we can obtain better security performance using the ERSA algorithm. Therefore, using ERSA algorithm to encrypt system information (λ, f) is a more appropriate method for strengthening the security of the data transmissions.

The evaluation results which were based on the Pollard's Rho method indicate that ERSA method has a better performance in view of security and efficiency as well.

Chapter 4

THE VIRTUAL OPTICAL HOLOGRAPHIC ENCRYPTION SYSTEM USING EDH-C ALGORITHM

This Chapter introduces a new approach for data encryption over a VOHE system using an expanded Diffie-Hellman algorithm. The expanding a Diffie-Hellman algorithm is performed by applying a two-dimensional complex function (EDH-C). The main reason of using a complex function is to strengthen security over conventional Diffie-Hellman algorithm. The Diffie-Hellman (DH) key exchange is one of the earliest algorithms for a key exchange, which enables both parties to securely exchange keys over an unsecured channel. Whitfield Diffie and Martin Hellman proposed the algorithm in 1976 and have since been applied to the security domain [136]. 2017, Hecht and Kamlofsky submitted some hyper complex numbers based on the Diffie-Hellman key agreement protocol HK17 [137]. Since then, numerous related studies have emerged for strengthening the security and improving the efficiency of the data processing.

The virtual optical encryption digital holographic system has been widely used in recent years, because of its advantage over other cryptographic systems, such as high-speed, multi-dimensional, high-capacity. In this study, a new scheme of optical encryption system using expanded Diffie-Hellman (EDH) algorithm which is done by applying a complex function.

This Chapter is organized as follows: In Section 4.1, the EDH-C encryption algorithm is briefly introduced. The security of the proposed EDH-C algorithm is evaluated using an extended Pollard's Rho method, which is given in Section 4.2. In Section 4.3, examples are presented of how the DH and

EDH-C encryption algorithms performs for generating a share key between a sender and a receiver. Finally, conclusions of this study are summarized in Section 4.4.

4.1. The Expanded Diffie-Hellman (EDH) Algorithm

The Interference Fringe Pattern (IFP) that is generated at the sender side is required to be securely transmitted to the receiver over unsecure channel, as shown in Fig. 4.1. The sender and the receiver are exchanging information using the EDH-C algorithm to construct a shared key. The XOR operations are performed between cipher text and the share key in the encryption / decryption processes [138]. Specifically, the XOR operations should be used with a one-time shared key *SK* to ensure the security of the transmitted data [139]. Therefore, we can select a different parameters each time and make the shared key *SK* different every time.

At the sender's end, when the encryption process is completed then a bitwise XOR operation is performed between a cipher text of the IFP and the SK_a. Using these two parameters, the secret text (ST) is calculated as follows

$$\mathrm{ST} = \mathrm{IFP} \oplus SK_{\mathrm{a}} \tag{4.1}$$

The transmission's media is implemented as means to carry IFP object's ST to the receiver.

At the receiver's end, the bitwise XOR operation is also performed between SK_b and ST result which has received from the sender. The IFP is calculated as follows

$$\mathrm{IFP} = \mathrm{ST} \oplus SK_{\mathrm{b}} \tag{4.2}$$

To summarize the proposed EDH-C algorithm, the following algorithms demonstrate of how to construct public keys.

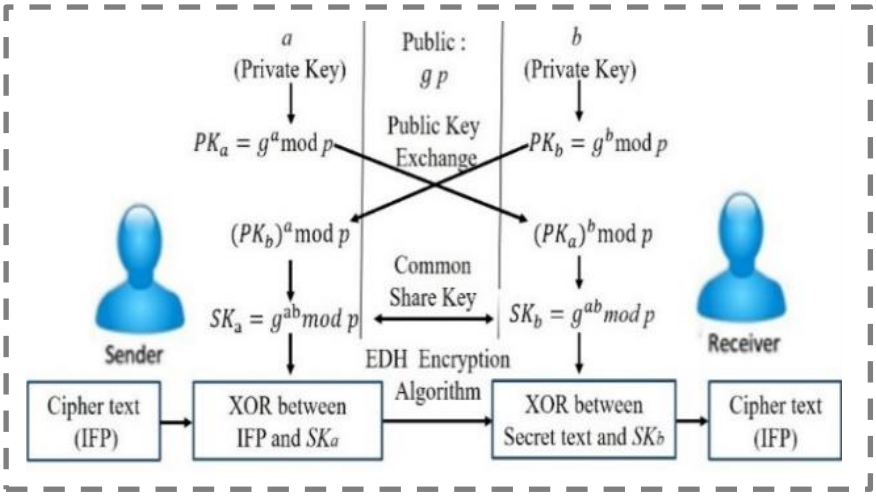

Figure 4.1. Schematic diagram of EDH-C exchange algorithm

In the algorithms 4.1 and 4.2, firstly, two numbers p and g are selected, where p is complex number [132] and its square absolute value $|p|^2$ is prime number and g is real number called a base. Secondly, two random variables (such as a and b) are selected as private keys. Then, the public keys (PK_a and PK_b) are calculated using module operations of complex numbers. Finally, by exchanging the public keys (PK_a and PK_b) between a sender and a receiver, respectively, another keys (SK_a and SK_b) which are called share keys will be generated.

Algorithm 4.1 EDH < sender>
Input: g, p, a
1: $PK_a = g^a \bmod p$
2: Send PK_a and Wait PK_b
3: Get PK_b
4: $SK_a = (PK_b)^a \bmod p$
5: Output SK_a

Algorithm 4.2 EDH <receiver>
Input: g, p, b
1: $PK_b = g^b \bmod p$
2: Send PK_b and Wait PK_a

3: Get PK_a

4: $SK_b = (PK_a)^b \bmod p$

5: Output SK_b

In EDH-C algorithm, p is held to be a complex function as $p = x_p + iy_p$. As a result, both sender and receiver calculate the share key.

$$SK_a = SK_b = g^{ab} \bmod (x_p + iy_p) \tag{4.3}$$

In traditional DH algorithm, p is a prime number when $y_p = 0$ then $p = x_p$. As a result, both the sender and the receiver calculate the shared key.

$$SK_a = SK_b = g^{ab} \bmod (x_p) \tag{4.4}$$

4.2. The Expanded Pollard's rho Method

To comprehend the process of the security of the EDH-C algorithm, an expanded Pollard's Rho method to calculate the complexity of finding the private key a or b for DH and EDH-C, respectively, and maintaining *PK*'s key-size same [86, 87]. Table 4.1 shows the *PK* and its size for DH and EDH-C.

Table 4.1. Details of *PK*, *p*, and the key size of DH and EDH-C

	PK	*p*	*PK* bit-size
DH	x	x_p	Length (x)
EDH-C	$x + iy$	$x_p + iy_p$	Length (x)+ Length (y)

In the algorithm 4.3 shows how to calculate private key a, out loop i and processing time t of PK_a with various key-size [134, 135]. Algorithm 4.3 shows the security evaluation of both DH and EDH-C based on Pollard's Rho method which calculates average output loop's parameter i. In addition, algorithm 4.3 can also evaluate the efficiency of both DH and EDH-C which is based on average processing time parameter t. (To comprehend the process of the Pollard's Rho method to calculate the complexity of finding the private key a for DH and EDH-C are displayed in Appendix 3 and Appendix

4, respectively.)

Algorithm 4.3 Pollard's rho method
Input: p :($\|p\|^2$ is prime number), PK_a , $g \in [0, \|p\|^2 - 1]$
s.t. $PK_a = g^a \bmod p$.
Start = time. Clock
1: $i := 0$
2: Repeat
3: i ++
4: Choose $a_i, \beta_i \in [0, \|p\|^2 - 2]$ randomly
5: $c_i = (PK)^{a_i} g^{\beta_i} mod(\|p\|^2 - 1)$
6: until $\exists_j$ s.t. $1 \leq j \leq i, c_j = c_i$
7:$a = (\beta_j - \beta_i)(\alpha_i - \alpha_j)^{-1} mod\ (\|p\|^2 - 1)$
8: t = time. Clock - Start
9: Output a, i and t.

It is possible to calculate a small size private key a from *PK* using a personal computer, but it is very difficult to calculate private key for long *PK* key-size and the calculation required a super computer. As an example, Fig. 4.2 (a) shows the average output loop *i* for calculating private key *a* using DH and EDH-C with different PK_a key-size of 8 bits, 16 bits, 24 bits and 32 bits, respectively. Fig. 4.2 (b) shows the average processing time *t* for calculating the private key *a* using DH and EDH-C with different PK_a key-size of 8 bits, 16 bits, 24 bits and 32 bits, respectively.

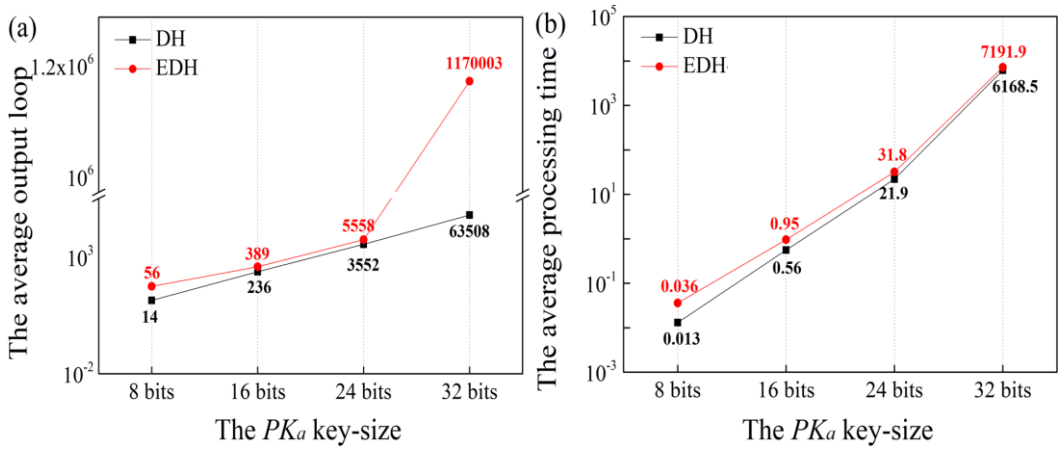

Figure 4.2. (a) The average output loop *i* of Pollard's rho method. (b) The average processing time *t* (sec) of Pollard's rho method.

The obtained results exhibit the average output loop *i* and processing time *t* that are calculated by pollard Rho method. In Fig. 4.2 (a), the results show that EDH-C is more secure than DH when the key-size is higher than 24-bit that makes EDH-C more appropriate method for strengthen the security. The results in Fig. 4.2 (b) show the processing time for both DH and EDH-C, and because of the trade-off between efficiency and security, we need to make a balance between them. The results show that EDH-C method takes a slightly longer processing time to break down the PK_a code than the DH algorithm.

4.3. The EDH algorithm process

To comprehend the process of these two methods, the following are examples of how to implement DH and EDH-C algorithms. We consider *p* has same key-size for both algorithms.

1) DH ALGORITHM

In previous section, the DH algorithm has been used to generate a share key at both a sender and a receiver. The share keys SK_a and SK_b are calculated by Algorithm 2.1 and 2.2 for DH algorithm, as mentioned in subsection 2.2.2 (in Chapter 2).

For the DH, the share keys SK_a and SK_b are calculated using the following example:

Select $g = 5$ and $p = 12979877$

Sender's private key $a = 373$

Receiver's private key $b = 433$

Step 1 sender calculates own public key

$$PK_a = g^{\,a} \bmod p = 3977122 \tag{4.5}$$

As a result, PK_a is sent to receiver.

Step 2 receiver calculates the public key

$$PK_b = g^{\,b} \bmod p = 10691878 \tag{4.6}$$

As a result, PK_b is sent to sender.

Step 3 sender computes the shared key SK_a from the received public key PK_b.

$$SK_a = g^{\,ab} \bmod p = 7522523 \tag{4.7}$$

Step 4 receiver computes the shared key SK_b from the received public key PK_a.

$$SK_b = g^{\,ab} \bmod p = 7522523 \tag{4.8}$$

2) EDH-C ALGORITHM

The EDH-C algorithm is used to generate a share key at both a sender and a receiver that were mentioned in subsection 4.2. The share keys SK_a and SK_b are calculated by Algorithm 4.1 and 4.2 for EDH-C, as mentioned in subsection 4.1.

For the EDH-C, the share keys SK_a and SK_b are calculated using the following example:

Select $g = 5$ and $p = 2561 + 2534i$

Sender's private key $a = 373$

Receiver's private key $b = 433$

Step 1 sender calculates own public key

$$PK_a = g^{a} \bmod p = 380+3241i \tag{4.9}$$

As a result, PK_a is sent to receiver.

Step 2 receiver calculates the public key

$$PK_b = g^{b} \bmod p = -263+3162i \tag{4.10}$$

As a result, PK_b is sent to sender.

Step 3 sender computes the shared key SK_a from the received public key PK_b.

$$SK_a = g^{ab} \bmod p = -447+1653i \tag{4.11}$$

Step 4 receiver computes the shared key SK_b from the received public key PK_a.

$$SK_b = g^{ab} \bmod p = -447+1653i \tag{4.12}$$

4.4. Conclusions

In this chapter, we have introduced a new method for encrypting holographic information using EDH encryption algorithm based on two-dimension complex function. The EDH-C encryption algorithm generated the share key for the sender and receiver for communication. The XOR operations are performed between cipher text and the share key in the encryption / decryption processes.

The evaluation results which were based on the Pollard's Rho method indicate that EDH-C method has a better performance in view of security and efficiency as well. Therefore, in this study, using the EDH-C algorithm to encrypt system information (IFP) is a more appropriate method for strengthening the security of the data transmissions.

Chapter 5

EVALUATION OF THE SYSTEM

This chapter carries out security evaluation of EDH algorithm and ERSA algorithm, separately, and compared them with conventional algorithms without extensions. Firstly, bits error check is required to make sure that the data stream is received by the receiver without error during data transmissions. The bits error check is done by calculating the mean square error of a decrypted code. Secondly, the randomness evaluation of the encrypted cipher is required, and the cipher should be highly random. The randomness evaluation is done using NIST Tests.

5.1. Bits Error Check for EDH and DH Algorithms

Through encryption and decryption processes of EDH algorithm, the mean square error (MSE) of a decrypted code's period with respect to the original code's period is calculated, [140, 141], and it's given by:

$$\text{MSE} = \frac{1}{\text{M}}\sum_{x=1}^{\text{M}}|x_m - \hat{x}_m|^2 \tag{5.1}$$

where, M is total number of samples in the code, x_m is the value of the original encrypted code on and $\hat{x}_m$ is retrieval decrypted code.

To ensure the accuracy of the information retrieved at a receiver, results of the MSE are attained for both EDH and conventional DH algorithms. The results of MSE values are obtained for both EDH and DH with various reference wave $\lambda_R$and focal length *f*, as shown in Fig.5.1. The EDH exhibits less minimum MSE in comparison with DH. When the reference wave λ_R is set at 632.8 nm, the minimum MSE value is 1.2×10^{-11} for EDH and 6.2×10^{-10} for DH, as shown in Fig.5.1, (a) and (b), respectively.

Similarly, the minimum MSE values are obtained for EDH and DH with various focal length *f*, and the results show that the EDH algorithm demonstrates better outcomes than DH, as shown in Fig.5.1, (c) and (d).

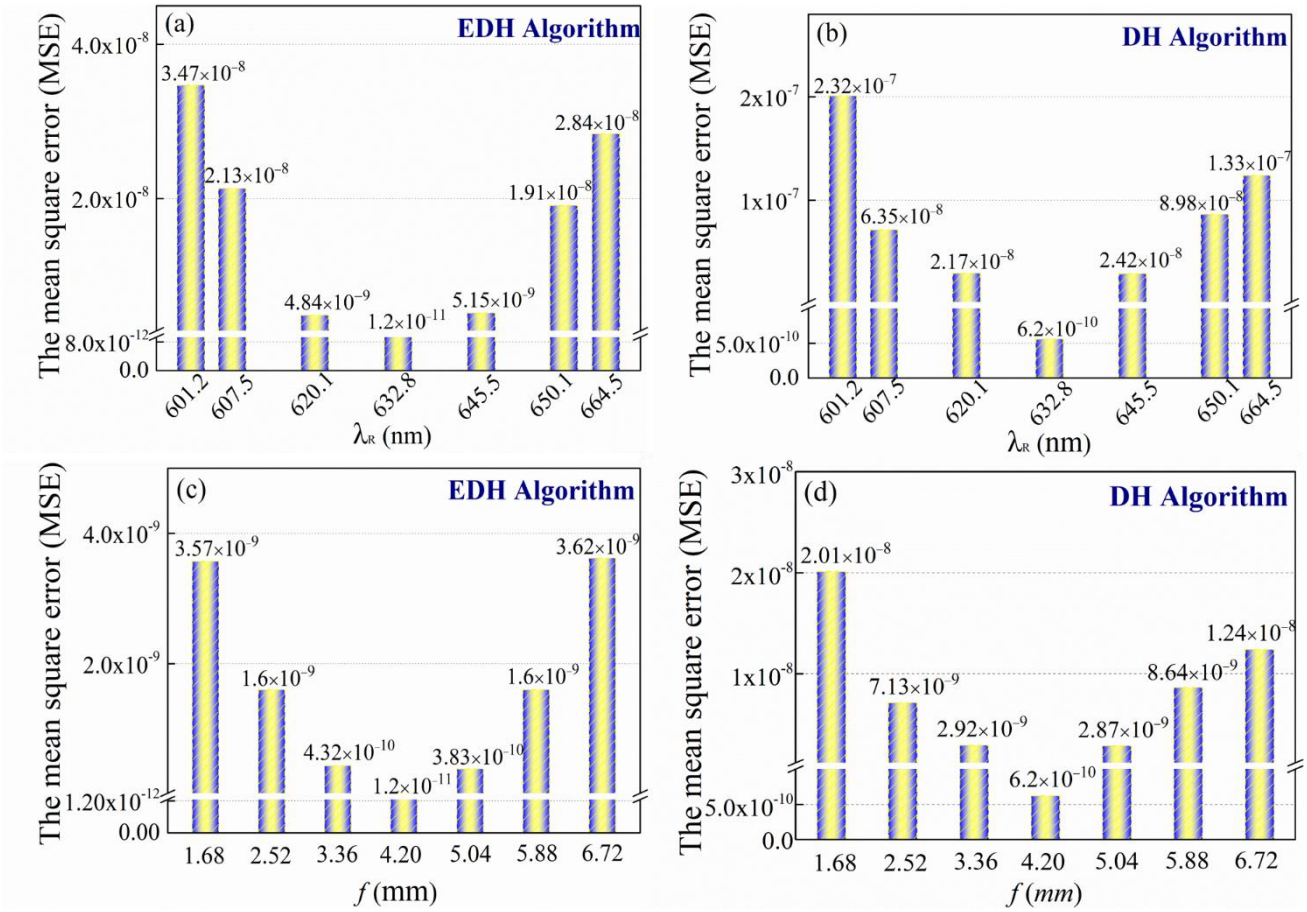

Figure 5.1. The minimum MSE data with various reference waves $\boldsymbol{\lambda_R}$ for (a) EDH and (b) DH, and the minimum MSE data with various focal length *f* for (c) EDH and (d) DH.

5.2. Evaluation and Analysis

5.2.1 The Randomness of ERSA Algorithm

This subsection evaluates the security of the ERSA algorithm based on a statistical test suite for random and pseudorandom number generators for cryptographic applications NIST test [142]. Constructing robust and unpredictable random numbers are of paramount importance in most cryptographic applications. The encrypted message *c* of the ERSA algorithm (in Chapter 3.3) is

required to be random enough against security attacks.

To verify the security of the encrypted message c, c is analyzed using the NIST method. This method calculates a P-value using the same key length for both RSA and ERSA. If the P-value has the highest value then the c value is considered having better randomness. The P-value is frequently called a "tail probability". If the P-value is < 0.01, then it is concluded that the c value has vulnerable randomness, otherwise the c value is considered as random.

Table 5.1 shows a comparison between RSA and ERSA encryptions using the NIST tests. To comprehend this process, a numerical example is presented to evaluate both systems. We consider that $N = p \times q$ has the same key-size for both algorithms. In the ERSA algorithm, two complex functions, such as $p = 155 + 168i$, $q = 187 + 122i$, are selected (in Chapter 3.3), and two prime numbers, such as $p = 49277$ and $q = 47221$, are selected for the RSA algorithm.

Table 5.1. NIST Test's results of RSA algorithm and ERSA algorithm

	Test Items	**RSA**	**ERSA**
		***P*-Value**	***P*-Value**
1	Frequency	0.423711	0.548506
2	Block frequency	0.423711	0.548506
3	Cumulative sums	0.322973	0.958638
4	Runs	0.203323	0.661694
5	Longest run	0.732505	0.810056
6	Rank	0.000000	0.000000
7	Approximate entropy	0.322153	0.758892
8	Serial	0.498531	0.999877
9	Linear complexity	0.000000	0.000000
10	FFT	0.168669	0.646355

Table 5.1 shows the NIST test results of the P-value generated by the ERSA and RSA algorithms,

separately. As shown in the results, all tested items pass all tests except the linear complexity and rank tests. Additionally, eight items of the test's results exhibit that the ERSA algorithm has higher-consistency results than RSA.

5.2.2 The Randomness of EDH Algorithm

This subsection evaluates the security of EDH-C algorithm using random evaluation test. As mentioned in Chapter 4.3, the secret text (ST) of the EDH-C algorithm must be generated in highly level of randomness.

To evaluate the randomness of the ST, the ST is analyzed using the National Institute of Standards and Technology (NIST) test suite method [142]. This method calculates *P*-value using same key length for both DH and EDH-C, if the *P*-value is high then the ST message is considered having better randomness. The *P*-value is often referred to as "tail probability" and if *P*-value is > 0.01 then the ST value has significant randomness, otherwise the ST value is weak randomness.

As show in Table 5.2, the results of *P*-value are obtained using NIST test suite and the table shows a comparison between DH and EDH-C. To evaluate the randomness of these two methods a numerical example is given with the same key-size [143]. In DH algorithm, primer number such as $p = 12979877$ is selected, and complex functions such as $p = 2561+2534i$ is selected for EDH-C algorithm (in Chapter 4.3).

Table 5.2. NIST Test's results of DH algorithm and EDH-C algorithm

	Test Items	**DH**	**EDH-C**
		***P*-Value**	***P*-Value**
1	Frequency	0.689157	0.841481
2	Block Frequency	0.689157	0.841481
3	Cumulative Sums	0.658638	0.929223

4	Runs	0.156112	0.551016
5	Longest Run	0.053571	0.928763
6	Rank	0.000000	0.000000
7	Approximate Entropy	0.438767	0.713633
8	Serial	0.016470	0.498961
9	Linear Complexity	0.221647	0.369399
10	FFT	0.013190	0.646355

In Table 5.2, the results show that the NIST test results of the randomness of the DH and EDH-C *P*-value are passed all tests except the Rank test. Also the results show that the randomness of EDH-C *P*-value is better than the *P*-value of the DH algorithm.

5.3. Conclusions

Minimum mean square error (MMSE) was used to evaluate the accuracy of the received signal. The security evaluation of the ERSA public key algorithm was also conducted using the NIST method for examining the randomness of the transmitted data.

Subsequently, NIST test suite method which is based in the VOHE system also showed that EDH-C algorithm exhibits higher security for data transmissions than DH in view of unpredictability and complexity.

Chapter 6

CONCLUSIONS AND PROSPECT

6.1 Conclusions

This work presents a new method of encrypting holographic information that can be employed communications between deep submergence research vehicles to provide fast communications with highest security. The encryption model has been successfully simulated using the COMSOL Multiphysics to simulate holograms and Fourier lens in the VOHE system. The system has two keys for encryption and decryption which are required to be coherent with each other. The wavelength λ was considered as a first key and the focal lengths *f* was considered as a second key.

In chapter 1, a brief introduction and background for the development of an optical information security development in view of recent emerged cryptology systems were given, and basic theories surrounding this technology were reviewed. The research's objectives goals of this study were designated and our proposal methods were discussed.

In chapter 2, the details of the VOHE system design process including the holographic encryption process, the holographic decryption process and the transmission's process were introduced.

In chapter 3, an expanded RSA (ERSA) algorithm is using a complex function to send system information such as (λ, *f*) (for e.g., λ = 632.8 nm, *f* = 4.20 mm) as a message to a receiver. The

evaluation results, which were based on Pollard's rho method have been used to compute $\bar{i}$ of modulus *N* for 8 bits, 12 bits, 16 bits and 32 bits, respectively. Accordingly and under the average output loop $\bar{i}$ of Pollard's rho method, the ERSA algorithm is more secure than the RSA algorithm when both have the same key size.

In Chapter 4, the sender and the receiver are exchanging information (IFP) using the EDH-C algorithm to construct a shared key. The obtained results exhibit the average output loop *i* and processing time *t* that are calculated by pollard Rho method. The obtained results shows that EDH-C is more secure than DH when the key-size is higher than 24-bit that makes EDH-C more appropriate method for strengthen the security. Beside of the security evaluation, efficiency evaluation has also been conducted. The results show that EDH-C method takes a slightly longer processing time to break down the PK_a code than the DH algorithm. As we mentioned in previous Chapters, there is a trade-off between efficiency and security, and we need to make a balance between them. Hence, the evaluation results which were based on the Pollard's Rho method indicate that EDH-C method has a better performance in view of security and efficiency as well.

In chapter 5, During the encryption and the decryption processes of EDH and DH algorithms, the minimum MSE results have obtained when the reference wave λ_R was set at 632.8 nm and the focal length was set at $f = 4.20$ mm. From the results, the EDH algorithm exhibits highest performance than DH in view of minimum MSE. Furthermore, security evaluation of the ERSA public key algorithm was also conducted using the NIST's test for examining the randomness of the transmitted data. Subsequently, the randomness of the transmitted message for both methods was evaluated using NIST

tests and the results show that the message that was encrypted by the proposed EDH-C algorithm had higher security than DH in view of unpredictability and complexity of the transmitted message over unsecure channel.

6.2 Prospect

In this work, we considered that the encryption process was only done between two nodes. In our future research, we will further investigate the security of data transmissions over multi-node network systems. Subsequently, we will further investigate the security of data transmissions over various hyper-complex number systems.

REFERENCE

[1] B. Javidi, *Optical and digital techniques for information security* vol. 1: Springer Science & Business Media, 2006.

[2] J. W. Goodman, *Introduction to Fourier optics*: Roberts and Company Publishers, 2005.

[3] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters,* vol. 20, pp. 767-769, 1995.

[4] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Optics & Laser Technology,* vol. 57, pp. 327-342, 2014.

[5] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Advances in Optics and Photonics,* vol. 6, pp. 120-155, 2014.

[6] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," *Applied optics,* vol. 37, pp. 6247-6255, 1998.

[7] D. C. Weber and J. D. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," *Optical Engineering,* vol. 38, pp. 62-68, 1999.

[8] K. H. Fielding, J. L. Horner, and C. K. Makekau, "Optical fingerprint identification by binary joint transform correlation," *Optical Engineering,* vol. 30, pp. 1958-1962, 1991.

[9] A. Stoianov, C. Soutar, and A. Graham, "High-speed fingerprint verification using optical correlator," in *Optical Pattern Recognition IX*, 1998, pp. 242-252.

[10] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Optics letters,* vol. 36, pp. 22-24, 2011.

[11] M. Cho, A. Mahalanobis, and B. Javidi, "3D passive photon counting automatic target recognition

using advanced correlation filters," *Optics letters,* vol. 36, pp. 861-863, 2011.

[12]E. Pérez-Cabré, H. C. Abril, M. S. Millán, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *Journal of optics,* vol. 14, p. 094001, 2012.

[13]W. He, X. Peng, X. Meng, and X. Liu, "Optical hierarchical authentication based on interference and hash function," *Applied optics,* vol. 51, pp. 7750-7757, 2012.

[14]S. K. Rajput and N. K. Nishchal, "Image encryption and authentication verification using fractional nonconventional joint transform correlator," *Optics and Lasers in Engineering,* vol. 50, pp. 1474-1483, 2012.

[15]S. K. Rajput and N. K. Nishchal, "An optical encryption and authentication scheme using asymmetric keys," *JOSA A,* vol. 31, pp. 1233-1238, 2014.

[16]W. Chen and X. Chen, "Optical multiple-image authentication based on modified Gerchberg–Saxton algorithm with random sampling," *Optics Communications,* vol. 318, pp. 128-132, 2014.

[17]X. Wang, W. Chen, and X. Chen, "Optical encryption and authentication based on phase retrieval and sparsity constraints," *IEEE Photonics Journal,* vol. 7, pp. 1-10, 2015.

[18]W. Chen and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," *Optics and Lasers in Engineering,* vol. 73, pp. 123-127, 2015.

[19]T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Information verification cryptosystem using one-time keys based on double random phase encoding and public-key cryptography," *Optics and Lasers in Engineering,* vol. 83, pp. 48-58, 2016.

[20]B. Wang, C.-C. Sun, W.-C. Su, and A. E. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," *Applied Optics,* vol. 39, pp. 4788-4793, 2000.

[21]G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding

in the fractional Fourier domain," *Optics letters,* vol. 25, pp. 887-889, 2000.

[22]B. Zhu, S. Liu, and Q. Ran, "Optical image encryption based on multifractional Fourier transforms," *Optics letters,* vol. 25, pp. 1159-1161, 2000.

[23]G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters,* vol. 29, pp. 1584-1586, 2004.

[24]G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," *Optics communications,* vol. 232, pp. 115-122, 2004.

[25]S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Processing Letters,* vol. 13, pp. 329-332, 2006.

[26]Z. Liu and S. Liu, "Random fractional Fourier transform," *Optics letters,* vol. 32, pp. 2088-2090, 2007.

[27]R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express,* vol. 15, pp. 16067-16079, 2007.

[28]R. Tao, J. Lang, and Y. Wang, "Optical image encryption based on the multiple-parameter fractional Fourier transform," *Optics letters,* vol. 33, pp. 581-583, 2008.

[29]N. Zhou, T. Dong, and J. Wu, "Novel image encryption algorithm based on multiple-parameter discrete fractional random transform," *Optics Communications,* vol. 283, pp. 3037-3042, 2010.

[30]J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain," *Optics Communications,* vol. 338, pp. 181-192, 2015.

[31]L. Sui, K. Duan, and J. Liang, "Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps," *Optics Communications,* vol. 343,

pp. 140-149, 2015.

[32]J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation," *Optics and Lasers in Engineering,* vol. 50, pp. 929-937, 2012.

[33]X. Luo, J. Fan, and J. Wu, "Single-channel color image encryption based on the multiple-order discrete fractional Fourier transform and chaotic scrambling," in *2012 IEEE International Conference on Information Science and Technology*, 2012, pp. 780-784.

[34]J. Lang and Z. Hao, "Novel image fusion method based on adaptive pulse coupled neural network and discrete multi-parameter fractional random transform," *Optics and Lasers in Engineering,* vol. 52, pp. 91-98, 2014.

[35]Q. Ran, D. S. Yeung, E. C. Tsang, and Q. Wang, "General multifractional Fourier transform method based on the generalized permutation matrix group," *IEEE Transactions on Signal Processing,* vol. 53, pp. 83-98, 2004.

[36]Q. Ran, H. Zhang, J. Zhang, L. Tan, and J. Ma, "Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform," *Optics letters,* vol. 34, pp. 1729-1731, 2009.

[37]Q. Ran, T. Zhao, L. Yuan, J. Wang, and L. Xu, "Vector power multiple-parameter fractional Fourier transform of image encryption algorithm," *Optics and Lasers in Engineering,* vol. 62, pp. 80-86, 2014.

[38]Q. Ran, L. Yuan, and T. Zhao, "Image encryption based on nonseparable fractional Fourier transform and chaotic map," *Optics Communications,* vol. 348, pp. 43-49, 2015.

[39]S. Somaraj and M. A. Hussain, "A novel image encryption technique using RGB pixel displacement for color images," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, 2016, pp. 275-279.

[40]H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyrator transform," *Optics and Lasers in Engineering,* vol. 51, pp. 768-775, 2013.

[41]B. Awdun and G. Li, "The color image encryption technology based on DNA encoding & sine chaos," in *2016 International Conference on Smart City and Systems Engineering (ICSCSE)*, 2016, pp. 539-544.

[42]X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access,* vol. 5, pp. 6429-6436, 2017.

[43]F. Han, X. Liao, B. Yang, and Y. Zhang, "A hybrid scheme for self-adaptive double color-image encryption," *Multimedia Tools and Applications,* vol. 77, pp. 14285-14304, 2018.

[44]O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi*, et al.*, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access,* vol. 7, pp. 4184-4194, 2018.

[45]C. Shen, J. Tan, C. Wei, and Z. Liu, "Coherent diffraction imaging by moving a lens," *Optics express,* vol. 24, pp. 16520-16529, 2016.

[46]J. Li, J. Li, L. Shen, Y. Pan, and R. Li, "Optical image encryption and hiding based on a modified Mach-Zehnder interferometer," *Optics express,* vol. 22, pp. 4849-4860, 2014.

[47]Y. Zhang and B. Wang, "Optical image encryption based on interference," *Optics Letters,* vol. 33, pp. 2443-2445, 2008.

[48]B. Wang and Y. Zhang, "Double images hiding based on optical interference," *Optics communications,* vol. 282, pp. 3439-3443, 2009.

[49]W. Chen, C. Quan, and C. Tay, "Optical color image encryption based on Arnold transform and interference method," *Optics communications,* vol. 282, pp. 3680-3685, 2009.

[50]C. J. Tay, C. Quan, W. Chen, and Y. Fu, "Color image encryption based on interference and virtual optics," *Optics & Laser Technology,* vol. 42, pp. 409-415, 2010.

[51]N. Zhu, Y. Wang, J. Liu, J. Xie, and H. Zhang, "Optical image encryption based on interference of polarized light," *Optics Express,* vol. 17, pp. 13418-13424, 2009.

[52]D. Weng, N. Zhu, Y. Wang, J. Xie, and J. Liu, "Experimental verification of optical image encryption based on interference," *Optics Communications,* vol. 284, pp. 2485-2487, 2011.

[53]C.-H. Niu, X.-L. Wang, N.-G. Lv, Z.-H. Zhou, and X.-Y. Li, "An encryption method with multiple encrypted keys based on interference principle," *Optics Express,* vol. 18, pp. 7827-7834, 2010.

[54]B.-C. Chen and H.-Z. Wang, "Optically-induced-potential-based image encryption," *Optics express,* vol. 19, pp. 22619-22627, 2011.

[55]Y. Zhang, B. Wang, and Z. Dong, "Enhancement of image hiding by exchanging two phase masks," *Journal of Optics A: Pure and Applied Optics,* vol. 11, p. 125406, 2009.

[56]P. Kumar, J. Joseph, and K. Singh, "Optical image encryption based on interference under convergent random illumination," *Journal of Optics,* vol. 12, p. 095402, 2010.

[57]P. Kumar, J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Applied optics,* vol. 50, pp. 1805-1811, 2011.

[58]X. Wang and D. Zhao, "Optical image hiding with silhouette removal based on the optical interference principle," *Applied optics,* vol. 51, pp. 686-691, 2012.

[59]X. Wang and D. Zhao, "Image encoding based on coherent superposition and basic vector operations," *Optics Communications,* vol. 284, pp. 945-951, 2011.

[60]L. Liu, M. Shan, Z. Zhong, and B. Liu, "Color image encryption based on enhanced optical

interference with different diffraction distances and linear phase color-blend," *Journal of Optics,* vol. 21, p. 015701, 2018.

[61]A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Optics letters,* vol. 30, pp. 1644-1646, 2005.

[62]Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Security analysis of optical encryption," in *Unmanned/Unattended Sensors and Sensor Networks II*, 2005, p. 598603.

[63]U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Optics Express,* vol. 14, pp. 3181-3186, 2006.

[64]X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *optics letters,* vol. 31, pp. 1044-1046, 2006.

[65]X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Optics letters,* vol. 31, pp. 3261-3263, 2006.

[66]X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," *Optics express,* vol. 23, pp. 18955-18968, 2015.

[67]G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," *Applied Optics,* vol. 46, pp. 5257-5262, 2007.

[68]G. Situ, D. S. Monaghan, T. J. Naughton, J. T. Sheridan, G. Pedrini, and W. Osten, "Collision in double random phase encoding," *Optics Communications,* vol. 281, pp. 5122-5125, 2008.

[69]G. Situ, G. Pedrini, and W. Osten, "Collision in double-phase encryption based on fractional Fourier transform," in *2009 International Conference on Optical Instruments and Technology:*

Optoelectronic Information Security, 2009, p. 751205.

[70] A. M. Youssef, "On the security of a cryptosystem based on multiple-parameters discrete fractional Fourier transform," *IEEE Signal Processing Letters,* vol. 15, pp. 77-78, 2008.

[71] W. Qin and X. Peng, "Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys," *Journal of Optics A: Pure and Applied Optics,* vol. 11, p. 075402, 2009.

[72] J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, and N. Bolognini, "Known-plaintext attack on a joint transform correlator encrypting system," *Optics letters,* vol. 35, pp. 3553-3555, 2010.

[73] Q. Wan, X. Peng, and X. Meng, "Cryptanalysis of optical encryption schemes based on joint transform correlator architecture," *Optical Engineering,* vol. 50, p. 028201, 2011.

[74] W. He, X. Peng, X. Meng, and X. Liu, "Collision in optical image encryption based on interference and a method for avoiding this security leak," *Optics & Laser Technology,* vol. 47, pp. 31-36, 2013.

[75] I. Mehra, S. K. Rajput, and N. K. Nishchal, "Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification," *Optical Engineering,* vol. 52, p. 028202, 2013.

[76] Y. Xiong, A. He, and C. Quan, "Cryptanalysis of an optical cryptosystem based on phase-truncated Fourier transform and nonlinear operations," *Optics Communications,* vol. 428, pp. 120-130, 2018.

[77] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering,* vol. 124, p. 105816, 2020.

[78] Y. Xiong, A. He, and C. Quan, "Hybrid attack on an optical cryptosystem based on phase-truncated Fourier transforms and a random amplitude mask," *Applied Optics,* vol. 57, pp. 6010-6016, 2018.

[79]R. L. Rivest, "Cryptography," in *Algorithms and complexity*, ed: Elsevier, 1990, pp. 717-755.

[80]Z. Kartit, A. Azougaghe, H. K. Idrissi, M. El Marraki, M. Hedabou, M. Belkasmi*, et al.*, "Applying encryption algorithm for data security in cloud storage," in *International Symposium on Ubiquitous Networking*, 2015, pp. 141-154.

[81]C. Paar and J. Pelzl, "Introduction to public-key cryptography," in *Understanding Cryptography*, ed: Springer, 2010, pp. 149-171.

[82]W. Stallings, "Cryptography and Network Security: Principles and Practices,‖ Prentice Hall," *Upper Saddle River, New Jersey, USA,* 2003.

[83]R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, pp. 120-126, 1978.

[84]V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, 1985, pp. 417-426.

[85]N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,* vol. 48, pp. 203-209, 1987.

[86]A. K. Lenstra, "Key lengths," Wiley 0471648302, 2006.

[87]A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of cryptology,* vol. 14, pp. 255-293, 2001.

[88]S. Moriai, "Security Evaluation of Cryptographic Technology Security," in *NICT NEWS No. 426* 3.2003, pp. 1-2.

[89]E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Applied Optics,* vol. 39, pp. 2313-2320, 2000.

[90]B. Javidi and T. Nomura, "Securing information by use of digital holography," *Optics letters,* vol.

25, pp. 28-30, 2000.

[91]L. Yu and L. Cai, "Multidimensional data encryption with digital holography," *Optics communications,* vol. 215, pp. 271-284, 2003.

[92]N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using digital holography," *Optical Engineering,* vol. 43, pp. 2959-2967, 2004.

[93]X. Peng, L. Yu, and L. Cai, "Double-lock for image encryption with virtual optical wavelength," *Optics express,* vol. 10, pp. 41-45, 2002.

[94]X. Peng, Z. Cui, and T. Tan, "Information encryption with virtual-optics imaging system," *Optics communications,* vol. 212, pp. 235-245, 2002.

[95]X. Meng, L. Cai, X. Xu, X. Yang, X. Shen, G. Dong*, et al.*, "Two-step phase-shifting interferometry and its application in image encryption," *Optics letters,* vol. 31, pp. 1414-1416, 2006.

[96]X. Meng, L. Cai, X. Xu, X. Yang, X. Shen, G. Dong*, et al.*, "Full-phase image encryption by two-step phase-shifting interferometry," *Optik,* vol. 119, pp. 434-440, 2008.

[97]N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *JOSA A,* vol. 16, pp. 1915-1927, 1999.

[98]X. Wang and D. Zhao, "Fully phase multiple-image encryption based on superposition principle and the digital holographic technique," *Optics Communications,* vol. 285, pp. 4280-4284, 2012.

[99]L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Optics Express,* vol. 14, pp. 8552-8560, 2006.

[100]P. Yang and T. Nagase, "Analysis of a Virtual Optical Encryption Holographic System: Decrypted code using the multiple-bit virtual optical encryption holographic system based on the COMSOL

Multiphysics," in *2019 6th International Conference on Systems and Informatics (ICSAI)*, 2019, pp. 799-803.

[101]Y. Peng, T. Nagase, S. You, and T. Kanamoto, "A VOHE System for Underwater Communications," *Electronics,* vol. 9, p. 1557, 2020.

[102]Y. Peng, T. Nagase, and T. Kanamoto, "An Optical Encryption Digital Holographic System Based on RSA Algorithm," *Information: an international Interdisciplinary journal,* vol. 23, pp. 139-147, 2020.

[103]S. Xi, N. Yu, X. Wang, X. Wang, L. Lang, H. Wang*, et al.*, "Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram," *Optics and Lasers in Engineering,* vol. 127, p. 105953, 2020.

[104]T. Zhao and Y. Chi, "A Multi-User Encryption and Authentication System Based on Joint Transform Correlation," *Entropy,* vol. 21, p. 850, 2019.

[105]R. Ren, Z. Jia, J. Yang, N. K. Kasabov, and X. Huang, "Quasi-Noise-Free and Detail-Preserved Digital Holographic Reconstruction," *IEEE Access,* vol. 7, pp. 52155-52167, 2019.

[106]H. T. Chang, Y.-T. Wang, and C.-Y. Chen, "Angle multiplexing optical image encryption in the Fresnel transform domain using phase-only computer-generated hologram," in *Photonics*, 2020, p. 1.

[107]K. B. Doh, K. Kim, and T.-C. Poon, "Computer generated holographic image processing for information security," in *International Conference on Parallel and Distributed Computing: Applications and Technologies*, 2004, pp. 111-115.

[108]B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Optics letters,* vol. 28, pp. 269-271, 2003.

[109]N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Optics Communications,* vol. 343, pp. 10-21, 2015.

[110]D. Kong, L. Cao, G. Jin, and B. Javidi, "Three-dimensional scene encryption and display based on computer-generated holograms," *Applied optics,* vol. 55, pp. 8296-8300, 2016.

[111]E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Applied Optics,* vol. 39, pp. 6595-6601, 2000.

[112]H. Kim, D.-H. Kim, and Y. H. Lee, "Encryption of digital hologram of 3-D object by virtual optics," *Optics express,* vol. 12, pp. 4912-4921, 2004.

[113]X. Wang, D. Zhao, F. Jing, and X. Wei, "Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics," *Optics express,* vol. 14, pp. 1476-1486, 2006.

[114]A. Chatterjee, J. Dhanotia, V. Bhatia, and S. Prakash, "Virtual optical encryption using phase shifted digital holography and RSA algorithm," in *2018 3rd International Conference on Microwave and Photonics (ICMAP)*, 2018, pp. 1-2.

[115]Y. Gao, Z. Zhang, and G. Liu, "Three-dimensional display using computer-generated hologram based on virtual optics," *Optik,* vol. 121, pp. 1395-1400, 2010.

[116]Y.-H. Seo, H.-J. Choi, J.-W. Bae, H.-J. Kang, S.-H. Lee, J.-S. Yoo*, et al.*, "A new coding technique for digital holographic video using multi-view prediction," *IEICE TRANSACTIONS on Information and Systems,* vol. 90, pp. 118-125, 2007.

[117]J. Kedmi and A. Friesem, "Optimal holographic Fourier-transform lens," *Applied optics,* vol. 23, pp. 4015-4019, 1984.

[118]D. B. Doherty, R. J. Gove, M. L. Burton, and R. D. Miller, "Pulse width modulation for spatial light modulator with split reset addressing," ed: Google Patents, 1996.

[119]M. K. Kim, "Principles and techniques of digital holographic microscopy," *SPIE reviews,* vol. 1, p. 018005, 2010.

[120]S. Jeon, J. Cho, J. Jin, and N.-C. Park, "Applications of digital holography with a single low-coherence light source," in *Asia Communications and Photonics Conference*, 2016, p. AF3J. 3.

[121]M. A. Bandres and J. C. Gutiérrez-Vega, "Ince–gaussian beams," *Optics letters,* vol. 29, pp. 144-146, 2004.

[122]D. C. O'Shea, T. J. Suleski, A. D. Kathman, and D. W. Prather, *Diffractive optics: design, fabrication, and test* vol. 62: SPIE press, 2004.

[123]N. Farr, A. Bowen, J. Ware, C. Pontbriand, and M. Tivey, "An integrated, underwater optical/acoustic communications system," in *OCEANS'10 IEEE SYDNEY*, 2010, pp. 1-6.

[124]I. Bányász, "Refractive index modulation vs. before-bleach optical density modulation characteristics of silver halide phase holograms," *Optics communications,* vol. 244, pp. 79-91, 2005.

[125]W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, pp. 644-654, 1976.

[126]N. K. Efremidis, Z. Chen, M. Segev, and D. N. Christodoulides, "Airy beams and accelerating waves: an overview of recent advances," *Optica,* vol. 6, pp. 686-701, 2019.

[127]B. Kaliski and J. Staddon, "PKCS# 1: RSA cryptography specifications version 2.0," RFC 2437, October1998.

[128]M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information*

theory, vol. 36, pp. 553-558, 1990.

[129]H. KUWAKADO, K. KOYAMA, and Y. TSURUOKA, "A New RSA-Type Scheme Based on Singular Cubic Curves y 2< cd02261. gif> x 3+ bx 2 (mod n)," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences,* vol. 78, pp. 27-33, 1995.

[130]H. Elkamchouchi, K. Elshenawy, and H. Shaban, "Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers," in *The 8th International Conference on Communication Systems, 2002. ICCS 2002.*, 2002, pp. 91-95.

[131]G. Castagnos, "An efficient probabilistic public-key cryptosystem over quadratic fields quotients," *Finite Fields and Their Applications,* vol. 13, pp. 563-576, 2007.

[132]G. Stergiopoulos, M. Kandias, and D. Gritzalis, "Approaching encryption through complex number logarithms," in *2013 International Conference on Security and Cryptography (SECRYPT)*, 2013, pp. 1-6.

[133]P. R. Anand, G. Bajpai, and V. Bhaskar, "Real-time symmetric cryptography using quaternion julia set," *IJCSNS International Journal of Computer Science and Network Security,* vol. 9, pp. 20-26, 2009.

[134]J. M. Pollard, "Monte Carlo methods for index computation (" *Mathematics of computation,* vol. 32, pp. 918-924, 1978.

[135]E. Teske, "Speeding up Pollard's rho method for computing discrete logarithms," in *International Algorithmic Number Theory Symposium*, 1998, pp. 541-554.

[136]R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM,* vol. 21, pp. 294-299, 1978.

[137]H. Li, R. Liu, Y. Pan, and T. Xie, "Cryptanalysis of HK17," *IACR Cryptol. ePrint Arch.,* vol.

2017, p. 1259, 2017.

[138]R. Churchhouse, R. Churchhouse, and R. Churchhouse, *Codes and ciphers: Julius Caesar, the Enigma, and the Internet*: Cambridge University Press, 2002.

[139]W. Tutte, "Fish and I," ed, 1998.

[140]D. Wackerly, W. Mendenhall, and R. L. Scheaffer, *Mathematical statistics with applications*: Cengage Learning, 2014.

[141]E. Swathika, N. Karthika, and B. Janet, "Image Encryption and Decryption using Chaotic System," in *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, 2019, pp. 30-37.

[142]F. Pareschi, R. Rovatti, and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Transactions on Information Forensics and Security,* vol. 7, pp. 491-505, 2012.

[143]E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, *Recommendation for key management: Part 1: General*: National Institute of Standards and Technology, Technology Administration, 2006.

Appendix A

A.1 Key size

Appendix 1 shows the key sizes of different Integers and Complex numbers are 8 bits, 12 bits, 16 bits, 24 bits, 28 bits, and 32 bits, respectively.

Key size	Integer	Complex number
8	{137,149,157,173,…,233,241}	{9+10*i,* 8+13*i*, 10+13*i*, 9+14*i*, 5+22*i*…}
12	{2053, 2381, 2677, 2837, 3121, 3449, 3617, 3929, 4001, 4073…}	{30+37*i,* 34+41*i*, 40+43*i*, 47+48*i*, 42+55*i*, 50+51*i*, 32+63*i*, 17+70*i*, 20+81*i*, 60+61*i*,... }
16	{34231, 38237, 40829, 44753, 46991, 49331, 53189, 55501, 60077, 65381…}	{130+131*i,* 134+139*i*, 140+139*i*, 142+145*i*, 150+157*i*, 171+176*i*, 182+185*i*, 191+196*i*, 202+203*i*, 220+223*i*,... }
20	{545473, 601021, 635939, 702011, 748133, 799303, 838403, 904297, 985403, 1007519...}	{614+539*i,* 775+536*i*, 741+596*i*, 557+532*i*, 740+621*i*, 676+641*i*, 780+733*i*, 863+830*i*, 909+904*i*, 1022+1003*i*,... }
24	{8725183, 9498409, 11112551, 12381361, 13237751, 14034649, 14791223, 15125567, 16630373, 16751627...}	{2347+2052*i*, 2561+2534*i,* 2939+2824*i*, 3240+2077*i,* 3247+2998*i*, 3980+3317*i,* 4022+2645*i*, 4054+2969*i*, 4046+3751*i*, 5462+1725*i*... }
28	{139657267, 146941699, 157894349, 182838211, 193173991, 213934901, 229365319, 233025703, 259243799, 265196483...}	{8971+8856*i*, 9805+9056*i*, 10750+10153*i,* 11181+10154*i,* 11630+11513*i*, 14261+12994*i,* 14149+12164*i*, 16289+12290*i,* 15012+14413*i*, 15949+15204*i*... }
32	{2279952011, 2495028917, 2720644939, 2906260613, 3088821539, 3231291307, 3457897997, 3677244997, 3883730813, 4222436927...}	{33362+39587*i*, 40315+39002*i*, 45157+37592*i,* 43468+42417*i,* 48049+44406*i*, 52948+38123*i,* 66565+40674*i*, 64669+54446*i,* 60540+54853*i*, 65631+61816*i*... }

A.2 Security bit (S-bit)

Appendix 2 show an example of how to calculate S-bit, we assign two parameters, one is decimal number and the second one is complex number, e.g., $g = 37$ and $g = 6 + 1i$, respectively. Different elements are generated by calculating the value of $Z = 3^k \bmod g$, where k is a safety bit we call it a security bit or S-bit [88]. The results of Z is a cyclic number and in this example the cyclic number is 18, therefore the S-bit is 18th.

$Z = 3^k \bmod g$	Z *for* $g = 37$	Z *for* $g = 6+1i$
$3^1 \bmod g$	3	$2+6i$
$3^2 \bmod g$	9	$2+5i$
$3^3 \bmod g$	27	$2+2i$
$3^4 \bmod g$	7	$0+5i$
$3^5 \bmod g$	21	$2+3i$
$3^6 \bmod g$	26	$1+2i$
$3^7 \bmod g$	4	$3+6i$
$3^8 \bmod g$	12	$5+5i$
$3^9 \bmod g$	36	$5+1i$
$3^{10} \bmod g$	34	$3+1i$
$3^{11} \bmod g$	28	$3+2i$
$3^{12} \bmod g$	10	$3+5i$
$3^{13} \bmod g$	30	$5+2i$
$3^{14} \bmod g$	16	$3+4i$
$3^{15} \bmod g$	11	$4+5i$
$3^{16} \bmod g$	33	$2+1i$
$3^{17} \bmod g$	25	$0+2i$
$3^{18} \bmod g$	1	$0+6i$
$3^{19} \bmod g$	3	$2+6i$

A.3 Pollard’s rho method (DH)

Select, $PK = 3977122$, $g = 5$, $p = 12979877$ the Pollard's Rho method to calculate the complexity of finding the private key a. ($PK = g^{a} \bmod p$)

i	x	α	β	X	A	B
1	5	1	0	6905733	1	1
2	6905733	1	1	1217613	3	2
3	2839498	2	2	8027728	6	5
4	1217613	3	2	5940330	7	6
5	6886952	6	4	10833336	14	13
6	8027728	6	5	4377158	56	52
7	1199009	7	5	8882371	112	106
8	5940330	7	6	5216626	113	107
9	11540636	14	12	616880	115	107
10	10833336	14	13	8120804	230	216
11	2587590	28	26	12285816	230	218
12	4377158	56	52	4382021	920	872
13	10145646	56	53	7114150	920	874
14	8882371	112	106	9115349	922	874
15	5472224	113	106	9327849	1844	1750
16	5216626	113	107	10241018	3688	3501
…	…	…	…	…	…	…
7897	9715877	4241792	2793116	1945840	12455892	4793135
7898	4538224	4241792	2793117	7876716	12455893	4793136
7899	9711243	4241793	2793117	3448422	11931911	9586272
7900	10809347	8483586	5586234	5473803	10883946	6192669
7901	12262222	8483586	5586235	7507895	8788016	12385339
7902	9391602	8483587	5586235	4538224	8788016	12385341
7903	3988550	3987298	11172470	10809347	4596158	11790806
7904	8633614	3987298	11172471	9391602	4596159	11790807
7905	4228439	3987299	11172471	8633614	9192318	10601739
7906	3574064	3987299	11172471	3574064	9192319	10601740
Output	**a = {373, 3245342, 6490311, 9735280}**				**i = 7906**	**t =28.324198s**

A.4 Pollard’s rho method (EDH-C)

Select, $PK = 380+3241i$, $g = 5$, $p = 2561+2534i$ an expanded Pollard's Rho method to calculate the complexity of finding the private key a. ($PK = g^{a} \bmod p$)

i	x	α	β	X	A	B
1	-2529+2561i	1	0	-2509+2561i	2	0
2	-2509+2561i	2	0	-1032+2315i	2	2
3	1439+2093i	2	1	-1664+2356i	3	3
4	-1032+2315i	2	2	-1091+1304i	3	5
5	-119+1358i	3	2	225+2997i	3	7
6	-1664+2356i	3	3	-593+2652i	7	14
7	-322+3310i	3	4	-54+243i	8	15
8	-1091+1304i	3	5	-2272+2326i	17	30
9	1670+2263i	3	6	-434+1821i	17	32
10	225+2997i	3	7	1658+2150i	19	32
11	-1639+2067i	6	14	144+2830i	19	34
12	-593+2652i	7	14	-937+2023i	40	68
13	-485+509i	8	14	1399+1661i	41	69
14	-54+243i	8	15	294+3334i	42	70
…	…	…	…	…	…	…
11802	-1449+1471i	7389361	1583309	293+3428i	7563801	1599045
11803	-2177+2233i	7389362	1583309	1865+2529i	7563802	1599046
11804	-1564+1896i	7389362	1583310	524+1171i	7563803	1599047
11805	-218+1797i	7389363	1583310	-423+2760i	7563804	1599048
11806	-1117+3890i	7389364	1583310	-619+2335i	2147733	3198096
11807	54+2782i	7389364	1583311	-2177+2233i	2147734	3198097
11808	216+3720i	7389365	1583311	-218+1797i	2147735	3198098
11809	-50+2863i	1798854	3166622	54+2782i	2147736	3198099
11810	-1691+2809i	1798854	3166623	-50+2863i	4295474	6396198
11811	924+1127i	1798854	3166624	924+1127i	4295474	6396200
Output	**a = {373, 463940, ..., 12516682}**				**i = 11811**	**t = 41.2824867s**

List of publications and presentations

Publications

① **Y. Peng,** T. Nagase, T. Kanamoto, T. Zeniya and S. You. "A virtual optical holographic encryption system using expanded Diffie-Hellman algorithm". *IEEE Access*, vol.9, pp. 22071-22077, 2021.

② **Y. Peng,** T. Nagase, S. You, and T. Kanamoto, "A VOHE System for Underwater Communications," *Electronics,* vol. 9, p. 1557, 2020.

③ **Y. Peng,** T. Nagase, and T. Kanamoto, "An Optical Encryption Digital Holographic System Based on RSA Algorithm," *Information: an international Interdisciplinary journal,* vol. 23, pp. 139-147, 2020.

④ **Y. Peng** and T. Nagase, "Analysis of a Virtual Optical Encryption Holographic System: Decrypted code using the multiple-bit virtual optical encryption holographic system based on the COMSOL Multiphysics," in *2019 6th International Conference on Systems and Informatics (ICSAI)*, 2019, pp. 799-803.

International presentations

① **Y. Peng** and T. Nagase. Analysis of a Virtual Optical Encryption Holographic System: Decrypted code using the multiple-bit virtual optical encryption holographic system based on the COMSOL Multiphysics, in 2019 6th International Conference on Systems and Informatics (ICSAI), 2-4,

November, 2019.

Domestic presentations

① **Yang P,** T. Nagase, Signal Processing based on Metamaterials. Information Processing Society of Japan-TOHOKU, Vol.2019-Hirosaki. 21, February, 2019.

② **Yang P,** T. Nagase, Virtual Optical Encryption Using Digital Lens and RSA Algorithm. Information Processing Society of Japan-TOHOKU, Vol.2019-Akita. 28, November, 2019.

③ **Yang P,** T. Nagase, Decrypted Code Using the Multiple-bit Virtual Optical Encryption Holographic System. Information Processing Society of Japan-TOHOKU, Vol.2020-Yamaga. 10, March, 2020.

④ **Yang P,** T. Nagase, A Virtual Optical Holographic Encryption System. Information Processing Society of Japan-TOHOKU, Vol.2021-Hirosaki. 18, February, 2021.