IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 23, 2020, accepted January 21, 2021, date of publication February 1, 2021, date of current version February 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055866

A Virtual Optical Holographic Encryption System Using Expanded Diffie-Hellman Algorithm

YANG PENG[1], TOMOYUKI NAGASE[1], (Senior Member, IEEE), TOSHIKI KANAMOTO[1], (Member, IEEE), TSUTOMU ZENIYA[1], (Member, IEEE), AND SHAN YOU[2]

[1]Graduate School of Science and Technology, Hirosaki University, Hirosaki 036-8561, Japan
[2]GBase, Tianjin 300384, China

Corresponding author: Tomoyuki Nagase (nagase@hirosaki-u.ac.jp)

ABSTRACT This paper presents a new method for encrypting information over a Virtual Optical Holographic Encryption (VOHE) system which employs a virtual optical system based on digital holography and Fourier lens. The VOHE system provides parameters such as propagation wavelength (λ) and focal length (f) of the Fourier lens which are keys that are used for encryption and decryption processes. The encrypted holographic information is based on an expanded Diffie-Hellman (EDH) algorithm. The method of expansion is presented based on a two-dimension complex function EDH-C. Furthermore, an expanded Pollard's Rho method was applied to evaluate the security of the proposed EDH-C algorithm. To determine the accuracy of the information retrieved by a receiver site, the mean absolute error (MAE) was calculated between the original code and retrieved code. Finally, 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 the unpredictability and complexity of the transmitted message over an insecure channel.

INDEX TERMS Optical encryption, holographic, Fourier lens, EDH algorithm, Pollard's Rho, NIST.

I. INTRODUCTION

Recently, with the rapid development of modern communication 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 will reduce the speed of the encryption process. The optical encryption technology based on holographic has emerge as a new technology that has many has many advantages such as high speed, high capacity and is multi-dimensional as well [1]–[3]. For these reasons, the optical holographic encryption technology is gradually received great attention and considered as an enabling technology [4], [5].

A Virtual Optical Holographic Encryption (VOHE) technology has been widely used in recent years to achieve better security especially in an uncommon transmission environment such as underwater communications. Numerous research efforts have 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 [6]. In the same year, E. Tajahuerce *et al.* used a digital holographic technique to encrypt 3D objects [7]. 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 [8]. Wang *et al.* has proposed a new method for synthesizing and encrypting information using a digital holographic and a virtual optical technology [9].

This paper introduces an approach for data encryption over a VOHE system using an expanded Diffie-Hellman algorithm. 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 [10]. However, we improve DH algorithm by using a

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

two-dimensional complex function (EDH-C). The main reason of using a complex function is to strengthen security over conventional Diffie-Hellman algorithm.

This paper is organized as follows: In section II, the VOHE system's encryption and decryption process and EDH-C encryption algorithm are briefly introduced, and then the security of the proposed EDH-C algorithm is evaluated using an extended Pollard's Rho method. Additional simulation and evaluation of the VOHE system's encryption and decryption process are conducted based on COMSOL Multiphysics, which is given in section III. The example is presented of how the EDH-C encryption algorithm performs for generating a share key between a sender and a receiver. In section IV, 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. Finally, the conclusions of this study are summarized in section V.

II. THE VOHE SYSTEM DESIGN

A. HOLOGRAPHIC ENCRYPTION

The structure of VOHE system that is based on digital holographic is shown in Fig. 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 pass through the Fourier to generate Fourier transformation [11]. The SLM which is an electrically programmable device that modulates light wave corresponding to a special designed pattern [12]. The digital holography information is processed and collected by CCD [13].

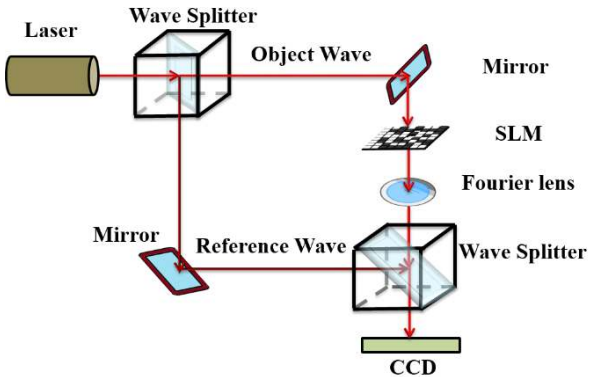


FIGURE 1. A VOHE system's model.

The light source of VOHE system is selected from a He-Ne laser with a wavelength of 632.8 *nm* [14]. 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.

B. THE ENCRYPTION AND DECRYPTION PROCESS

To comprehend the process of a VOHE system, Fig. 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 (10100101), which can be seen in the fifth row's pattern of the SLM device as shown in Fig. 1.

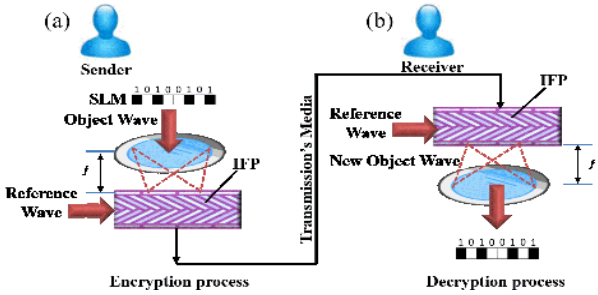


FIGURE 2. A schematic diagram of holographic encryption and decryption. (a) Encryption process; (b) Decryption process.

At the sender site, Fig. 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 transmission's media such as optical signals and acoustic signals are implemented as means for sending IFP that carries object information to a receiver [15].

At the receiver site, in Fig. 2 (b), the decryption process is done by illuminating only the reference wave with a length of λ_R which is a first decryption key to produce a new object wave. Then, the focal length f is a second decryption key and the new object wave that passes through the Fourier lens is transformed to a digital stream.

C. EXPANDED DIFFIE-HELLMAN ALGORITHM

The IFP that is generated at the sender side is required to be secured during a transmission process to the receiver over unsecure channel, as shown in Fig. 3. 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 [16].

Specifically, the XOR operations should be used with a one-time shared key SK to ensure the security of the transmitted data [17]. Therefore, we can select a different p each time and make the shared key SK different every time.

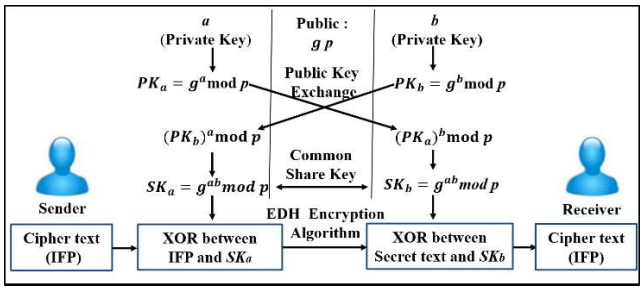


FIGURE 3. Schematic diagram of EDH-C exchange algorithm.

To summarize the proposed EDH-C algorithm, two-dimension complex function EDH-C is demonstrated of how to construct public keys.

In the algorithms 1 and 2, firstly, two numbers p and g are selected, where p is complex number [18] 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 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 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.

$$SK_a = SK_b = g^{ab} mod(x_p + iy_p) \tag{1}$$

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.

$$SK_a = SK_b = g^{ab} mod(x_p) \tag{2}$$

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 [19], [20].

In the algorithm 3 shows how to calculate private key a, out loop i and processing time t of PK_a with various key-size [21], [22]. Algorithm 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 3 can also evaluate the efficiency of both DH and EDH-C which is based on average processing time parameter t.

Algorithm 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 small size private key a from PK using 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 (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. Fig. 4 (b) shows the average processing time t 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.

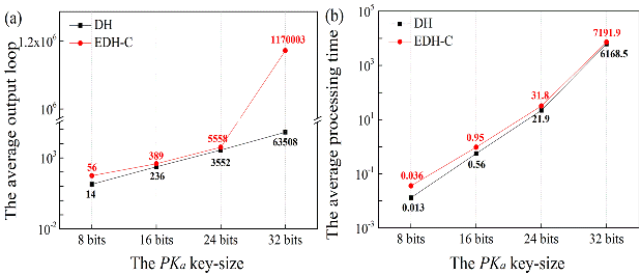


FIGURE 4. (a) The average output loop i of Pollard's rho method. (b) The average processing time t (sec) of Pollard's rho method.

The obtained results exhibit the average output loop i and processing time t that are calculated by pollard Rho method. In Fig. 4 (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 (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. As the

results show that EDH-C method takes a slightly longer processing time to break down the PK_a code than the DH algorithm.

III. SIMULATION AND DATA ANALYSIS

Computer based simulation is conducted based on a COMSOL Multiphysics tool and applying a full-wave method [23]. The parameters that are used in our simulation is given as follows: the object wavelength $\lambda_o = 632.8\ nm$, the reference wavelength $\lambda_R = 632.8\ nm$, and a Fourier lens of focal length $f = 8.3\ mm$.

A. ENCRYPTION PROCESS

To demonstrate of how the VOHE system works, the following is an example. The object's information with code (10100101) is programmed and embedded in the SLM device. Then, the output signal from SLM will proceed to the Fourier lens with a focal length of $f = 8.3\ mm$ will be a new object wave which is considered as an initial cipher. The electric field amplitude of the initial cipher is shown in Fig. 5 (a). The holography encryption process is done by creating IFP as the second cipher. The IFP is produced by interactions between initial cipher from the top side and reference wave from the left side, as shown in Fig. 5 (b). As we mentioned above that λ_o and λ_R have same value at 632.8 nm, accordingly IFP will be grafted at a 45-degree angle.

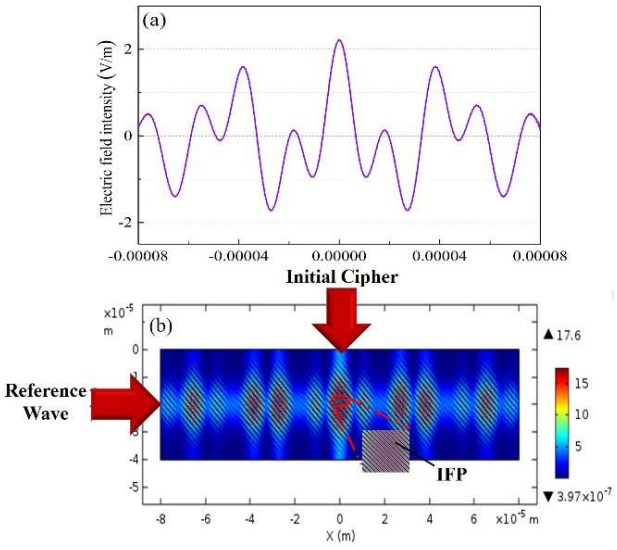


FIGURE 5. (a) The electric field amplitude of the initial cipher. (b) The encryption strength and electric field of the second cipher at $\lambda_o = \lambda_R = 632.8nm$. (Inset: the IFP with at a 45 degree angle).

The information of the IFP information should be secure and ready to be transmitted to the receiver through transmission's media.

B. EDH ALGORITHM PROCESS

The EDH-C algorithm is used to generate a share key at both a sender and a receiver that were mentioned in section II.B. The share keys SKa and SK_b are calculated by Algorithm 1 and 2 for DH and EDH-C, respectively.

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

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

$$PK_a = 3977122 \tag{3}$$

As a result, PK_a is sent to receiver.
Step 2 receiver calculates the public key

$$PK_b = 10691878 \tag{4}$$

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.

$$SK_a = 7522523 \tag{5}$$

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

$$SK_b = 7522523 \tag{6}$$

2) EDH-C ALGORITHM

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

$$PK_a = 380 + 3241i \tag{7}$$

As a result, PK_a is sent to receiver.
Step 2 receiver calculates the public key

$$PK_b = -263 + 3162i \tag{8}$$

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.

$$SK_a = -447 + 1653i \tag{9}$$

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

$$SK_b = -447 + 1653i \tag{10}$$

C. DECRYPTION PROCESS

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

$$\mathrm{ST} = \mathrm{IFP} \oplus SK_a \tag{11}$$

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 the SK_b and ST result which has received from the sender. The IFP is calculated as follows

$$\mathrm{IFP} = \mathrm{ST} \oplus SK_b \tag{12}$$

The decryption process is shown in the Fig. 6. The reference wave is used to decrypt the IFP and creates a new object wave when the decryption key is chosen to be λ_R= 632.8 *nm*, as shown in Fig. 6 (a). Hence, λ_R is considered as first key in the decryption system. Fig. 6 (b) shows that the decryption process will be failed if a different key has been selected, e.g. λ_R= 601.2 *nm*. This key λ_R is crucial because the image will not be recovered if λ_R has a different value.

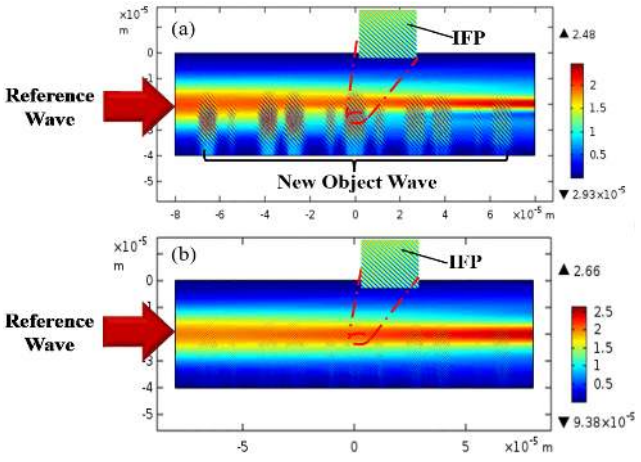


FIGURE 6. The decryption strength and electric field at: (a) λ_R = 632.8 *nm*, (Inset: the IFP with at a 45 degree angle); (b) λ_R = 601.2 *nm*.

The simulation is also performed to verify an accurate reference wavelength at the receiver during decryption process. In Fig. 7 the original code (e.g. "10100101") is compared with decrypted code using different reference wavelengths. The reference wave is tuned from 613.8 *nm* to 651.8 *nm* and keeping a Fourier lens of focal length f value at 8.30 *mm*. The comparisons between the original code of λ_R = 632.8 *nm* and that of the reference waves of (from 613.8 *nm* to 651.8 *nm*) have been conducted, and the results are shown in Fig. 7 (a), (b) and (c). We can see from these figures that the reference wave of 632.8 *nm* has highest amplitude and exhibits optimal electric field's strength, it means that the signal (in the red color) has a highest degree of matching with that of the original code's period.

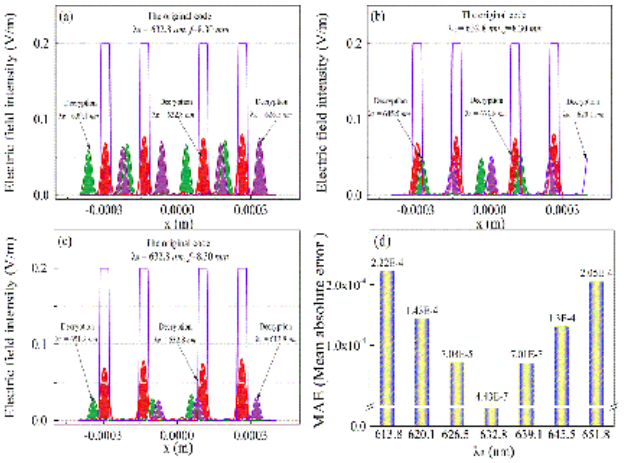


FIGURE 7. Comparisons between the original code of 632.8 *nm* and the decrypted code of the different reference wave λ: (a) 626.5 *nm*, 632.8 *nm* and 639.1 *nm*, (b) 620.1 *nm*, 632.8 *nm* and 645.5 *nm*, and (c) 613.8 *nm*, 632.8 *nm* and 651.8 *nm*; (d) The MAE of data decrypted using different reference waves from 613.8 *nm* to 651.8 *nm*.

To insure the accuracy of the information retrieved at the receiver side, the Mean Absolute Error (MAE) was calculated and different reference waves have been selected [24], [25]. As show in Fig. 7 (d), minimum MAE at $4.43e^{-7}$ is obtained when the reference wave λ_R is set to 632.8 *nm* and the result of decryption is close to that of the original code. Therefore, we can conclude that the signal with reference wave of λ_R = 632.8 *nm* is accurate value for decrypting data.

In the Fourier lens model, focal length f is considered as a second decryption key when the new wave passes through the Fourier lens to achieve the Fourier transformation. As shown in Fig. 8, the original code (e.g. "10100101") is compared by selecting various focal length f between 3.64 *mm* and 6.76 *mm* and keeping the reference wave at λ_R = 632.8 *nm*, as shown in Fig. 8 (a), 8 (b) and 8 (c). The results show that the signal of the focal length of f = 8.30 *mm* (in the red color) is matched with that of the original code's period.

As shown in Fig. 8 (d), minimum MAE at $4.43e^{-7}$ is obtained when the focal length is at f = 8.30 *mm*. It means that the signal with focal length of f = 8.30 *mm* is accurate value for decrypting data.

IV. SECURITY EVALUATION OF EDH-C ALGORITHM

This section evaluates the security of EDH-C algorithm using random evaluation test. As mentioned in section III.C, 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 NIST test suite method [26]. 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 non-random.

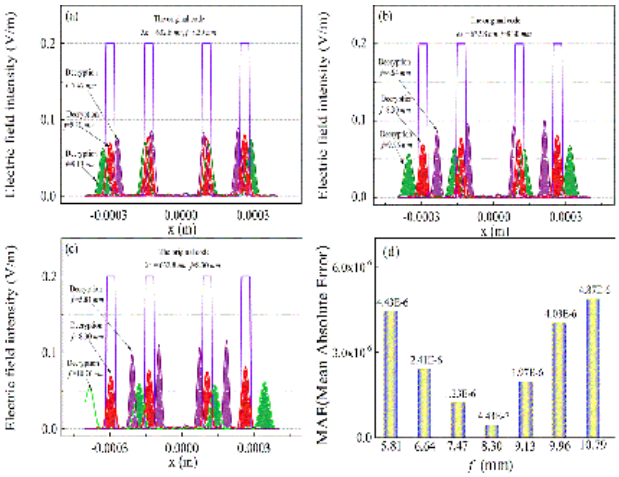


FIGURE 8. Comparisons between the original code of 8.30 *mm* and the decrypted code of the different focal length *f*: (a) 7.47 *mm*, 8.30 *mm* and 9.13 *mm*, (b) 6.64 *mm*, 8.30 *mm* and 9.96 *mm*, and (c) 5.81 *mm*, 8.30 *mm* and 10.76 *mm*; (d) The MAE of data decrypted using the different focal length from 5.81 *mm* to 10.79 *mm*.

As show in Table 1, 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 [27]. 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 section III.B).

TABLE 1. NIST test results.

Test items	DH	EDH-C
	P-value	*P*-value
Frequency	0.689157	0.841481
Block Frequency	0.689157	0.841481
Cumulative Sums	0.658638	0.929223
Runs	0.156112	0.551016
Longest Run	0.053571	0.928763
Rank	0.000000	0.000000
Approximate Entropy	0.438767	0.713633
Serial	0.016470	0.498961
Linear Complexity	0.221647	0.369399
FFT	0.013190	0.646355

In Table 1, 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. Additionally, the results show that the randomness of EDH-C *P*-value is better than the *P*-value of the DH algorithm.

V. CONCLUSION

In this paper, 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. In the VOHE system, the wavelength λ is considered as a first key and the focal lengths f is considered as a second key. The keys (λ and f) for encryption and decryption are required to be coherent with each other.

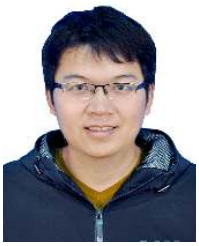
The evaluation results which are based on the Pollard's Rho method indicate that EDH-C method has a better performance in view of security and efficiency. Subsequently, NIST test suite method also showed that EDH-C algorithm exhibits higher security for data transmissions than DH in view of unpredictability and complexity. In our future research, we aim to further investigation EDH-C algorithm with other hyper-complex number systems. Furthermore, Minimum MAE was also achieved to calculate the probability of the errors of the received signal.

Ultimately, the optical encryption technology has numerous advantages such as fast operation, high security level, low cost and can be widely used.

REFERENCES

[1] S. Xi, N. Yu, X. Wang, X. Wang, L. Lang, H. Wang, W. Liu, and H. Zhai, "Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram," *Opt. Lasers Eng.*, vol. 127, Apr. 2020, Art. no. 105953.
[2] T. Zhao and Y. Chi, "A multi-user encryption and authentication system based on joint transform correlation," *Entropy*, vol. 21, no. 9, p. 850, Aug. 2019.
[3] 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.
[4] 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," *Photonics*, vol. 7, no. 1, p. 1, Dec. 2019.
[5] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.*, vol. 25, no. 1, pp. 28–30, Jan. 2000.
[6] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.*, vol. 39, no. 14, pp. 2313–2320, 2000.
[7] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.*, vol. 39, no. 35, pp. 6595–6601, Dec. 2000.
[8] H. Kim, D.-H. Kim, and Y. H. Lee, "Encryption of digital hologram of 3-D object by virtual optics," *Opt. Exp.*, vol. 12, pp. 4912–4921, Oct. 2004.
[9] X. Wang, D. Zhao, F. Jing, and X. Wei, "Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics," *Opt. Exp.*, vol. 14, no. 4, pp. 1476–1486, 2006.
[10] R. C. Merkle, "Secure communications over insecure channels," *Commun. ACM*, vol. 21, no. 4, pp. 294–299, Apr. 1978.
[11] J. Kedmi and A. Friesem, "Optimal holographic Fourier-transform lens," *Appl. Opt.*, vol. 23, no. 22, pp. 4015–4019, 1984.
[12] D. B. Doherty, R. J. Gove, M. L. Burton, and R. D. Miller, "Pulse width modulation for spatial light modulator with split reset addressing," U.S. Patent 5 497 172 A, Mar. 5, 1996.
[13] M. K. Kim, "Principles and techniques of digital holographic microscopy," *Proc. SPIE*, vol. 1, Apr. 2010, Art. no. 018005.
[14] S. Jeon, J. Cho, J. Jin, and N.-C. Park, "Applications of digital holography with a single low-coherence light source," in *Proc. Asia Commun. Photon. Conf.*, 2016, p. 1, Paper AF3J.3.
[15] Y. Peng, T. Nagase, S. You, and T. Kanamoto, "A VOHE system for underwater communications," *Electronics*, vol. 9, no. 10, p. 1557, Sep. 2020.
[16] R. Churchhouse, R. Churchhouse, and R. Churchhouse, *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge, U.K.: Cambridge Univ. Press, 2002.
[17] W. T. Tutte, "Fish and I," in *Coding Theory and Cryptography*. Berlin, Germany: Springer, 2000, pp. 9–17.

[18] G. Stergiopoulos, M. Kandias, and D. Gritzalis, "Approaching encryption through complex number logarithms," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, 2013, pp. 1–6.
[19] A. K. Lenstra, *Key Lengths*. Hoboken, NJ, USA: Wiley, 2006.
[20] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *J. Cryptol.*, vol. 14, no. 4, pp. 255–293, Sep. 2001.
[21] J. M. Pollard, "Monte Carlo methods for index computation (mod p)," *Math. Comput.*, vol. 32, no. 143, pp. 918–924, 1978.
[22] E. Teske, "Speeding up Pollard's rho method for computing discrete logarithms," in *Proc. Int. Algorithmic Number Theory Symp.*, 1998, pp. 541–554.
[23] 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 *Proc. 6th Int. Conf. Syst. Informat. (ICSAI)*, Nov. 2019, pp. 799–803.
[24] C. Willmott and K. Matsuura, "Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance," *Climate Res.*, vol. 30, no. 1, pp. 79–82, 2005.
[25] E. Swathika, N. Karthika, and B. Janet, "Image encryption and decryption using chaotic system," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 30–37.
[26] 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 Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 491–505, Apr. 2012.
[27] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, *Recommendation for Key Management: Part 1: General*. Gaithersburg, MD, USA: National Institute of Standards and Technology, Technology Administration, 2006.



YANG PENG was born in Shanxi, China, in 1988. He received the B.S. and M.S. degrees in electrical engineering from the North University of China, in 2008 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Graduate School of Science and Technology, Hirosaki University, Japan. His research interests include signal processing and information security.

TOMOYUKI NAGASE (Senior Member, IEEE) received the Ph.D. degree in computer science from Tohoku University, Japan, in 1992. He has eight years working experience in telecommunications practically in switching systems with industrial companies in Japan. From 2001 to 2002, he was an Adjunct Lecturer with San Diego State University. He is currently an Associate Professor with Hirosaki University, Japan. He is a member of IEICE and IPSJ.

TOSHIKI KANAMOTO (Member, IEEE) received the Ph.D. degree in information science from Osaka University, Osaka, Japan. From 1991 to 2003, he was with Mitsubishi Electric Corporation, Tokyo. Since 2016, he has been a Professor with the Department of Electronics and Information Technology, Graduate School of Science and Engineering, Hirosaki University, Aomori, Japan. He is a Senior Member of IEICE and IPSJ. Since 2001, he has been a member of the Japan Electronics and Information Technology Industries Association (JEITA).

TSUTOMU ZENIYA (Member, IEEE) received the Ph.D. degree in engineering from Yamagata University, Japan, in 2002. From 2009 to 2016, he was a Laboratory Chief with the National Cerebral and Cardiovascular Center Research Institute, Japan. He is currently a Professor with the Graduate School of Science and Technology, Hirosaki University, Japan. His research interest includes medical imaging technology.

SHAN YOU was born in Shandong, China, in 1991. He received the M.S. degree in electrical engineering from Hirosaki University, Japan, in 2020. He has five years working experience in signal processing and security in Japan. His research interests include signal processing and information security.