Three-key Triple Data Encryption Algorithm of a Cryptosystem Based on Phase-shifting Interferometry

Seok Hee Jeon¹ and Sang Keun Gil²*

¹Department of Electronic Engineering, Incheon National University, Incheon 22012, Korea
²Department of Electronic Engineering, The University of Suwon, Hwaseong 18323, Korea

(Received July 21, 2023 : revised October 19, 2023 : accepted October 22, 2023)

In this paper, a three-key triple data encryption algorithm (TDEA) of a digital cryptosystem based on phase-shifting interferometry is proposed. The encryption for plaintext and the decryption for the ciphertext of a complex digital hologram are performed by three independent keys called a wavelength key \( k_1(\lambda) \), a reference distance key \( k_2(d_r) \) and a holographic encryption key \( k_3(x,y) \), which are represented in the reference beam path of phase-shifting interferometry. The results of numerical simulations show that the minimum wavelength spacing between the neighboring independent wavelength keys is about \( \delta \lambda = 0.007 \) nm, and the minimum distance between the neighboring reference distance keys is about \( \delta d_r = 50 \) nm. For the proposed three-key TDEA, choosing the deviation of the key \( k_1(\lambda) \) as \( \delta \lambda = 0.4 \) nm and the deviation of the key \( k_3(d) \) as \( \delta d = 500 \) nm allows the number of independent keys \( k_1(\lambda) \) and \( k_2(d_r) \) to be calculated as \( N(k_1) = 80 \) for a range of 1,530–1,562 nm and \( N(d_r) = 20,000 \) for a range of 35–45 mm, respectively. The proposed method provides the feasibility of independent keys with many degrees of freedom, and then these flexible independent keys can provide the cryptosystem with very high security.

Keywords : Cryptosystem, Digital hologram, Fourier optics, Optical encryption, Phase-shifting interferometry

OCIS codes : (060.4785) Optical security and encryption; (070.1170) Analog optical signal processing; (070.4560) Data processing by optical means; (090.1995) Digital holography; (090.2880) Holographic interferometry

I. INTRODUCTION

In recent years, information hacking by unauthorized persons has become a serious problem because hacking techniques are being developed with rapid computer processing capability. In order to prevent attackers from getting confidential information, a cryptosystem is introduced in a data communication network to hide information. As for the digital types of information encryption methods, the advanced encryption standard (AES) [1] and triple data encryption standard (3DES) [2] are the most popular standard block encryption algorithms. Among the block cipher algorithms that use a symmetric key to encrypt information, 3DES is an approach that extends the short key size of DES. However, no matter how much the key size of 3DES increases, this algorithm needs more processing time and the larger quantity of data, notwithstanding increased security. Cheng et al. [3] compared overall encryption efficiency in terms of speed for a given electronic hardware platform with the three standard block encryption schemes DES, 3DES and AES. Digital encryption techniques generally use electronic devices to cipher information, while optical methods to encrypt information have been researched due to high-speed parallel processing and two-dimensional

*Corresponding author: skgil@suwon.ac.kr, ORCID 0000-0002-3828-0939

Color versions of one or more of the figures in this paper are available online.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Copyright © 2023 Current Optics and Photonics

pISSN: 2508-7266 / eISSN: 2508-7274

https://doi.org/10.3807/COPP.2023.7.6.673
large data handling advantages. Various methods for optical cryptosystems have been proposed [4–6], among which digital holography [7–9] and phase-shifting interferometry [8–15] are promising methods to mix with digital processing. In particular, a complex digital hologram function with amplitude and phase information is digitally calculated by interferograms detected on a charge-coupled device (CCD) in phase-shifting interferometry. Recently, researchers have presented optical double or triple-key encryption methods to enhance security strength and data processing volume. Jeon and Gil [16] proposed a triple DES algorithm and its optical implementation based on dual XOR logic operations, Ahouzi et al. [17] proposed an advanced algorithm using a triple random-phase encryption (TRPE) scheme in the Fourier transform domain that improves the security of optical encryption based on double random-phase encryption (DRPE), and Kumari et al. [18] also suggested a TRPE cryptosystem in the Fresnel domain. As for the multiple keys for optical encryption, Zhang and Wang [19] applied the parameters of the optical configuration to serve as additional keys for optical image encryption based on interference, which motivated us to introduce the concept of three independent keys for phase-shifting digital interferometry.

In this paper, we propose the three-key triple data encryption algorithm (TDEA) of a digital cryptosystem based on phase-shifting interferometry. The proposed method carries out digital encryption and decryption processes with three independent keys called a wavelength key, a reference distance key and a holographic encryption key. The independent wavelength keys are assumed to be determined by the tunable wavelength of a light source and the independent reference distance keys are determined by varying placement of the reference input from the Fourier transform lens in optical interferometry. In Section II, 3DES is briefly reviewed, and the proposed three-key TDEA is described. In Section III, an evaluation of the proposed method is verified by the results of numerical simulations. Conclusions are summarized in Section IV.

II. PROPOSED TRIPLE DATA ENCRYPTION ALGORITHM METHOD

The DES has been the most widely used symmetric key block cryptography and was chosen as a standard by the American National Standard Institute (ANSI) in 1977. The algorithm uses a fixed-length 56-bit key to encrypt and decrypt a 64-bit block of data. However, its 56-bit key can no longer guarantee enough security in recent cryptanalytic attacks against block ciphers. Generally, increasing the key length makes the cryptosystem more secure. The problem of increasing the key length can be overcome by using double or triple-length keys. In 1998, a 3DES called triple data encryption algorithm (TDEA), in which DES is applied three times, was adopted as the standard ANSI X9.52 [2]. Figure 1 shows a block diagram of the 3DES encryption and decryption procedure. The 3DES algorithm consists of three DES keys ($k_1$, $k_2$ and $k_3$) for the cryptosystem. There are two variations of 3DES. If three 56-bit keys $k_1$, $k_2$ and $k_3$ are independent DES keys, it is referred to as three-key 3DES and produces an effective key length of 168 bits. If two keys, $k_1$ and $k_2$, are independent keys and $k_3$ is the same as $k_1$, it is referred to as two-key 3DES and gives a smaller effective key length of 112 bits. The resultant 3DES algorithm is much harder to break compared to a single DES. The encryption and decryption of the 3DES algorithm is as follows. Assume that $k_1$, $k_2$ and $k_3$ are three independent keys in the 3DES cryptosystem. The encryption and decryption processes are expressed as

$$c(x,y) = E_{k_3}\left\{E_{k_2}\left\{E_{k_1}\left\{m(x,y)\right\}\right\}\right\}, \quad (1)$$

$$m(x,y) = D_{k_3}\left\{D_{k_2}\left\{D_{k_1}\left\{c(x,y)\right\}\right\}\right\}, \quad (2)$$

where $m(x,y)$ is a plaintext to be encrypted and $c(x,y)$ is a ciphertext.

In this paper, a cryptosystem that performs three-key TDEA based on the phase-shifting interferometry principle is proposed. The concept of the proposed method is described by the optical configuration shown in Fig. 2, which is based on a Mach–Zehnder interferometer architecture. A tunable laser diode beam is collimated by a collimating lens (CL) and is linearly polarized by a polarizer (P1), and it is divided by a beam splitter (BS1) into two plane waves of the object and the reference beams traveling in different directions. When shutters S1 and S2 are open, the downward object beam passes through an input amplitude-type spatial light modulator (SLM1) and a random phase mask (RPM), while the rightward reference beam passes through an input phase-type spatial light modulator (SLM2) and a $\lambda/4$ plate. Two lenses (L1 and L2) form a Fourier transform of the input functions into a CCD. A random phase mask is adopted to improve the dynamic range of the spatial frequency in the spatial frequency plane on the CCD. The RPM function is represented as $r(x,y) = \exp\{2\pi i q(x,y)\}$, where $q(x,y)$ is a randomly distributed function over the interval $[0, 1]$. A $\lambda/4$ plate makes the wave along the vertical axis (s-polarization axis) occur with no phase shift and the wave along the horizontal axis (p-polarization axis) occur with a phase shift of $\pi/2$ radians. This scheme provides two-step phase-shifting interferometry [20].

Firstly, a cryptosystem based on optoelectronic two-step phase-shifting interferometry, considering the wavelength

![FIG. 1. Block diagram of 3DES encryption and decryption.](Image)
of light and the distance between the input and the lens, is briefly described. Let \( m(x, y) \) be a plaintext to be encrypted and \( k(x, y) \) be a holographic encryption key in phase-shifting interferometry. The Fourier transform diffraction patterns of the object and reference beams form complex amplitude distributions at the output spatial frequency \((u, v)\) plane, and are expressed as

\[
U_o(u, v; \lambda, d_o) = \frac{1}{j\lambda f} \exp \left[ j \frac{k}{2f} \left( 1 - \frac{d_o}{f} \right) \left( u^2 - v^2 \right) \right] \\
\times \iint_{-\infty}^{\infty} m(x, y) r(x, y) \exp \left[ -j \frac{2\pi}{\lambda f} (ux - vy) \right] dx dy,
\]

(3)

\[
U_r(u, v; \lambda, d_r) = \frac{1}{j\lambda f} \exp \left[ j \frac{k}{2f} \left( 1 - \frac{d_r}{f} \right) \left( u^2 - v^2 \right) \right] \\
\times \iint_{-\infty}^{\infty} k(x, y) \exp \left[ -j \frac{2\pi}{\lambda f} (ux - vy) \right] dx dy,
\]

(4)

where \( \lambda \) is the wavelength of the light source, \( k = 2\pi/\lambda, f \) is the focal length of the lens, \( d_o \) is the object distance between SLM1 and lens L1, and \( d_r \) is the reference distance between SLM2 and lens L2. The output complex distribution will be the exact Fourier transform of the input except for the phase factor outside the integral when the distance between the input and the lens is the focal length of the lens, that is \( d_o = f \) and \( d_r = f \). It is denoted from Eqs. (3) and (4) that the phase factor in front of the Fourier transform of \( m(x, y) \) \( r(x, y) \) is \( P_o(u, v; \lambda, d_o) \) and the phase factor in front of the Fourier transform of \( k(x, y) \) is \( P_r(u, v; \lambda, d_r) \), respectively. It is interesting to note that even if the object distance \( d_o \) has any distance value, resulting in any phase factor \( P_o(u, v; \lambda, d_o) \), it does not affect the phase change contribution in Eq. (3) because the RPM function \( r(x, y) \) includes a random phase distribution, while the phase factor \( P_r(u, v; \lambda, d_r) \) with different reference distance \( d_r \) affects the phase change contribution in Eq. (4). If the object distance \( d_o \) is assumed to have the focal length \( f \) for convenience, and if the integral part in Eqs. (3) and (4), which represent Fourier transforms of the object and reference complex distributions in the spatial frequency domain, are expressed as \( M(u, v) = F \{ m(x, y) \} \) and \( K(u, v) = F \{ k(x, y) \} \), respectively, then Eqs. (3) and (4) are rewritten by

\[
U_o(u, v; \lambda) = |M(u, v)| e^{i\phi_M(u, v)},
\]

(5)

\[
U_r(u, v; \lambda, d_r) = P_r(u, v; \lambda, d_r) |K(u, v)| e^{i\phi_K(u, v)} = |P_r(u, v; \lambda, d_r)| e^{i\phi_{r}(u, v; \lambda, d_r)} |K(u, v)| e^{i\phi_K(u, v)}
\]

(6)

With Eqs. (5) and (6), the intensity pattern recorded by the CCD is given by

\[
I(u, v; \lambda, d_r; \delta) = |U_o(u, v; \lambda) + U_r(u, v; \lambda, d_r; \delta)|^2,
\]

(7)

where \( \delta \) is a phase shift in the reference beam. Two interference intensities at the output plane can be achieved with digital two-step phase-shifting interferometry when a phase shift of \( \pi/2 \) occurs between the s-polarization axis and the p-polarization axis in the reference beam. The suitable polarization direction of an output polarizer (P2) in front of the CCD gives two interference intensities. Representing the complex amplitude distribution of the object and the reference beams with Eqs. (5)–(7) can be expressed as

\[
I(u, v; \lambda, d_r; \delta) = |M|^2 + |P_r| |K|^2 + 2|P_r| |K| \cos(\Delta \phi + \delta),
\]

(8)
where variables in spatial frequency coordinates are omitted and \( \Delta \phi(u, v; \lambda, d) = \phi(u, v) - \{ \phi_R(u, v; \lambda, d) + \phi_K(u, v) \} \) denotes the phase difference between the reference and the object beams. This intensity pattern recorded by the CCD shows a noise-like random distribution due to the randomness of Eq. (3). Additionally, only the intensity distribution of the object beam \( I_o = |M(u, v)|^2 \) and only the intensity distribution of the reference beam \( I_r = |P(u, v; \lambda, d)|^2 \), which are DC-terms in the interference intensity of Eq. (8), are recorded on the CCD by controlling shutters S1 and S2 in the optical setup. In this method, a complex digital hologram function generated from phase-shifting interferometry is a kind of ciphertext that also provides random phase and random amplitude distributions. If the complex digital hologram function is assumed to be \( H(u, v; \lambda, d) = A(u, v; \lambda, d) e^{i \Delta \phi(u, v; \lambda, d)} \), the amplitude \( A(u, v; \lambda, d) \) and the phase \( \Delta \phi(u, v; \lambda, d) \) can be calculated by two intensities \( I_o(u, v; \lambda, d; \pi/2) \) and \( I_r(u, v; \lambda, d; 0) \) after removing the DC-term \( |M|^2 + |P|^2 \) \( |K|^2 \) from Eq. (8) as

\[
A(u, v; \lambda, d) = \left| P \right| K, \quad \Delta \phi(u, v; \lambda, d) = \frac{1}{2} \left[ I_r(u, v; \lambda, d; \pi/2) + (I_o(u, v; \lambda, d; 0))^2 \right],
\]

(9)

To decrypt \( m(x, y) \) of the plaintext, the object complex function \( M(u, v) \) should be retrieved from the ciphertext of the complex digital hologram function \( H(u, v; \lambda, d) \) by the complex distribution function \( U(u, v; \lambda, d) \) of Eq. (4) including the holographic encryption key \( k(x, y) \) used in phase-shifting interferometry. According to the hologram memory principle, the object wavefront is reconstructed by illuminating the reference wavefront to the hologram. Likewise, the object complex function \( M(u, v) \) can be reconstructed only with knowledge of the reference complex function \( U(u, v; \lambda, d) \) which is now acting as a decryption key. Consequently, the complex distribution \( M(u, v) \) and the plaintext \( m(x, y) \) are recovered as follows:

\[
D(u, v; \lambda, d) = \frac{H(u, v; \lambda, d) U(u, v; \lambda, d)}{|U(u, v; \lambda, d)|^2} = |M(u, v)| e^{i \Phi_M(u, v)},
\]

(11)

\[
d(x, y) = |F^{-1}(D(u, v; \lambda, d))| = |m(x, y)| = m(x, y),
\]

(12)

where \( F^{-1} \{ \cdot \} \) denotes an inverse Fourier transform.

From now on, we propose a new digital method of three-key TDEA to introduce three keys in the phase-shifting interferometry scheme, which easily improves security without adding optical components to the phase-shifting interferometry encryption system. From the proposed optical configuration shown in Fig. 2, let us consider the wavelength of laser diode light as an independent key \( k_1(\lambda) \) and the reference distance between SLM2 and lens L1 as another independent key \( k_2(d) \), respectively, while the holographic encryption key \( k(x, y) \) in phase-shifting interferometry is maintained as an independent key \( k_3(x, y) \). With this concept, the complex distribution function \( U(u, v; \lambda, d) \) of Eq. (4) is modified into \( U(u, v; k_1(\lambda), k_2(d)) \) so that the interference intensity of Eq. (7) is expressed as

\[
I(u, v; k_1(\lambda), k_2(d_r); \delta) = |U_o(u, v; k_1(\lambda)) + U_r(u, v; k_1(\lambda), k_2(d_r); \delta)|^2.
\]

(13)

Since the object and the reference beams in Eq. (13) are changed by two keys, \( k_1(\lambda) \) and \( k_2(d) \), the two-step phase-shifting interferometry makes it so that the complex digital hologram function of the ciphertext is modified into

\[
H(u, v; k_1(\lambda), k_2(d_r), k_3) = A(u, v; k_1(\lambda), k_2(d_r), k_3) e^{i \Delta \phi(u, v; k_1(\lambda), k_2(d_r), k_3)},
\]

(14)

where the amplitude \( A \) and the phase \( \Delta \phi \) are rewritten by replacing \( \lambda \) and \( d \) in Eqs. (9) and (10) with \( k_1(\lambda) \) and \( k_2(d) \). This means that the complex hologram function is dependent on the wavelength and the reference distance in the cryptosystem, and therefore the ciphertext is made by using three independent keys, \( k_1(\lambda) \), \( k_2(d) \), and \( k_3(x, y) \). Now, to decrypt \( m(x, y) \) of the plaintext from the ciphertext \( H(u, v; k_1(\lambda), k_2(d), k_3) \), it is necessary to know all three keys, not only about \( k_1(\lambda) \) of the light wavelength but also about \( k_2(d) \) of the holographic encryption key \( k_3(x, y) \) location in the reference beam. The decryption process for the proposed three-key TDEA is accomplished as follows:

\[
D(u, v; k_1(\lambda), k_2(d_r), k_3) = \frac{H(u, v; k_1(\lambda), k_2(d_r), k_3) U(u, v; k_1(\lambda), k_2(d_r))}{|U(u, v; k_1(\lambda), k_2(d_r))|^2} = |M(u, v)| e^{i \Phi_M(u, v)},
\]

(15)

\[
d(x, y) = |F^{-1}(D(u, v; k_1(\lambda), k_2(d_r), k_3))| = |m(x, y)| = m(x, y).
\]

(16)

Flowcharts of the encryption and decryption processes for the proposed three-key TDEA are shown in Fig. 3, where \( \otimes \) represents the inner product between pixels, FT and IFT denote Fourier transform and inverse Fourier transform, PSI denotes phase-shifting interferometry, SQ denotes a square function, and TH denotes a function to make binary data by a proper threshold. Although wavelength tuning of the light source and precise location control of the distance are required to implement independent keys \( k_1(\lambda) \) and \( k_2(d) \) optically, the effect of three-key encryption is so powerful that the cryptosystem can improve security.

In the proposed digital algorithm applied from the optical configuration as shown in Fig. 2, a pair of a wavelength key and a reference distance key \( k_1(\lambda), k_2(d) \) can be used as a variable public key like a one-time password (OTP). If a specific wavelength key \( k_1(\lambda) \) is challenged to the host
Current Optics and Photonics, Vol. 7, No. 6, December 2023

server, a specific reference distance key \( k_2(d_{rs}) \) is acknowledged to the user according to a predetermined specific key pair \( \{ k_1(\lambda_s), k_2(d_{rs}) \} \). With these two specific key pairs, a user can encrypt private information with a holographic encryption key \( k_3(x, y) \) which is used independently as a private key of a user. Conceptually, the encryption and decryption processes of the proposed three-key TDEA are expressed as

\[
\begin{align*}
c(x, y) &= E_{k_3} \{ E_{k_1 \text{and } k_2} \{ m(x, y) \} \}, \\
m(x, y) &= D_{k_1 \text{and } k_2} \{ D_{k_3} \{ c(x, y) \} \}.
\end{align*}
\]  

III. NUMERICAL SIMULATIONS AND RESULTS

In the encryption process for the proposed three-key TDEA, generating a ciphertext of a complex digital hologram can be performed optically or digitally. However, it is very difficult to control the wavelength \( \lambda \) of light and to align the reference distance \( d \) precisely in implementing the optical setup shown in Fig. 2. A practical method that ignores these limited optical problems is to apply the proposed algorithm to computer-oriented digital processing, which is more convenient than the optical technique. To demonstrate the validity of the proposed method, numerical simulations using MATLAB (R2021) are carried out to show the performance. In this paper, all the data size of inputs is 256 × 256 pixels. A binary image of a monkey, instead of encoded digital data from information, is used as an input plaintext \( m(x, y) \) for visual convenience, as shown in Fig. 4(a).

From the proposed new algorithm shown in Figs. 3 and 4, a specific wavelength of light is chosen as the first independent wavelength key \( k_1(\lambda) \) and a specific reference distance is chosen as the second independent distance key \( k_2(d) \) before processing the phase-shifting interferometry encryption. The third holographic encryption key \( k_3(x, y) \) used in phase-shifting interferometry is assumed to have a randomly generated pattern, as shown in Fig. 4(b). By using Eq. (14), a complex digital hologram function \( H(u, v; k_1(\lambda), k_2(d), k_3) \) is generated by the three keys. It is clear that a plaintext is encrypted in a ciphertext with noise-like random phase and random amplitude distributions, \( A(u, v; k_1(\lambda), k_2(d), k_3) \) and \( \Delta \phi(u, v; k_1(\lambda), k_2(d), k_3) \), respectively. Figures 4(c) and 4(d) show the randomly distributed amplitude and phase maps of the complex digital hologram of the ciphertext.

To verify the reliability of the proposed algorithm, the

![Flowcharts of the proposed three-key TDEA process: (a) Encryption and (b) decryption.](image-url)
The influence of three independent keys, $k_1$, $k_2$, and $k_3$, on the decrypted image is evaluated. The mean square error (MSE) between the decrypted binary image $d(x, y)$ and the original plaintext image $m(x, y)$, representing a relative error between them, is introduced as
\[
MSE = \frac{1}{pq} \sum_{x=1}^{p} \sum_{y=1}^{q} |d(x, y) - m(x, y)|^2 \times 100\%,
\]
where $p \times q$ is the pixel size of the image data. If the decrypted image is retrieved without any error, the MSE is calculated as 0%. In a phase-shifting interferometry cryptosystem, the most important encryption key is the holographic encryption key $k_i(x, y)$, which is determined by independent users selecting a 2-D random distribution function in the key. A detailed explanation about phase-shifting digital holographic optical encryption is given in the [16, 20]. In this paper, we omit the role of the third key $k_3(x, y)$.

First, we examine the suitability of the wavelength key $k_1(\lambda)$ as an independent encryption key. To know the influence of the key $k_1(\lambda)$ on the decrypted image, the MSE according to fractional wavelength change is analyzed for three different light sources. The key $k_1(\lambda)$ with three different designing center wavelengths $\lambda_i$ is given by $k_1(\lambda_1 = 1,550 \text{ nm}), k_1(\lambda_2 = 1,300 \text{ nm})$ and $k_1(\lambda_3 = 670 \text{ nm})$, respectively. The deviation of the wavelength and the fractional wavelength change are defined as $\delta \lambda = \lambda_i - \lambda$ and $\Delta \lambda = \delta \lambda / \lambda$, respectively. Figure 5(a) shows an MSE graph with respect to fractional wavelength change. As shown in Fig. 5(a), the shorter wavelength with $k_1(\lambda_3 = 670 \text{ nm})$ allows larger MSE compared to the long wavelength with $k_1(\lambda_1 = 1,550 \text{ nm})$ for $\Delta \lambda < 0.5 \times 10^{-3}$% when the same $\delta \lambda$ is given. However, the MSE reaches more than 90% for $\Delta \lambda > 0.5 \times 10^{-3}$% regardless of different wavelengths, which means that the decrypted image $d(x, y)$ is quite a different from the original image $m(x, y)$. The deviation of the wavelength of $k_1(\lambda_1 = 1,550 \text{ nm})$ is about $0.007 \text{ nm}$ when $\Delta \lambda = 0.5 \times 10^{-3}$%, for example. It is interesting that a very small deviation of the light wavelength can separate a new independent wavelength key $k_1(\lambda_1 + \delta \lambda)$ with different wavelength from an independent wavelength key $k_1(\lambda_i)$.

Second, to examine the influence of the distance key $k_2(d)$ on the decrypted image as an independent encryption key, the MSE according to fractional reference distance change is analyzed for different distances. The key $k_2(d)$ with different reference distances $d$ is chosen as $k_2(d_1 = 30 \text{ mm}), k_2(d_2 = 40 \text{ mm}), k_2(d_3 = 50 \text{ mm}), k_2(d_4 = 60 \text{ mm})$ and $k_2(d_5 = 70 \text{ mm})$, respectively. The deviation of the distance and the fractional distance change are defined as $\delta d = d$.

![Input data and a complex digital hologram](image)

**FIG. 4.** Input data and a complex digital hologram: (a) Binary image $m(x, y)$ to be encrypted, (b) encryption key $k_i(x, y)$ for PSI, (c) amplitude map $A$, and (d) phase map $\Delta \phi$ of complex digital hologram $H(u, v; k_1(\lambda), k_2(d), k_3)$.

![MSE with respect to fractional wavelength change](image)

**FIG. 5.** Mean square error (MSE): (a) MSE with respect to fractional wavelength change, (b) MSE with respect to fractional reference distance change.


\[ \Delta d = \delta d/d, \]

respectively, where \( d \) is a designing center reference distance from the lens to the input location. Figure 5(b) shows an MSE graph with respect to fractional distance change. As shown in Fig. 5(b), the longer distance with \( k(d_o = 70 \text{ mm}) \) allows a larger MSE compared to the wavelength with \( k(d_o = 30 \text{ mm}) \) for \( \Delta d < 1.5 \times 10^{-5} \% \) when the same \( \Delta \lambda \) is given. The deviation of the reference distance of \( k(d_o = 40 \text{ mm}) \) is about \( \delta d = 60 \text{ nm} \) when \( \Delta d = 1.5 \times 10^{-4} \%, \) for example. The decrypted image \( d(x, y) \) is not discriminated from the original image \( m(x, y) \) for \( \Delta d > 1.5 \times 10^{-5} \% \) because the MSE reaches more than 90% regardless of different distances. It is also noted that the distance separating the next independent wavelength key \( k_2(d_1 + \delta d) \) with different reference distance from an independent distance key \( k_3(d_o) \) is very small.

In addition, Fig. 6 shows the results of decryption for the plaintext of binary image \( m(x, y) \) when the correct wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \) and the correct reference distance key \( k_2(d_o = 40 \text{ mm}) \) are given in the proposed three-key TDEA. Figures 6(a)–6(c) show the decrypted images with MSE = 14.1% in the case of \( \delta \lambda = 0.002 \text{ nm (} \Delta \lambda = 0.13 \times 10^{-5} \% \text{ deviation error)} \), MSE = 63.7% in the case of \( \delta \lambda = 0.004 \text{ nm (} \Delta \lambda = 0.26 \times 10^{-5} \% \text{ deviation error)} \), and MSE = 89.3% in the case of \( \delta \lambda = 0.007 \text{ nm (} \Delta \lambda = 0.45 \times 10^{-5} \% \text{ deviation error)} \), respectively. Figures 6(d)–6(f) show the decrypted images with MSE = 45.0% in the case of \( \delta d = 20 \text{ nm (} \Delta \delta d = 0.5 \times 10^{-5} \% \text{ deviation error)} \), MSE = 74.1% in the case of \( \delta d = 30 \text{ nm (} \Delta \delta d = 0.75 \times 10^{-5} \% \text{ deviation error)} \), and MSE = 91.3% in the case of \( \delta d = 50 \text{ nm (} \Delta \delta d = 1.25 \times 10^{-5} \% \text{ deviation error)} \), respectively.

Third, let us evaluate the dependence of the MSE on the change of the wavelength key \( k_1(\lambda) \) and the distance key \( k_2(d_o) \). To examine the effectiveness of key \( k_1(\lambda) \) and key \( k_2(d_o) \), it is assumed that the specific parameters used for the correct encryption and decryption in simulation are as follows: The wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \), the reference distance key \( k_2(d_o = 40 \text{ mm}) \), the object distance \( d_o = 50 \text{ mm} \), and focal length of the lens \( f = 50 \text{ mm} \) shown in Fig. 2, and the correct holographic encryption key \( k_3(x, y) \) shown in Fig. 4(b). Figure 7(a) shows an MSE graph for wavelength deviation from the correct wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \) with the correct reference distance key \( k_2(d_o = 40 \text{ mm}) \). Although a very small deviation occurs, the MSE increases steeply, and the original plaintext cannot be decrypted. Figure 7(b) shows a detailed part near the correct wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \). The solid blue line shows the MSE for a wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \), while the red dashed line shows the MSE for another wavelength key \( k_1(\lambda = 1,550.007 \text{ nm}) \). If \( k_1(\lambda = 1,550 \text{ nm}) \) is the correct wavelength key in the proposed TDEA cryptosystem, then \( k_1(\lambda = 1,550.007 \text{ nm}) \) is the incorrect key in the same TDEA cryptosystem. From the solid blue line, about 90% of the MSE is shown at a wavelength of \( \lambda = 1,550.007 \text{ nm} \). This means that \( k_1(\lambda = 1,550 \text{ nm}) \) and \( k_1(\lambda = 1,550.007 \text{ nm}) \)

![Fig. 6](image_url)

FIG. 6. Results of decryption for the plaintext of binary image \( m(x, y) \) when the correct wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \) and the correct reference distance key \( k_2(d_o = 40 \text{ mm}) \): Decrypted image with (a) mean square error (MSE) = 14.1% in case of \( \delta \lambda = 0.002 \text{ nm (} \Delta \lambda = 0.13 \times 10^{-5} \% \text{ deviation error)} \), (b) MSE = 63.7% in case of \( \delta \lambda = 0.004 \text{ nm (} \Delta \lambda = 2.6 \times 10^{-5} \% \text{ deviation error)} \), (c) MSE = 89.3% in case of \( \delta \lambda = 0.007 \text{ nm (} \Delta \lambda = 0.45 \times 10^{-5} \% \text{ deviation error)} \), (d) MSE = 45.0% in case of \( \delta d = 20 \text{ nm (} \Delta \delta d = 0.5 \times 10^{-5} \% \text{ deviation error)} \), (e) MSE = 74.1% in case of \( \delta d = 30 \text{ nm (} \Delta \delta d = 0.75 \times 10^{-5} \% \text{ deviation error)} \), (f) MSE = 91.3% in case of \( \delta d = 50 \text{ nm (} \Delta \delta d = 1.25 \times 10^{-5} \% \text{ deviation error)} \).
are keys that are independent from each other. Figure 8(a) shows an MSE graph for distance deviation from the correct reference distance key $k_2(d_r = 40 \text{ mm})$ with the correct wavelength key $k_1(\lambda = 1,550 \text{ nm})$. A very small deviation of the reference distance makes a steep MSE increase, similarly to the deviation of the wavelength. Figure 8(b) shows the detailed part near the correct reference distance key $k_2(d_r = 40 \text{ mm})$. The solid blue line shows the MSE for a distance key $k_2(d_r = 40 \text{ mm})$, while the red dashed line shows the MSE for another distance key $k_2(d_r = 40.00005 \text{ mm})$. If $k_2(d_r = 40 \text{ mm})$ is the correct wavelength key in the proposed TDEA cryptosystem, then $k_2(d_r = 40.00005 \text{ mm})$ is the incorrect key in the same TDEA cryptosystem. From the solid blue line, about 90% of the MSE is shown at a reference distance of $d_r = 40.00005 \text{ mm}$. This means that $k_2(d_r = 40 \text{ mm})$ and $k_2(d_r = 40.00005 \text{ mm})$ are keys that are independent from each other. Also, it is meaningful to show the separability of the incorrect keys $k_1(\lambda = 1,550.007 \text{ nm})$ and $k_2(d_r = 40.00005 \text{ mm})$ in the role of the independent key. In Fig. 7(b), the magenta dashed line shows the MSE for a correct wavelength key $k_1(\lambda = 1,550 \text{ nm})$ and an incorrect distance key $k_2(d_r = 40.00005 \text{ mm})$, which is a different view of the incorrect distance key $k_2(d_r = 40.00005 \text{ mm})$ shown in Fig. 8(b) with respect to wavelength. Similarly, the magenta dashed line in Fig. 8(b) shows the MSE for an incorrect wavelength key $k_1(\lambda = 1,550.007 \text{ nm})$ and a correct distance key $k_2(d_r = 40 \text{ mm})$, which is a different view of the incorrect wavelength key $k_1(\lambda = 1,550.007 \text{ nm})$ shown in Fig. 7(b) with respect to reference distance. According to a similar study on optical image encryption based on interference in [19], the simulation results showed that the wavelength sensitivity is $2 \times 10^{-5} \text{ nm}$ and the distance sensitivity is 2 nm.

To verify the cipher resistance to differential attacks on the proposed method, a number of pixel changing rate (NPCR) test is performed on the ciphertext $c(x, y)$. The NPCR $N(c_1, c_2)$ is defined as

$$t(x, y) = \begin{cases} 0, & \text{if } c_1(x, y) = c_2(x, y) \\ 1, & \text{if } c_1(x, y) \neq c_2(x, y) \end{cases}$$

FIG. 7. Mean square error (MSE): (a) MSE for wavelength deviation from the correct wavelength key $k_1(\lambda = 1,550 \text{ nm})$ with the correct reference distance key $k_2(d_r = 40 \text{ mm})$, (b) the detailed part near the correct wavelength key $k_1(\lambda = 1,550 \text{ nm})$.

FIG. 8. Mean square error (MSE): (a) MSE for distance deviation from the correct reference distance key $k_2(d_r = 40 \text{ mm})$ with the correct wavelength key $k_1(\lambda = 1,550 \text{ nm})$, (b) the detailed part near the correct reference distance key $k_2(d_r = 40 \text{ mm})$. 
The first evaluation is an NPCR randomness test for the proposed three-key TDEA, where \( c_1 \) and \( c_2 \) are ciphertexts before and after one pixel change in a plaintext. \( N(c_1, c_2) \) is calculated as about 4.88% from 10,000 iterations, which gives 0.003% of the MSE. The second consideration is that \( c_1 \) and \( c_2 \) are ciphertexts obtained by deviation from the correct wavelength key \( k_1(\lambda = 1,550 \text{ nm}) \) or the correct reference distance key \( k_d(d = 40 \text{ mm}) \) in the optical configuration. When the wavelength deviation \( \delta \lambda \) is 0.007 \text{ nm}, \( N(c_1, c_2) \) is calculated as about 95.4%. When the distance deviation \( \delta d \) is 50 \text{ nm}, \( N(c_1, c_2) \) is calculated as about 94.5%. These NPCR results suggest that the proposed method provides strong cipher resistance to attacks.

Finally, we discuss the feasibility of the proposed method in secure block cryptography with symmetric key. According to the three-key TDEA standardized as ANSI X9.52, the key length is 168 bits for block encryption. However, the proposed three-key TDEA provides a digital cryptosystem that has three independent keys, a wavelength key \( k_1(\lambda) \), a distance key \( k_d(d) \) and a 2-D holographic encryption key \( k_2(x, y) \) of 256 \times 256 bits. At first, \( k_1(x, y) \) is dependent on the displaying capability of the SLM in implementing the cryptosystem optically. However, the size of key \( k_1(x, y) \) does not matter if only the proposed cryptosystem is implemented digitally. The only limitation to determine key \( k_1(x, y) \) is that a longer key needs a longer processing time in encryption. In this paper, we choose key \( k_1(x, y) \) of size 256 \times 256 bits, which is reasonable for the optical or digital design. Next, the number of independent wavelength keys \( k_1(\lambda) \) is determined by considering a range of the wavelength. In the results as shown in Fig. 5(a) and Fig. 7(b), the minimum wavelength deviation to separate the independent keys of \( k_1(\lambda) \) is about \( \delta \lambda = 0.007 \text{ nm} \). But we choose the deviation of the key \( k_1(\lambda) \) as \( \delta \lambda = 0.4 \text{ nm} \), which is sufficient enough to discriminate each independent key \( k_1(\lambda) \). Next, we consider a tunable range of \( k_1(\lambda) \) as 1,530–1,562 nm because a tunable laser diode source within such a wavelength range can be achieved with the commercial laser diodes used in optical technology. The reason why we select \( \delta \lambda = 0.4 \text{ nm} \) in the range of 1,530–1,562 nm is that it is the wavelength spacing used in the dense wavelength division multiplexing (DWDM) optical communication technique. From the range of 1,530–1,562 nm, we achieve the total number of independent wavelength keys \( k_1(\lambda) \) as \( N(k_1) = (1,562 - 1,530) / 0.4 = 80 \). It is also possible to get \( N(k_1) = (1,562 - 1,530) / 0.01 = 3,200 \) increasingly if we select \( \delta \lambda = 0.01 \text{ nm} \), which has no problem in the proposed digital cryptosystem. Lastly, the number of independent reference distance keys \( k_d(d) \) is determined by considering a range of reference distance. In the results as shown in Fig. 5(b) and Fig. 8(b), the minimum distance deviation to separate the independent keys of \( k_d(d) \) is about \( \delta d = 50 \text{ nm} \), but we choose the deviation of the key \( k_d(d) \) as \( \delta d = 500 \text{ nm} \), which gives sufficient deviation to separate each independent key \( k_d(d) \). In this paper, we consider a tunable range of \( k_d(d) \) as 35–45 mm with a designing center distance of \( k_d(d = 40 \text{ mm}) \). From the range of 35–45 mm, we achieve the total number of independent distance keys \( k_d(d) \) as \( N(k_d) = (45 - 35) / 0.0005 = 20,000 \). If we expand the range of \( k_d(d) \) as 25–55 mm, then \( N(k_d) = (55 - 25) / 0.0005 = 60,000 \), three times larger than in the case of 35–45 mm. Furthermore, if we choose the deviation of the key \( k_d(d) \) as \( \delta d = 100 \text{ nm} \), which is two times larger than the minimum distance deviation of the independent keys of \( k_d(d) \) in the proposed cryptosystem, the total number of independent distance keys \( k_d(d) \) as \( N(k_d) = (45 - 35) / 0.0001 = 100,000 \) can be achieved. This flexibility is an advantage of a digital processing cryptosystem compared to an optical technique. The conventional three-key TDEA standard has a key length of 168 bits. This means that \( 2^{168} \) attempts are needed to find the exact security key, which is very sufficient to protect against key attacks in general. However, the proposed method is assumed to have the 2-D holographic encryption key \( k_2(x, y) \) of size 256 \times 256 bits, and in addition to that, the wavelength key \( k_1(\lambda) \) and the distance key \( k_d(d) \) are assumed to have \( N(k_1) = 80 \) and \( N(d) = 20,000 \), respectively. Thus, the proposed cryptosystem requires \( 2^{256} \times 256 \times 80 \times 20,000 \) attempts to hack the correct block data, which provides much more robustness to the cryptosystem under attack, and more importantly, it can handle 256 \times 256 bits block encryption of data instead of encrypting a 64-bit block of data in the conventional three-key TDEA.

**IV. CONCLUSION**

We propose three-key TDEA of a digital cryptosystem based on phase-shifting interferometry, where a ciphertext of an encrypted binary image is acquired as a complex digital Fourier hologram function with complex amplitude and phase distribution functions. The encryption process is performed with the use of three encryption keys called a wavelength key \( k_1(\lambda) \), a reference distance key \( k_d(d) \) and a holographic encryption key \( k_2(x, y) \), which are independently represented in the reference beam path of the phase-shifting interferometry optical architecture. Different wavelengths of the light source and different reference distances determine independent keys \( k_1(\lambda) \) and \( k_d(d) \), respectively, which provides the keys with many degrees of freedom, and these flexible independent keys can protect against attacks on cryptosystems. The decryption process is carried out by digital processing for the ciphertext of the complex digital hologram with the three keys used in encryption. For the proposed three-key TDEA, the minimum wavelength deviation between the neighboring wavelength keys of \( k_1(\lambda) \) and the minimum distance deviation between the neighboring distance keys of \( k_d(d) \) are achieved as about \( \delta \lambda = 0.007 \text{ nm} \) and about \( \delta d = 50 \text{ nm} \), respectively. For the proposed method in this paper, by choosing the deviation of the key \( k_1(\lambda) \) as \( \delta \lambda = 0.4 \text{ nm} \) and the deviation of
the key $k_2(\delta d)$ as $\delta d = 500$ nm, the number of independent keys $k_1(\lambda)$ and $k_2(\delta d)$ is calculated as $N(k_1) = 80$ for a range of $1,530–1,562$ nm and $N(\delta d) = 20,000$ for a range of $35–45$ mm, respectively, so that $2^{256} \times 80 \times 20,000$ attempts are needed to find the correct key. The results of numerical simulations verify the feasibility of the proposed method.

**FUNDING**

Incheon National University (International Cooperative) Research Grant in 2021.

**ACKNOWLEDGMENTS**

This work was supported by Incheon National University (International Cooperative) Research Grant in 2021.

**DISCLOSURES**

The authors declare no conflicts of interest.

**DATA AVAILABILITY**

Data underlying the results presented in this paper are not publicly available at the time of publication, but may be obtained from the authors upon reasonable request.

**REFERENCES**